



"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 6.4 – Citizen Summits on Privacy, Security and Surveillance: Country report Hungary

Lead Beneficiary: Median

Author(s): Andrea Körmöczy (Median), Márta Szénay (Median), Tímea Venczel (Median)

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 Políticas y Bienes Públicos/
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



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

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

Table of Contents

Executive Summary	i
1 Introduction	1
2 Privacy, security and surveillance in the national context	2
2.1 General national context and country profile of Hungary	2
2.2 Major security policy and strategies	2
2.3 Major privacy issues	3
2.4 Public discourse on surveillance-oriented security technologies and related practices	4
2.4.1 Video surveillance, CCTV	4
2.4.2 Data retention, SLT	5
3 Process design – the citizen summit in Hungary	6
3.1 Organisational setting	6
3.1.1 Citizen recruitment strategy	6
3.1.2 Seating Plan	7
3.1.3 Incentives	7
3.1.4 The venue	7
3.2 Structure of the citizen panel	7
3.3 How citizens assessed the summit	9
4 Empirical results of the citizen summit	10
4.1 General attitudes on privacy and security	10
4.2 How do participants perceive the use of surveillance-oriented security technologies?	14
4.2.1 General attitudes	14
4.2.2 Main perceived advantages and disadvantages of the discussed SOSTs	15
4.2.3 Perceived effectiveness vs. intrusiveness of SOSTs	17
4.2.4 Perceived intrusiveness was weighted in three constitutive dimensions:	18
4.2.5 Acceptability	20
4.2.6 Avoidance, resistance	22
4.2.7 Risk-balance (Trade-off)	23
4.2.8 General attitudes towards technology to foster security	24
4.2.9 Information privacy concerns	25
4.2.10 Proximity	26
4.3 Trustworthiness of security authorities and the role of alternative security approaches	28
4.3.1 Institutional trustworthiness	28
4.3.2 Alternative security approaches	30
4.4 Citizens' recommendations to policy makers	31
4.4.1 Recommendations with regards to regulations and control	32
4.4.2 Recommendations to enhancing information and transparency	32
4.4.3 Recommendations how to protect privacy	33

4.4.4 Topics evoking debates	33
5 Summary and Conclusions	35
6 Bibliography	38
7 List of Figures	39
8 List of Tables	40
9 List of Abbreviations	41
10 Annex	42
10.1 Table recommendations	42
10.2 Postcards	49

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 nine¹ EU member and associated states on the question of the security-privacy "trade-off" as they evaluate different security technologies and measures.

The main objective of this deliverable is to present the Hungarian results of the large-scale participatory assessment completed as part of the SurPRISE project. The Hungarian citizen summit took place in Budapest in January of 2014 with the participation of 211 citizens representing the adult population of the country. During this summit, besides general questions about surveillance, privacy and security, the research concentrated in greater detail on two surveillance-based security technologies: smartphone location tracking (SLT) and smart CCTV.

The deliverable consists of five chapters: after a short introductory chapter, background information is provided about Hungary related to the topic of the SurPRISE project. The third chapter describes the methodology of the empirical research, the fourth contains the main results of this research, and the fifth is a short summary describing the main findings of the empirical research.

1989 proved to be an important turning point for Hungary with considerable consequences related to the main topics of this research: surveillance, privacy and security. This year marked the beginning of political changes, when, after 40 years of a socialist economic system and surveillance-based, one-party communist rule, the country was peacefully transferred to a market economy and a multi-party democratic political system. Soviet troops were withdrawn from the country, after which Hungary went on to join NATO in 1999. Hungary was eventually admitted to the EU in 2004.

Freedom of information and the protection of privacy were key issues in Hungary after sweeping away the earlier totalitarian observation of the communist state, and Hungary led the way in Europe with its privacy act adopted in 1992. However, the new privacy law of 2012 can be seen as a step backward, because it removed the independent commissioner for data protection and freedom, and set up a data protection authority, which – although formally independent – is part of the administrative hierarchy.

At the same time, a large counterterrorism centre was set up with authorization to monitor citizens without the need for a special court order, despite the very low level of terrorist threat to the country.

However, this encroaching move by the authorities was not considered to be a matter of concern by the vast majority of society, because the issues of surveillance and privacy are currently of marginal concern in Hungary. This fact was evident from the comparative analysis of the empirical data. Compared to the other European countries analysed in SurPRISE, privacy concerns in Hungary are relatively low. This relatively careless attitude of Hungarians with regard to personal data and privacy is similarly reinforced by other comparative studies such as Eurobarometer surveys.

A cultural explanation for the lack of debate on privacy issues is largely linked to the fact that democratic development in Hungary was not a long, organic process, as the transition from the dictatorial system to

---

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

democracy was directed from “above” and took place within a very short period of time. Consequently, there is a lack of tradition in this area with a poor mass base of social movements resulting in a weak civil sphere. There are only a few NGOs dealing with data protection and privacy issues, and these groups or organisations similarly lack the mass support they would require. Also, the issue of privacy is dwarfed by the growing economic and financial problems faced by the local population. A further explanation may also be found in the fact that, although Hungary was a surveillance society before 1990, the abolishment of the surveillance- and spy-based oppressive political system resulted in people tending towards the other extreme, and a kind of negligence and carelessness started to develop with regards to personal data and privacy.

It is also highly probable that a general lack of awareness is also major factor when it comes to a relative indifference towards surveillance and its potential effect on privacy. This aspect was further reinforced during the citizens’ summit, where the majority of recommendations made were for the supply of more information as well education in explanation of the technologies employed, their regulation and control in public education, and also for educational campaigns targeted specifically at adults through the public media and other channels.

While privacy concerns are the lowest in Hungary among the nine countries involved in the research, Hungarians seem to be much more concerned about public and personal safety. People in this country are far more concerned about the threat burglary and theft. The incidence of such crimes is continuing to increase as the economic situation deteriorates further. Such fears contribute strongly to the high level of support for smart and traditional CCTV cameras. Although citizens see many collective advantages of CCTV, especially in preventing crime and improving compliance with traffic regulations, this technology has a huge perceived private advantage: it provides an increased level of security in the areas where it is installed based purely on its effect as a deterrent. Negative attitudes towards video surveillance cameras came not from their possible intrusive effect, but rather from their often poor effectiveness when it comes to preventing crime. These personal or indirect negative experiences related to the failure of CCTV resulted in positive attitudes towards the more intelligent smart cameras, which were often seen as the more effective variants of this technology. CCTV measures are regarded as not especially intrusive as the link to identity is not as direct as with smartphone location tracking (SLT), also discussed at the citizen summit.

When considering SLT, people tend to see advantages from the side of personal security and convenience rather than from the side of national security. They do not consider this measure as effective against professional criminals because professionals are always one step ahead. At the same time, SLT increases a sense of personal safety in a completely different way to CCTV cameras: acting as a pocket computer, it provides the possibility to solve problems or ask for help, or helps to maintain contact with family members in their care (e.g. children, old people), and helps to find lost mobile telephones. Although these factors all lead to an increased sense of safety, they are largely due to the convenience features of the device itself. This technology is not seen as a tool that can prevent crime, consequently it has a much weaker effect on the perception of personal security. At the same time, citizens see a lot of drawbacks: e.g. its unfavourable effect on human rights as it may be used for political purposes, and can reveal information not intended to be shared, such as political views, sexual orientation, religion, etc.

The connection between surveillance by smart CCTV and the feeling of security is much stronger than in the case of SLT. In addition, CCTV is perceived as being more effective than SLT as it not only provides information about the place where someone was at a certain time, but also what that person was doing there. On the other hand, although citizens expressed some similar privacy concerns about SLT as with Smart CCTV, these fears often emerged on a more moderate level in relation to video surveillance.

While worries about private and public security were the highest in Hungary, a major deviation from the sample total also showed a considerable difference in regard to the perception of online security. However, this difference appeared in the opposite direction: Hungarians are the least worried of the nine participating nations about internet security. One reason for this may well lie in the fact that Hungary lags behind Western European countries in internet use. Internet penetration and the everyday use of the internet, e.g. for purchasing is significantly less in Hungary than in Western Europe. Also, according to the most recent Eurobarometer survey on cyber security, Hungarians feel less informed about the risks of cyber-crime, which again comes down to a lack of information.

An unexpected connection was also observable between the perception of security and the fear of privacy infringement. Those who feel safe in their daily life tended to worry about privacy less; in other words, if an individual feels generally safe, they similarly feel safe from surveillance. This connection was even stronger in the context of online security: those who worry about security when they are online especially fear of the effect of SOSTs on their privacy. People tend to fear surveillance not just because it might undermine their privacy, but because they fear that data collected about them may be abused and used to harm them.

These results might support a hypothesis that the trade-off model oversimplifies the real life situation. Feeling of insecurity may also be attributed to the effect of mass surveillance. Should this be the case, sacrificing privacy for more security will make no sense. According to the empirical research, the trade-off context applies to assessing SOSTs for every second Hungarian citizen in case of SLT, and significantly less, only one third of citizens, with regard to smart CCTV. They are those, who consider the SOST as useful in terms of security, but risky in terms of privacy. The others regarded the SOSTs as not useful and/or not intrusive. A significant part of those who see these technologies as effective but risky do not intend to sacrifice their privacy for an increased level of security, which is again an argument against the trade-off theory.

Taking SLT and smart CCTV into account, we can observe some factors, which influence the trade-off between security and privacy:

- Sacrificing privacy is more acceptable if identity is not strongly linked to the data that is gathered about a person – SLT is directly linked, while smart CCTV is not
- Sacrificing privacy is less acceptable if the information gathered is more private (e.g. surveillance at the workplace, following every movement of citizen)
- If the surveillance can be “switched off” by the citizen, this makes it more acceptable (e.g. some younger citizens leave their smartphone at home when they go to participate in a political event)
- If surveillance is conducted in a public place (e.g. smart CCTV on the streets, at banks, in shops, at public events, etc.) it is more acceptable, as citizens feel it less intrusive, while surveillance carried out in private spaces (e.g. at home, in an individual’s garden) is seen as less acceptable
- If citizens perceive an obvious link between the use of the technology and its effectiveness to enhance security, it makes the use of the technology more acceptable, even if it is regarded as intrusive to some extent, as in case of smart CCTV
- Having more information about the existence of effective data protection and regulation would make surveillance technologies more acceptable for citizens even if they were aware that the measure might have a negative effect on their privacy

Worrying about the future development of these two technologies was the lowest in Hungary. This is a consequence of the generally lower level of privacy concerns, which is partly a cultural difference between Hungary and the Western European countries in the sample of the project.

Hungarian culture is rather individualistic; consequently, the exceptionally high rate of those who only worry about smartphone location tracking if it hurts their own interest is not surprising.

This same cultural aspect invoked a very different result with regard to smart CCTV. This surveillance measure is not seen as disturbing Hungarian citizens. They see a lot of individual advantages in their use, and, at the same time, the associated risk of privacy infringement is perceived as low, thus video surveillance is welcomed by Hungarian citizens especially in larger cities where alienation is high and the social cohesion is low.

Compared to other countries, Hungarian citizens trust in security agencies slightly more when they use CCTV, and slightly less when they use SLT. Similarly to other countries, a great number of people are afraid of authorities using SOSTs and their potential abuse. When citizens support these technologies despite significant concerns about their privacy and about their abuse by authorities, their respect is often about the technology itself, as a possibility to use it as a national security tool. Compared to other technology assessments, in the case of SOSTs, the advantages are difficult to weight on country level. At

the same time, the associated risk, i.e. the negative effect of mass surveillance is connected to the measure not directly but through the user, i.e. through the political power, which – in addition – is subjected to continuous change, which is again difficult to take into consideration.

Perhaps this is the reason behind the high support of alternative solutions not based on surveillance despite the high level of acceptance of the two technologies discussed, especially (smart) CCTV. Only a very small minority, less than ten percent of citizens, would give preference to SOSTs against alternatives.

The most common alternative suggestion that emerged during table debates was the request for more police rather than more SOSTs. Some participants expressed concern that these technologies might result in a decrease of the number of police, because they felt that these solutions were not able to provide a suitable substitute for police officers.

Another alternative solution was raised in the context of surveillance cameras especially in smaller communities, where people pay greater attention to each other, and this kind of spontaneous neighbourhood watch would make cameras superfluous to requirements.

Preventative and more socially sensitive solutions were also formulated as alternative possibilities:

- Strengthening local communities
- Crime prevention with greater attention to the upbringing of the youth
- Paying more attention to the integration of criminals in society in a way that provides them with special education as well as the opportunity to socialise

These humanistic attitudes, compared to the technocratic approach, include the wish that instead of increasing the control, society should be changed in a way that would see classical moral values regain meaning and support.

Most recommendations of citizens to policymakers reflected the three major problems they see in connection with the usage of surveillance-oriented security technologies:

1. Low level of trust in security authorities, regulation and control
2. Information need of citizens
3. The negative effect of surveillance on privacy

1. Raising the level of trust in security authorities, regulation and control

The far most important recommendation of citizens is that it is necessary to build much stricter regulation in connection with data protection and control.

Citizens feel it necessary that this regulation be made internationally, at the level of the European Union.

Another important issue of the regulation is that a politically independent and professional organization should be delegated to control surveillance and data collection, and that privacy and other human rights should not be harmed. It also emerged that civil organisations would have to undertake this role, but as stated earlier, the NGO sector is weak in Hungary and it should be supported in order to be able to perform these kinds of functions effectively.

It would be important to ensure that regulation does not lag behind the development of security technologies: the European Union should invest more in coping with this development.

2. Informing citizens

It would be necessary to inform citizens about surveillance-oriented security technologies with regard to the following areas:

- What kinds of technologies are used in Hungary?
- How do they work?
- Why are they used?
- How is the collected data protected and controlled?
- How long is the data stored for?

It is also important to inform citizens about their rights in connection with surveillance, and how they might protect their privacy.

3. Weakening the negative effect of surveillance on privacy

It is a common fear of citizens that the use of surveillance-oriented security technologies has a strong negative effect on citizens' privacy. Thus it was an important topic among their recommendations to policy makers to help to protect "innocent" citizens' privacy.

A general expectation from citizens is that surveillance should not be performed without the permission or information of the citizen: e.g. when using smart CCTV, it is important that a sign is placed in a visible place; in connection with SLT, information on these topics should be given by companies to their customers when they buy a smartphone.

Citizens want to have the right to check the data collected about them.

Although citizens were mainly satisfied with the information material they received before the event and the films that were shown to them, and felt that they had gained new insight by participating in the citizens' summit, they were a vaguely sceptical about the effect of the event on decision-makers and politicians.

1 Introduction

The general assumption in Europe has been that more security justifies less privacy. Politicians and decision-makers often prioritize the collection of information about citizens and overlook or ignore the associated privacy issues. At the same time, surveillance technologies and measures are always considered as improving security. But research results question the simple security-privacy trade-off that tends to dominate security policy and practice. The SurPRISE project re-examines the relationship between security and privacy especially in cases when the security solutions involve the collection of information about citizens leading to the possible infringement of their privacy. It empirically investigates the opinion of citizens, i.e. those who are directly affected by the use of these measures, and asks them what they think about surveillance-oriented security technologies (SOSTs). Citizens' summits with around 200 participants were organised in nine countries within the framework of a deliberative opinion research project. The main objective of this report is to present how the Hungarian people perceive security and privacy and look at their opinions about and attitudes towards the surveillance made possible by new developments in security technology.

The Hungarian citizen summit, where Hungarian people had the possibility to discuss these topics and to share their informed opinion, took place in Budapest in January of 2014 with the participation of 211 citizens representing the adult population of the country. The methodology applied qualitative and quantitative data gathering.

An information magazine was sent out to participants before the summit, and they were also shown informative films during the event. Plenary and group sessions followed by turns. Two particular SOSTs were discussed in groups of 6-8 citizens moderated by table facilitators, and at the end of the summit, citizens formulated recommendations towards local and European politicians. In Hungary, Smartphone Location Tracking (SLT) was discussed as the first topic and smart CCTV as the second.

The discussions and the recommendations provide a rich qualitative information base about citizens' attitudes towards these technologies. In addition, quantitative data was also gathered: participants individually answered questions. The questionnaire was projected onto a large screen, and participants voted for a particular answer using electronic clickers. This "technological" approach allowed for immediate feedback on the distribution of the answers in the form of charts projected onto the screen.

The current report summarises the main findings of the Hungarian citizen summit. Chapter 2 provides a short description of the Hungarian country profile, and provides an introductory, national context to the interpretation of the empirical results in Chapter 4, which follows Chapter 3 presenting the methodology of the empirical research as well as the evaluation of the summit itself by the participants. Chapter 5 summarises the main findings.

2 Privacy, security and surveillance in the national context

2.1 General national context and country profile of Hungary

Hungary is located in Central Europe. The country's population is close to ten million². Hungary's public administrative regional units are comprised of the capital city and nineteen counties. Budapest is the only metropolitan city in the country, where one fifth of the total population live. The number of inhabitants is 1.7 million. There are eight large cities with populations of between 100,000 and 200,000. Hungary has a total of 3,152 settlements.

The Hungarian language, unlike the great majority of European languages, does not belong to the Indo-European language family.

Hungary together with Austria formed the Austro-Hungarian Empire between 1867 and 1919. Before this period, Hungary was part of the Habsburg Empire. After World War I, the Treaty of Trianon established new borders for Hungary, according to which Hungary lost 71 percent of its territory and 66 percent of its population³. Hungary entered World War II on the side of the Axis Powers in the hope of regaining at least a part of its former territories. Following the fall of Nazi Germany, Soviet troops occupied the country, and Hungary gradually became a communist satellite state of the Soviet Union known as the People's Republic of Hungary, under a one-party regime from 1949 onwards.

The year 1990 was a turning point in the history of Hungary, when the transformation of the system of political institutions and the economy was peacefully completed in little more than a year. The change of the regime resulted in the soviet-type economy changing to a market economy and multi-party democracy being restored. The prevailing communist ideology, which had been forced on the Hungarian people for decades, was swept out almost from one year to another. The main slogan of the change period was "We're going to Europe", expressing that the new regime wanted to integrate the country both economically and culturally into Western Europe. These efforts were eventually rewarded in full when Hungary joined the EU in 2004.

A new turn, which is important as a part of the background of the examined topic, occurred in the parliamentary election of 2010. The right-wing alliance of Fidesz-KDNP won a two-thirds supermajority of seats. The new government adopted a new constitution in 2011, and modified several aspects of the institutional and legal framework. These modifications have been criticized by the European Parliament as the changes do not comply fully "with the rule of law and its key requirements on the constitutional setting, the system of checks and balances and the independence of the judiciary, as well as on strong safeguards for fundamental rights"⁴.

In the last parliamentary elections in April 2014, the Fidesz-KDNP alliance retained their supermajority in parliament with only 44 percent of the votes, having transformed the electoral system according to their own interest and will.

2.2 Major security policy and strategies

During the past two decades, Hungary has witnessed significant changes on an international level. This period, starting with the Hungarian regime change in 1989-1990 and the collapse of the Soviet Union in 1991 brought many new challenges to the newly established Central European democracy. In the shaping of a new security environment marked by the end of the cold war, it soon became clear that Hungary no longer had to declare any state its enemy, and consequently the threat of a possible military aggression against Hungary was minimal. Thus, the risk of any traditional type of threat became very low, although new types of challenges would soon emerge.

² The number of the population is slightly but continuously decreasing, and it was 9,937,628 according to the latest population census taken in 2011.

³ Compared to the pre-war Kingdom of Hungary, the Hungarian half of the Austro-Hungarian monarchy.

⁴ <http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2013-0229&language=EN>

From the moment of its birth, democratic Hungary showed commitment to participate in the Euro-Atlantic integration process, that is, to become a member of both the NATO and the European Union in the course of time. A decade of transition led first to NATO membership in 1999 and was followed by admission into the European Union in 2004, where Hungary, along with the other newly established independent democracies in its region, laid particular emphasis on the defence of its national interests that followed from its new democratic constitution. Notions, such as “national interest” and “national security” were new phenomena for a country like Hungary, where, for decades, the country had been kept within the sphere of interest of the Soviet Union.

Once Hungary’s Euro-Atlantic integration was completed, the notion of “national security” had to be widened, and the interests and priorities had to be included, which were listed in the strategies and other documents of NATO and the European Union. With Hungary’s national interests becoming interconnected with the interests of its new allies – i.e. the other member states of both organisations – the challenges Hungary was facing, along with the responses to be given to these threats, were set along these new lines. From this it followed that Hungary’s security strategies were based on the same principles and values, repeating the same fundamental points found in the strategies of the other member states.

Democratic Hungary’s first national security strategy was adopted in 2002 that was followed by a new one in 2004, after Hungary’s admission into the European Union, while the most recent strategy was released in 2012. These strategies define security in a comprehensive way, in which the concept of security, over and above traditional political and defence components, includes economic, social – incl. human rights and minority rights – and environmental elements. As core values, the strategies mention peace, security, stability, sovereignty, democracy, the rule of law, freedom of enterprise and fundamental freedoms.

2.3 Major privacy issues

Owing to its different economical, historical and political development, Hungary, as the only former Eastern Bloc country in the project⁵, has significant cultural differences to the other countries in the research consortium. These cultural differences also have an interesting linguistic aspect: there is no direct translation of the term “privacy” in Hungarian. This fact also acts as an indicator of the relatively low importance of privacy in the Hungarian culture. However, the fact that a single word or an identical phrase for privacy is non-existent in Hungarian does not automatically infer that the idea of privacy has not taken root in Hungarian public thought. The fact that surveillance is a marginal concern in Hungary is largely related to the economic and political development of Hungary, which was rather different from the development of Western European countries.

Hungary is a relatively new democracy, where the middle-aged and older generations were socialized in the communist era, when the right to personal privacy was barely recognized. At the same time, surveillance of the citizens by the one-party state was rather strong. Surveillance was based primarily on a network of informers that controlled the entire society, including workplaces, churches, as well as residential communities. Even letters arriving from abroad were opened and read before being delivered. At that time, the main technical solution was to secretly eavesdrop via phone or various listening devices often placed in the homes of politically suspected citizens. Other than direct surveillance, state authorities tracked all kinds of personal data in a manner that would be considered as unlawful today.

Hungary was at the forefront with its privacy act adopted in 1992, as the freedom of information and the protection of privacy compared to the earlier totalitarian observation of the communist state was among the central issues in Hungary’s democratic transition of 1989. Between 2004 and 2011, an independent parliamentary commissioner for data protection and freedom of information operated in Hungary leading a staff of 48 employees⁶.

⁵ East Germany (GDR) also belonged to this bloc, but the project does not differentiate between the two former German states.

⁶ According to the state on 31st of December, 2010; Source: Report on the activity of the commissioner in 2010, p. 297.

From January 2012, a new privacy law replaced the office of the commissioner with a data protection authority, which is – although formally independent – part of the administrative hierarchy, thus the new privacy act can also be seen as a step backward. In April 2012, an action was brought by the EU justice commissioner to the European Court of Justice regarding this concern.

Compared to the former system, the new regulations provide the authority with broader competency to pursue violations of informational rights. In 2013, the average number of employees was 56⁷, thus about 15 percent higher than in the office of the commissioner. The increase of the number of employees can be regarded as reasonable when considering these new powers and associated tasks.

The possibility of secret surveillance by the secret services without a court order has actually been possible in Hungary for a longer time. This possibility was significantly expanded by the establishment of a new, large organisation in September 2010 known as the Counterterrorism Centre.

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

Reactions to the expansion of state surveillance through the setting up of the Counterterrorism Centre, as well as to the abolishment of the office of the independent data protection commissioner were sporadic, and the media coverage of these actions was insignificant.

While significant and widely discussed domestic topics have not emerged with regard to surveillance-based security solutions, the Snowden case reached more than half of the population by the end of 2013⁸. However, the case has not generated a larger public discourse about the local use of these technologies, but rather contributed to an increase in anti-American sentiment.

Compared to Western European countries, the matter of surveillance and privacy is a rather marginal concern in Hungary. It only tends to become the focus of interest when someone is personally affected.

Besides historical, political and cultural reasons, the relatively low level of economic development might also be responsible for Hungarians' lower interest in surveillance matters, as the issue of privacy is dwarfed by their financial problems.

Another reason for the lack of debate on privacy issues is perhaps the fact that the process of democratic development in Hungary was not organic, and – as a consequence – a mass base for social movements is missing, the civil sphere is weak. There are only a few NGOs dealing with data protection and privacy issues, and these groups also lack the support of the masses.

2.4.1 Video surveillance, CCTV

The deployment of CCTV systems by public authorities, primarily in Budapest, was started shortly after the year 2000. And smart cameras began to be deployed a couple of years ago. The existence of smart cameras is generally not known among lay people, who mostly are not aware of the difference between traditional and smart surveillance cameras.

Although it is mandatory to inform citizens about the installation and use of video surveillance cameras – by posting public notices in monitored areas – the authorities failed to comply with the rule in the majority of cases. Surveillance cameras now monitor almost every street and square of downtown Budapest. It has been reported that some of these cameras are equipped with night vision and face recognition capabilities. Authorities have claimed that video cameras are efficient tools against crime. However, some NGOs do not entirely accept this argument, and demand impact studies to be conducted.

In March 2007, after almost three years of litigation, and, finally, as a result of a Supreme Court decree, NGOs managed to receive information from the authorities on the location of the CCTV cameras. This information was then published on a map on the internet.

⁷ Report on the activity of the National Authority for Data Protection and Freedom of Information in 2013. National Authority for Data Protection and Freedom (2014) Budapest p. 26.

⁸ Medián Opinion and Market research weighted the awareness of the Snowden case in November, 2013 on a national representative sample of the population aged 18+.

The law on CCTVs was modified several times. First, in 2008, the police act was amended in order to serve the more precise provision of video surveillance in public spaces. One year later, the act on public space supervision authorised local governments to install video surveillance systems without the participation of the police.

Currently, most typically, it is the local government who decides on setting up a new camera, but it is the police that install, maintain and operate them at the cost of the local government.

The equipment of public transport vehicles of Budapest with cameras has also generated some debate. The Budapest Transport Company (BKV) has started to install CCTV systems in some of its vehicles in 2009. The data protection commissioner – whose office still existed at the time – founded this step as a violation of privacy and also unlawful. Despite this, the deployment of cameras continued, and finally, the legal terms were created by a legislative amendment completed at the end of 2010 by the current government. Further investments were announced for supplying more vehicles in Budapest with cameras.

From spring of 2012, fines can be imposed on motoring offences, registered by surveillance cameras in Budapest, as the police started to use also CCTVs for this purpose.

In 2011, the Hungarian State Railway Company started installing CCTV systems at its stations and on its trains.

2.4.2 Data retention, SLT

The penetration of smartphones showed a significant increase in Hungary in 2013. While in Q4 of 2012, the rate of those who had a smartphone in the adult population (aged 18+) was 17 percent, this rate went up to 27 percent by Q4 of 2013⁹.

The Data Retention Directive (Directive 2006/24/EC) of the European Parliament and the European Council was implemented in Hungary in 2008 with the harmonisation of the Electronic Communications Act¹⁰. At that time, the data protection commissioner expressed constitutional concerns about the modifications, however, it had no effect on the acceptance of the law, and there were no remarkable public debates on this issue either.

In Hungary, the providers of publicly available electronic communications services and public communications networks are obliged to retain all traffic data for one year except for data on unsuccessful call attempts. The latter should be retained for six months only. All the related costs are paid by the service providers.

The law enables investigating bodies, public prosecutors, courts and the secret services to perform their duties, and enables the police and the National Tax and Customs Office to investigate intentional crimes carrying a prison term of two or more years¹¹. Only the police, the National Tax and Customs Office, the secret services, public prosecutors, and courts can have access to retained telecommunications data. Police and the National Tax and Customs Office need the prosecutor's authorisation, while prosecutors and the secret services – including the Counterterrorism Centre (TEK) – may access such data without a court order.

⁹ The source of the data is Medián Omnibus database. Medián Omnibus is completed on a monthly basis on a randomly selected, nationally representative sample of 1200 people. Medián Omnibus is a service product of Medián Opinion and Market Research, a partner of the SurPRISE consortium.

¹⁰ http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0300100.TV

¹¹ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011DC0225:EN:HTML>

3 Process design – the citizen summit in Hungary

3.1 Organisational setting

3.1.1 Citizen recruitment strategy

In the recruitment for the SurPRISE citizen summit, we strived to get a group of citizens who are not professionals in the area of surveillance, privacy and security, and who reflect the national demographics regarding the following criteria:

- Age
- Gender
- To represent both rural, urban and metropolitan areas
- Educational level
- Minorities

We recruited people for this special event with mixed methods to ensure a real mix of participants. We used the following 3 methods:

1. For 8 months our interviewers gave short information on the citizen summit to all respondents of our regular monthly omnibus, which is made on a national representative sample of 1200 respondents per month. If a respondent was interested, interviewers took his/her contact information.
2. We used our interviewer network to recruit participants personally in certain regions. Interviewers asked all the people they met during the active recruitment period (29/12/2013.-05/01/2014.) about their willingness to attend the citizen summit. If an individual showed a willingness to attend, interviewers gave them the contact letter and took their information. We set quotas on age, gender, education and settlement type (urban-rural). We recruited people through our interviewer network from the following counties:
  - Budapest and Pest County
  - Fejér County
  - Győr-Moson-Sopron County
  - Jász-Nagykun-Szolnok County
  - Komárom-Esztergom County
  - Nógrád County
3. Since there are certain groups (higher class people, and youngsters), who are hard to catch offline, we used different online platforms to spread information about the event with the possibility to register:
  - we created a Facebook site for the citizen summit¹²
  - we put an article about the event to our own website¹³
  - as a dissemination activity we had an article published about the citizen summit on one of the main news portal (www.hvg.hu) along with a short radio interview on a major new station (InfoRadio). The possibility to register was mentioned in both

¹² See: <https://www.facebook.com/surprise.hungary?fref=ts>

¹³ See: <http://median.hu/object.1541d7a2-029c-40a8-8a8a-eaf69dd1ac5f.ivy>

All registered potential participants were called from central office to confirm participation and answer a few preliminary questions about:

- their personal details
- whether they were professionals in the area of surveillance, privacy or security
- their internet and mobile phone usage
- also a few questions about plans for travel, food allergies and everything we needed for organizing

From among those who confirmed participation, we selected non-professionals and sent a consent form, a confirmation letter about the project and the program of the day. Also practical information about time and place, public transportation and parking, travel reimbursement, as well as the information magazine was sent to the invited citizens. Those not selected received a letter of thanks and explanation.

3.1.2 Seating Plan

We made a seating plan before the summit to have a good mixture of people at each table. The mixing gave the citizens an opportunity to talk to people from other parts of the country and with different backgrounds to their own. Mixing them in this way also helped ensure that their deliberation would reflect different experiences and points of view, thereby ensuring that the citizens had reflected on other opinions and points of view before casting their vote.

We used the following method to prepare a seating plan according to the above mentioned principles.

We had a data file with all the information we had about participants. We had personal data from registration and other data from the questionnaire we asked them when calling back. It also asked whether they would come with someone they knew. We made the same identification number for those who knew each other.

Then we ranked all participants by phone number (randomly) and gave every eighth person the same table number. Then we checked whether there were acquaintances at the same table and also tried to avoid people sitting at the same table from the same town (except Budapest). If changes were needed, we also checked age and education composition of the table and tried to make the exchange to make the table a good composition of all the type of people.

3.1.3 Incentives

All participants received a gift voucher for the value of HUF 4,000 (approx. EUR 13) as an incentive.

All participants were paid transport reimbursement, and were provided with free food and drinks while participating in the summit.

3.1.4 The venue

The citizen summit took place at VAM Design Centre, an exhibition and event hall in central Budapest (6th District). Participants were seated in the atrium (670 m²) at 32 round tables. At each there were 5-7 participants and a table facilitator. 3 tables also had someone taking notes. There was an extra table for the press (including journalists from the national news agency and a TV channel). The buffet was set up also in the atrium, while the preparation room was separated. There was a separate, manned cloakroom, and an extra room for the morning briefing of the table facilitators. We used 2 screens to ensure that everybody could see the material presented.

3.2 Structure of the citizen panel

We sent invitation letters to 257 citizens, out of which 215 participated.

Recruitment was very successful among the youngest age group, who are typically the hardest to reach. The gender of participants was generally balanced. Participants tended to have a higher level of schooling than the average, perhaps due to the fact that they had a greater interest in discussing such issues.

All types of residential area were represented among participants: one third of participants lived in a metropolitan area, another third in an urban area, and almost one quarter in a rural area.

Most of the participants were active in work: the employment status of general population was suitably represented at the summit. The same was true for minority groups.

In summary, it can be said that, compared to the relatively low number of the sample, the average Hungarian population was well represented at the Hungarian citizen summit (Table 1).

	Participants N=215	Population ¹⁴ aged 18-69 N=6 988 516
Total	100	100
Age		
18-29	27	21
30-39	14	23
40-49	22	19
50-59	22	20
60-69	14	17
70+	1	
Gender		
female	56	51
male	43	49
n.a.	1	
Education		
primary school (8 th year or less)	5	20
lower secondary (vocational without graduation)	14	26
upper secondary (with graduation)	30	28
vocational qualification (after graduation)	17	6
university – undergraduate (college, BA/BSc)	21	12
university – postgraduate (university, MA/MSc, PhD)	12	8
n.a.	1	
Residential area		
metropolitan area	39	39 ¹⁵
urban area	38	31 ¹⁶
rural area	22	30
n.a.	1	

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

¹⁴ Population Census, 2011

¹⁵ Budapest, County towns and County authorities

¹⁶ The other cities

3.3 How citizens assessed the summit

The summit was very successful in providing new insight for participants: more than two-thirds of participants expressed satisfaction at the end of the summit (see Figure: 1).

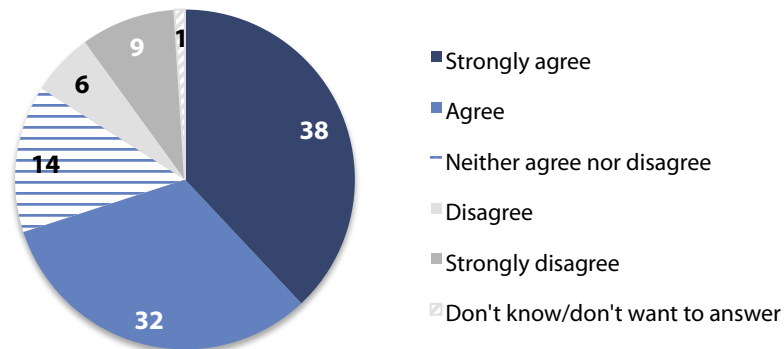


Figure: 1: „I have gained new insight by participating in the citizen summit” (percentage, N=193)

Participants were slightly more sceptical about the influence the summit could have on politicians. Most participants agreed that it generated valuable knowledge for politicians, the other part could not totally agree with this (see Figure: 2).

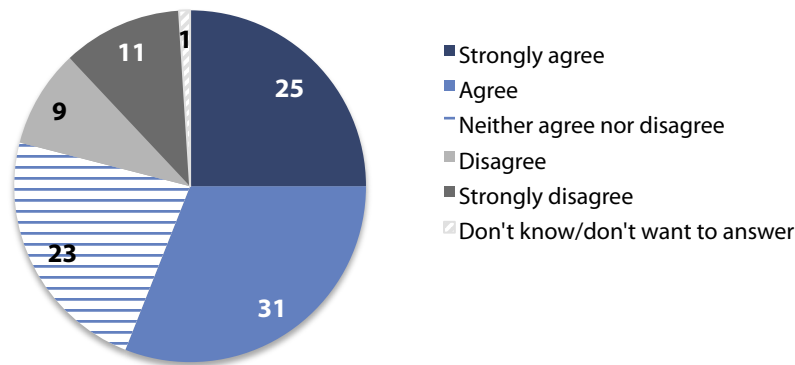


Figure: 2: „I believe the citizen summit has generated valuable knowledge for the politicians”(percentage, N=196)

The summit did not change general attitudes of participants: two-thirds of them felt their attitudes to be the same as before. One-quarter of citizens felt more positive about security-oriented surveillance technology than before the summit, and it was 9 percent who became more negative (see Figure: 3)

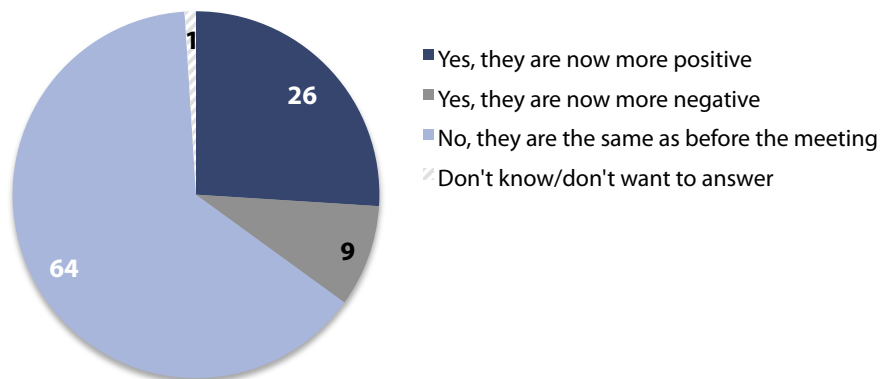


Figure: 3: Has this experience changed your attitudes regarding security oriented surveillance technology? (percentage, N=206)

4 Empirical results of the citizen summit

4.1 General attitudes on privacy and security

Among the nine countries that were involved in the research, the citizens of Hungary expressed the largest concerns with safety, especially when they evaluated this aspect from a collective point of view: only 31 percent of them regarded Hungary a safe place in which to live (Table 2), while this rate was 66 percent in the total sample of the nine countries.

From an individual point of view, opinions were more positive about safety (Table 2), although again the rate of those who generally felt safe in their daily life was significantly below the sample total: it was 45 percent compared to 63 percent in the total sample of nine countries.

The issue of security is perceived in the context of the Hungarian state of affairs. Citizens do not experience the danger of terror attacks in everyday life, as Hungary is not a prime target of terrorist groups. For an average Hungarian citizen, terror attacks appear only in the foreign news when watching TV news or reading newspaper. Hungarians are more afraid of being a victim of a crime that targets their person or their possessions, or of social insecurity (increasing level of unemployment, economic crisis, being permanently ill).

Major deviation from the sample total characterised Hungarians with regard to the perception of online security as well, but this difference was in the opposite direction. Hungarians worry about internet security the least out of the nine countries. A reason behind this may be that Hungary lags behind Western European countries in internet use: internet penetration is lower as is the use of the internet to deal with everyday tasks: e.g. online purchase is also significantly behind the Western European countries. In addition, Hungarians feel less well informed about the risks of cybercrime according to the most recent Eurobarometer survey on cyber security¹⁷.

	N	Strongly agree	Agree	Neither, nor	Disagree	Strongly disagree	NA	Total
		Percentages						
"I generally feel safe in my daily life"	204	9	36	33	17	4	1	100
"I feel that this country is a safe place in which to live"	205	5	26	31	25	13	0	100
"I worry about security when I am online"	205	17	19	31	22	10	1	100

Table 2: General attitudes on security

When examining the aspect of privacy in terms of surveillance-based security technology, we first have to talk about the awareness of these technologies.

Citizens generally reported low information levels concerning surveillance-oriented security technologies. Before applying to participate in the citizen summit, the great majority (71 percent) had only some knowledge or knew almost nothing about these topics (see Figure 4).

¹⁷ Special Eurobarometer 404 - Cyber security, 2013. pp. 7-22.

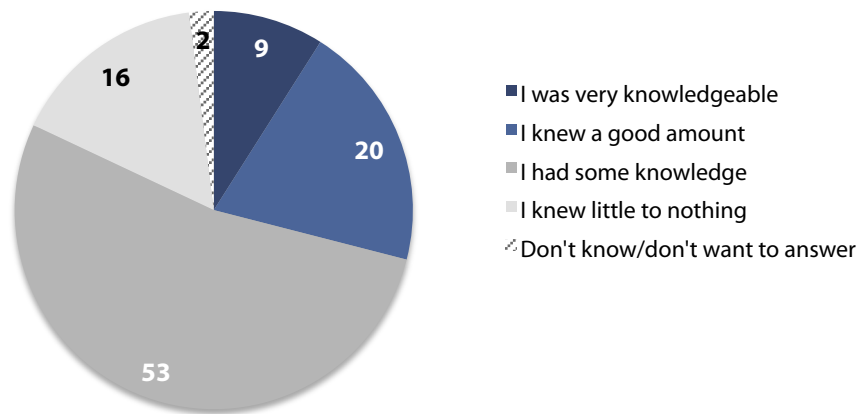


Figure 4: Before reading the SurPRISE information booklet how would you rate your knowledge of surveillance-oriented security technologies? (percentage, N=203)

Not surprisingly – because the topic is a “technical one” – male participants knew a lot more about these things than females (Table 3).

	N	I was very knowledgeable	I knew a good amount	I had some knowledge	I knew little to nothing	NA	Total
<i>Percentages</i>							
Females	112	7	12	62	19	-	100
Males	87	12	31	42	11	3	100

Table 3: Prior knowledge on surveillance-oriented security technologies according the gender

Besides gender, awareness of the surveillance-based security technologies showed huge differences between the generations (Table 4). While younger citizens used many new IT technologies on a daily basis thus having vivid experiences, and feeling more comfortable talking about this topic as they had wider vocabulary expressing their thoughts, members of older generations felt a little lost in this “technocrat” world. But they all agreed that the rapid development of the technologies goes hand in hand with the development of society – although this development is difficult to follow, citizens often formulated the opinion that they have no other choice than to accept it.

	N	I was very knowledgeable	I knew a good amount	I had some knowledge	I knew little to nothing	NA	Total
<i>Percentages</i>							
18-39 years	84	12	27	42	14	5	100
40-59 years	85	7	16	59	18	-	100
60+ years	31	6	10	68	16	-	100

Table 4: Prior knowledge on surveillance-oriented security technologies according the age

The differences between generations could also be observed when talking about the phenomenon of surveillance itself, independently from the technology applied. While younger citizens often summarized their attitude towards surveillance with responses like:

"If you live an honest life, you don't have anything to hide."

Surveillance itself often evoked painful memories and negative feelings in older citizens:

"This surveillance is the same as we experienced during the communist regime, only carried out by different technologies."

On the other hand, when talking about privacy issues, we observed the opposite attitudes: younger citizens were more sensitive about this topic than members of the older generations. Older citizens believed that they were *"small fish"* and that their personal data was not interesting enough for anybody. While younger participants saw this issue from a different perspective. They had much more personal experience on seeing the personal data of others, e.g. on Facebook, and could mention several problems occurring from this kind of *"transparency"* of personal information. In addition, younger citizens were much more aware of the fact that each citizen's personal data could be of interest to, for example, a company for marketing.

Facebook is often used as a reference base when talking about the relationship between surveillance/personal data collection and privacy. Using the analogy of problems that emerge by letting other people see our personal data on Facebook makes it clearer for citizens how the collection of personal data by mass surveillance can affect citizens' privacy. Typical examples mentioned were:

- Others can see that we are on holiday, so they can burgle our home, or it could cause trouble at the workplace if we reported illness for that period
- When applying for a job, an human resources department can check our personal data as well reading our CV

While half of participants were concerned that the use of surveillance-oriented security technologies were eroding privacy in general, opinions were more divided, when the same question was formulated not on a general level but with reference to themselves. An explanation for this can be that talking about the topic in general refers rather to the theoretical level of the phenomenon, thus the consideration of the question is less restricted in space and time, and might include general concerns related to the future or because of the experience of others. At the same time, answers from a person's personal point of view tend to refer more to the present, daily, more concrete worries. *"Theoretically"* 51 percent of citizens worried about the privacy infringing effect of SOSTs in general, while only 44 percent of them expressed stronger fears that these technologies might endanger their own privacy (Table 5). Compared with other countries in this research, Hungarian people showed the lowest level of concern about privacy. This, let us say, relatively careless attitude of Hungarians with regard to personal data and privacy is also supported by other international studies¹⁸.

Possibly owing to the fact that the lack of knowledge often stands behind fear of the new, the concerns about the privacy-infringing aspect of SOSTs decreased by the end of the citizen meeting as a consequence of the knowledge gained (Table 5). However, this positive change of opinion tended not to characterize the summits of other countries, where the opposite tended to occur, and the

¹⁸ Special Eurobarometer 359 - Attitudes on Data Protection and Electronic Identity in the European Union, 2011.
Special Eurobarometer 390 - Cyber security, 2012.
Special Eurobarometer 404 - Cyber security, 2013.

deliberation process intensified concerns initially expressed. A part of the explanation may be that smart CCTV was the second topic to be discussed in Hungary, and this SOST was evaluated rather positively both from the point of view of effectiveness and its effect on privacy (see Chapter 4.2.2.2).

In Hungary, where concerns about public security were the highest, citizens saw a good solution in smart cameras.

		N	Strongly agree	Neither, nor	Disagree/ Strongly disagree	NA	Total
			Percentages				
<i>"I am concerned that the use of surveillance-oriented security technologies is eroding <u>privacy in general</u>"</i>	Before the event	208	51	24	25	-	100
	After the event	202	38	31	30	-	100
<i>"I am concerned that the use of surveillance-oriented security technologies is eroding <u>my privacy</u>"</i>	Before the event	207	44	26	30	1	100
	After the event	196	39	21	39	1	100

Table 5: General attitudes on privacy with respects to intrusiveness of surveillance-oriented security technologies

An unexpected connection can be observed between the perception of security and the fear of privacy infringement. Those who felt safe in their daily life tended to worry about privacy less, in other words, those individuals who feel safe also feel safe in relation to surveillance. This connection cannot be observed with regard to the perception of public security, but was even stronger in the context of online security. Those who worried about security when they were online especially fear the effect of SOSTs on their privacy (see Table 6).

Although Deep Packet Inspection was not discussed in Hungary, the Snowden case and its consequences were still topics in the media at the time of the Hungarian fieldwork in January 2014, and despite the strong predominance of domestic political news in the Hungarian media, news reports about the Snowden case reached the majority of the Hungarian citizens.¹⁹ There were participants on the Hungarian citizen summit, especially young people, who would have been strongly interested in the DPI topic²⁰. A few explicitly expressed the suspicion that it was not a coincidence that this topic could not be discussed in Hungary, and supposed that it was not allowed. These opinions can be interpreted as expressions of some kind of distrust towards the Hungarian or European authorities.

These results might support the hypothesis that the trade-off model oversimplifies the situation of real life. The reason for feeling insecure may also be attributed to mass surveillance. If this is the case, sacrificing privacy for more security will make no sense.

¹⁹ According to a national representative survey of Medián in November of 2013, 58 percent of the adult population has heard about the Snowden case.

²⁰ Three topics were included in the information magazine, from which only two were discussed in each country. The distribution of topics among the countries took into consideration the cultural similarities and dissimilarities, as well as the penetration data. Each SOST out of the three was tested by 6 countries.

		<i>"I am concerned that the use of surveillance-oriented security technologies is eroding privacy in general"²¹</i>				
	<i>N</i>	Strongly agree/ Agree	Neither, nor	Disagree/ Strongly disagree	NA	Total
<i>Percentages</i>						
Private security:						
Generally feel safe in daily life	92	43	21	36	-	100
Neither, nor	65	62	26	12	-	100
Generally do not feel safe in daily life	44	52	32	16	-	100
Online security:						
Don't worry about online security	74	36	23	42	-	100
Neither, nor	63	54	30	16	-	100
Worry about online security	64	62	19	19	-	100

Table 6: Connection between perceived private security, online security and privacy

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

4.2.1 General attitudes

During the Hungarian citizen summit, participants discussed smartphone location tracking and smart CCTV.

Although the great majority of citizens had knowledge on the location tracking function of their mobile phone (see Figure 5) which makes phone calls possible, it turned out during the discussion that they had rather limited knowledge of this technology:

- they were not aware of the data collection itself

"Service providers should call our attention to the fact of data collection when we sign the contract."

- older citizens were unable to determine the difference between data collection based on the use of GPS versus collecting data through phone masts, and did not really understand the way these features work:

"They cannot watch me because I only use my mobile phone for making calls."

²¹ The question on privacy asked before the event was included in the table, but similar connection can be observed using the same question asked at the end of the event or taking into consideration the question referring to participants own privacy.

While talking about the different features of smartphones and SLT, the differences between the different generations increased: members of the older age group felt that the development of the technologies and their users were apart from each other:

"We do not understand our phone, it's starting to live a life of its own."

A general observation of the table moderators was that, when talking about smart CCTVs, a great number of citizens did not differentiate between smart and traditional CCTV cameras, and the two types of these technologies mixed in their answers when voting in response to questions. Traditional (non-smart) cameras are widely known in Hungary, but smart cameras are generally not known, and for some citizens, especially older people, even the smart functions proved difficult to fully understand.

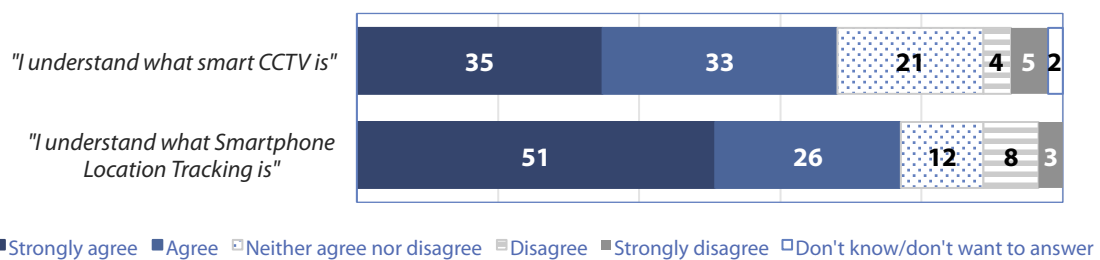


Figure: 5: Knowledge about how the technology works (percentage)

Those who live in smaller settlements or in the suburbs of a larger city rarely or never come into contact with CCTV cameras in the area where they live (see Figure 6).

The great majority of participants at the Hungarian meeting owned a mobile phone (see Figure 6).

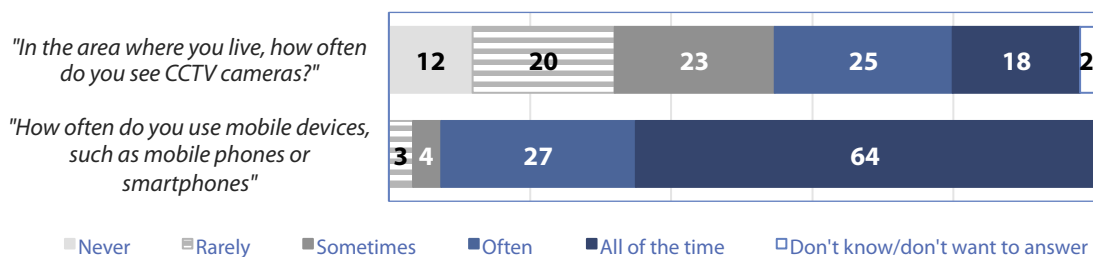


Figure: 6: The extent to which someone is getting "in touch" with the technology in daily life (percentage)

4.2.2 Main perceived advantages and disadvantages of the discussed SOSTs

In this chapter we summarise the table discussions on the main perceived advantages and disadvantages of the two SOSTs that were discussed during the Hungarian citizen summit.

4.2.2.1 Smartphone location tracking

When taking positive aspects of SLT technology account, mainly younger citizens accepted the convenient features of SLT, while older ones often did not really see a reason for using these features:

"I prefer to read road maps."

Citizens perceived the advantage of the convenience, which is offered by SLT from a mainly individual point of view:

- GPS: one can get from A to B more easily and quickly – this feature can enhance mobility of users
- In case of an accident, it is easier to find the injured person
- Finding lost relatives (e.g. kids or old people)
- Finding lost or stolen mobile phones
- Controlling kids by checking where they go
- Can help building relationships: finding friends who are nearby

Besides personal convenience, citizens saw some collective advantages of the use of SLT:

- Detection of criminals and their networks – although criminals also use devices like mobile phones, SLT can be suitable to detect only less sophisticated criminals, as “professionals” are always one step ahead of technology
- Organization of traffic – offering alternative routes for drivers, optimising fuel consumption thus saving the environment
- Tracking the shipping of an important consignment

Concerning the perceived advantages and disadvantages of SLT, citizens saw more drawbacks, and reported more fears in connection with the use of this technology than advantages:

- Citizens said that they could not control who might do what with their personal data:

“I can imagine that some companies buy this data from the service provider and bombard us with their marketing.”

“For some good money, the mobile service provider can hand over the data to someone who will use this data for their own purposes.”

- Using SLT will have the unfavourable effect of decreasing the level of human rights, as SLT technology is a suitable tool for surveillance with political aims, as it reveals information that is not intended to be shared like political views, sexual orientation, and religion.

“It is a suitable tool for intimidation not only for enhancing security.”

- A less strong but still existing fear concerning SLT is that location data sometimes is not accurate enough, meaning that use of this data may incriminate innocent people.

“It can happen that I was at the place of a crime, just because I live nearby, but they think that I committed the crime based on this data.”

4.2.2.2 Smart CCTV

Citizens see many advantages of using smart CCTV. Most of CCTV's advantages have collective as well as individual aspects.

Individual advantages:

- Increases the feeling of security e.g. at night, or at deserted places
- Help can come quicker if someone is in trouble
- Finding lost people

Collective advantages:

- Finding criminals, screening suspicious people at festivals / events, finding wanted persons
- Examining accidents
- It can change people's behaviour: preventing crime and defacement – CCTV has a preventative effect even if it is not watched by an operator or not linked to the police
- Improving compliance with traffic regulations
- Scientific purposes: e.g. monitoring human behaviour

Although citizens see many advantages of smart CCTV, they also mentioned several disadvantages of the usage of this technology:

- There are no fewer crimes in general, as criminals only go to districts where there is no CCTV
- Functional disorder: CCTV cameras cannot work well in bad weather or at night – provide bad quality data
- The algorithm on which the smart CCTV based on is not perfect leading to possible false alarms
- Data gathered by CCTV can be manipulated, e.g. time code can be changed
- Criminals can easily hide themselves wearing a hood or a helmet, or by shining a light into the camera which loses its focus for a while
- Smart CCTV cannot see everything, there are "grey areas"
- Unreliability of operators: an operator sitting at a screen might be tired, or can make mistakes
- Expensive

4.2.3 Perceived effectiveness vs. intrusiveness of SOSTs

According to the risk-benefit framework, the beneficial and less risky a technology is perceived to be, the higher the level of acceptance²². In the context of this study, perceived benefits are covered by the variable "perceived effectiveness". This variable was weighted with four reference variables:

- perceived security as a personal benefit
- accuracy, i.e. the extent to which the security system properly detects and identifies risk
- validity, i.e. the extent to which the security system actually addresses a real threat
- public security

The first three were weighted on the Likert Scale, while the fourth was an answer possibility of a multi-choice question²³.

A large number of citizens believed that both SOSTs were effective national security tools, however, in the case of (smart) CCTV, it was the majority of participants thought that this measure was capable of enhancing national security. Opinions were strongly divided whether these were the appropriate technologies to address national security threats.

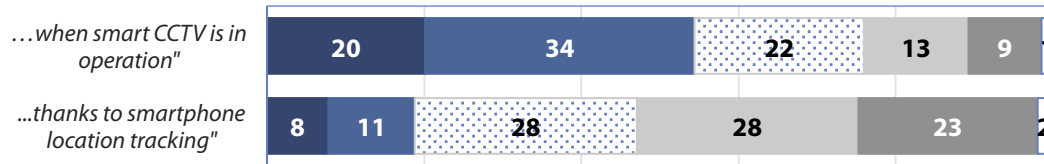
²² Pavone, V., Degli Esposti, S., Santiago, E. (2013) „Draft Report on Key Factors“, „D2.2 of Surprise Project“, p. 93.

²³ See the questionnaire in D4.2.

Every second participant's subjective feeling of safety increased if (smart) CCTV was used. SLT had a much weaker effect on the perception of personal security: only one-fifth of participants felt more secure or protected because of the use of SLT (see Figure 7).

Dimension 1: Perceived security as a personal benefit

"I feel more secure ..."



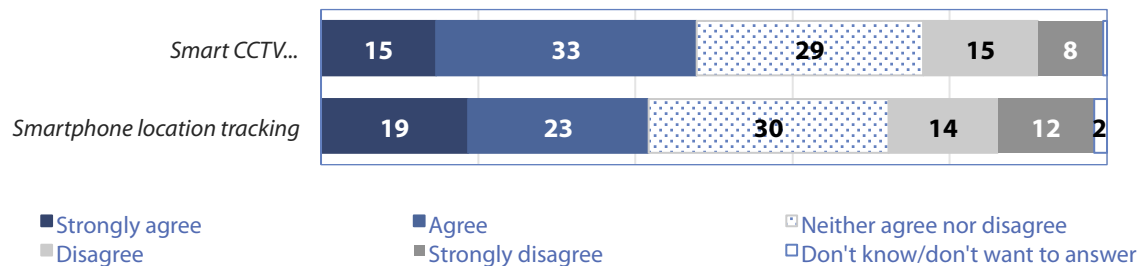
Dimension 2: Accuracy

"In my opinion, ... is an effective national security tool"



Dimension 3: Validity

"... is an appropriate way to address national security threats"



Dimension 4: Public security

"I believe ... improves national security"

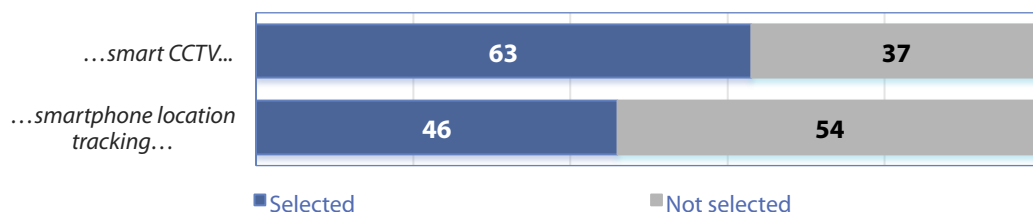


Figure 7: Perceived effectiveness (percentage)

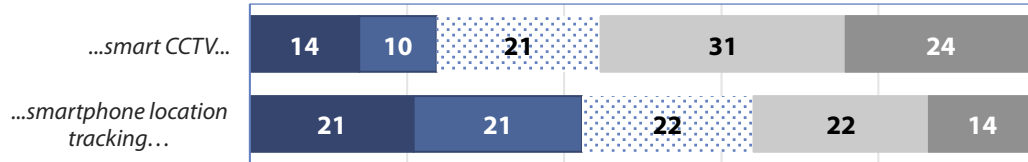
4.2.4 Perceived intrusiveness was weighted in three constitutive dimensions:

- risk of embarrassment
- intrusiveness, as the extent to which the security system is forced upon someone without invitation or permission
- risk of the infringement of civil liberties: this variable was weighted on both a personal and a public level

SLT was regarded significantly more intrusive than (smart) CCTV, especially because it has a negative effect on fundamental human rights. In actual fact, only the minority of participants regarded (smart) CCTV to be an intrusive security measure (see Figure 8)

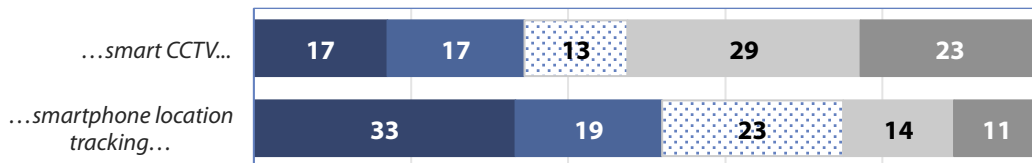
Dimension 1: Risk of embarrassment

"The idea of ... makes me feel uncomfortable"



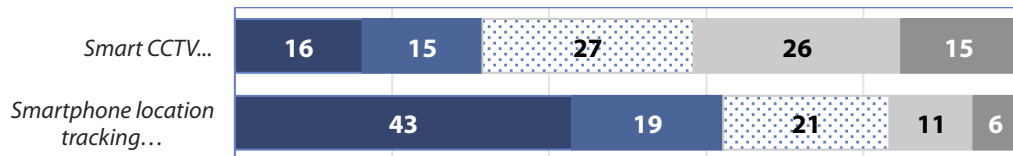
Dimension 2: Intrusiveness in terms of forcing it upon someone

"I feel that ... is forced upon me without my permission"



Dimension 3a: Risk of civil liberties infringement – individual aspect

"... worries me because it could violate my fundamental human rights"



Dimension 3b: Risk of civil liberties infringement – collective aspect

"... worries me because it could violate everyone's fundamental human rights"

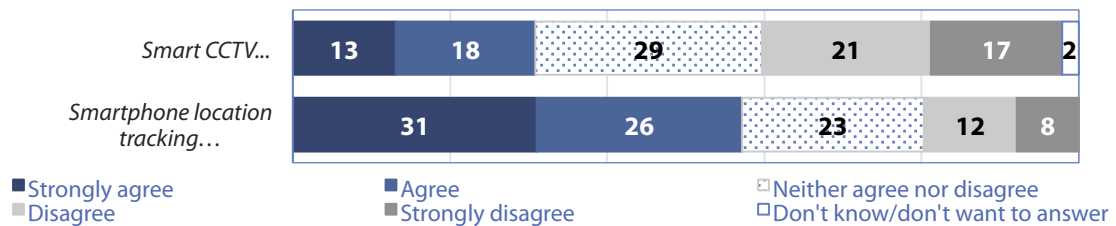


Figure 8: Perceived intrusiveness (percentage)

Substantive privacy concerns, a variable developed for the sake of this study, considers anxieties related to both information and physical privacy. Preoccupations related to the impact of specific SOSTs on one's identity, disclosure of sensitive information, broadcasting of intimate relationships and wiretapping of personal communications can affect the extent to which people are willing to accept, engage with or be monitored by technology. The variable is partitioned into three dimensions in our analysis: intimacy, solitude, anonymity²⁴.

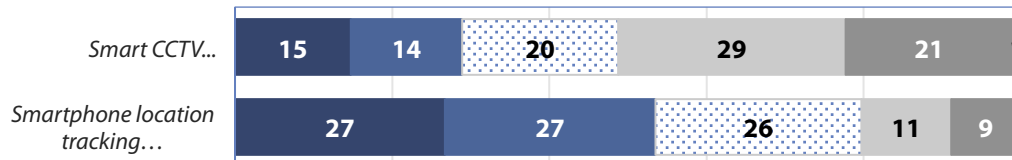
Actually, privacy concerns regarding (smart) CCTV (see Figure 9) were the weakest in Hungary compared to the other five countries where this security measure was discussed.

²⁴ For more detailed description, see this deliverable of the Surprise project: Pavone, V., Degli Esposti, S., Santiago, E. (2013) "Draft Report on Key Factors", "D2.2 of Surprise Project", pp. 92-93.

Negative attitudes towards video surveillance cameras did not primarily stem from their possible intrusive effect, but rather from their ineffective use. There was someone at almost each table, who told a story when the camera had been there but the crime – despite this fact – had occurred. These experiences resulted in positive attitudes towards the more intelligent, smart cameras that could possibly increase effective use. Substantive privacy concerns were significantly stronger with regard to SLT, although it was slightly more moderate than in the total sample of countries where SLT was discussed.

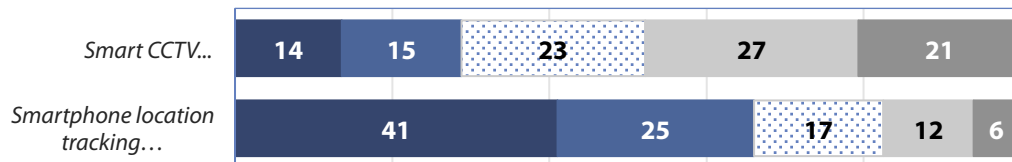
Dimension 1: Intimacy

"... worries me because it could reveal sensitive information about me"



Dimension 2: Solitude

"... worries me because it could let strangers know where I am"



Dimension 3: Anonymity

"... worries me because it could result in my behaviour being misinterpreted"

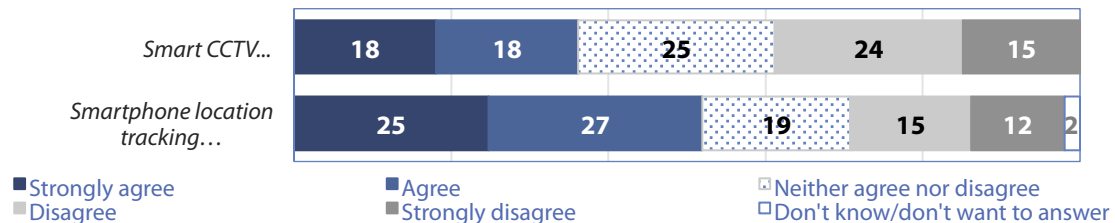


Figure: 9: Substantive privacy concerns²⁵ (percentage)

4.2.5 Acceptability

Both discussion rounds were finished with a question on acceptability of the discussed technology. Especially (smart) CCTV was regarded as an acceptable solution for the increase of national security: the great majority of participants (82 percent) supported its adoption.

The acceptability of smartphone location tracking was also high: two-thirds of participants supported this measure. However, while the rate of those who definitely rejected the use of surveillance cameras was very low at only 8 percent, the number of those definitely opposed to the use of SLT for security purposes by security agencies was twice as much: 17 percent (see Figure 10).

²⁵ The fourth dimension of substantive privacy concern, "Reserve", which is about guarding communications from prying, can be interpreted only with regards to DPI, which technology was not discussed in Hungary.

"Overall I support the adoption of ..... as a national security measure"

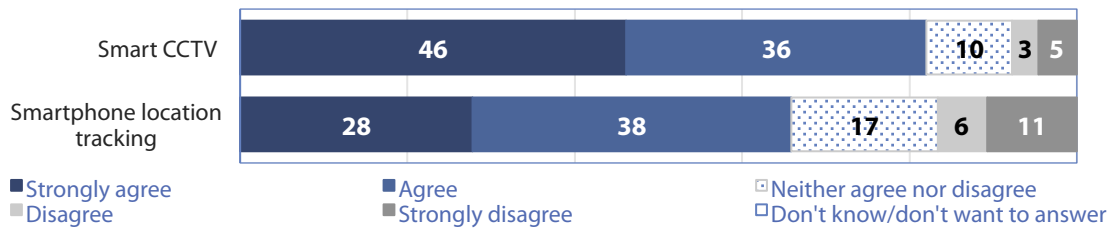


Figure: 10: Acceptability of smart CCTV and Smartphone location tracking (percentage)

The main reasons why Smart CCTV was regarded as a more acceptable measure than SLT are the following:

- Citizens had more personal experience of CCTV in general, as they have seen them operating on the streets, in banks, in shops and on roads controlling drivers.
- Citizens generally reported that smart CCTV was less intrusive in private life than SLT technology, as the link to identity was not that direct. There are three cases when surveillance by CCTV is not accepted:
  - when CCTV is used at the workplace, where identity can be directly linked to the data of CCTV
  - when surveillance covers private homes or private gardens
  - when surveillance is made by a private person, and not for official/social aims
- Connection between surveillance made by smart CCTV and the feeling of security is much stronger than in case of SLT, as citizens mentioned real life examples when prevalence of crime decreased after CCTV had been installed. In addition, it was seen as more effective than SLT as it not only gives information about the place where someone was at a certain time, but also what the person was doing there.

"In the 8th District of Budapest, the prevalence of crime fell dramatically when they started to use CCTV on the street, like on Blaha Lujza Square."

"It does not bother me at all if they use it in public areas, but it actually gives me a feeling of security."

On the other hand, citizens expressed some fears in connection with smart CCTV as well. Some of these fears are the same like in case of SLT, but often emerged on a more moderate level:

- Fears concerning data protection and control like in case of SLT, although these fears were a bit more moderate probably due to the fact that data collected by smart CCTV perceived as less intrusive.
- Another fear is that the usage of smart CCTV might increase unemployment, as less policemen and operators will be needed behind the screens.
- It can have unfavourable effect on human rights, like in the case of SLT technology.
- A less strong but still existing fear is that smart CCTV cannot operate well in bad circumstances (the recorded picture is not clear enough), and so innocent people might be incriminated.

Despite these fears, the overall acceptability of CCTV in Hungary is very high even when compared to the other countries where smart CCTV was discussed. Its acceptability was higher only in the UK, where CCTV cameras have a long tradition, and citizens are used to it. But in Hungary, the reasons are different.

Here their mass deployment only goes back for the last couple of years, and the use of the smart versions has only started recently. Actually, the main security problem of citizens here is crime and petty crime, and people expect cameras to have a deterrent effect. This perceived psychological effect is the reason why, despite the fact that several citizens shared experiences when a CCTV was unable to prevent a crime, people generally showed a high acceptance of this measure. We have to stress again that the acceptability referred not especially to the smart variant of CCTV, but to CCTV in general.

4.2.6 Avoidance, resistance

The number of those strongly opposed to the discussed SOSTs was lower in Hungary than in the total sample. Every tenth citizen would actively protest against them, and, in addition, 5-10 percent would support these protesters in spirit (Table 7).

The need for more information is significantly higher with regard to SLT, which is a less known technology among the citizens. They were particularly unaware of the smart functions, and this technology primarily proved difficult to fully understand for those who used traditional phones and who – although they possessed a smartphone – rarely used the smart functions, generally because they came from an older generation.

	smart CCTV (N=201)	smartphone location tracking (N=198)
	<i>Percentages</i>	
I am prepared to use any means I can to prevent its use	3	6
I am prepared to campaign actively against its use	8	6
I would support others who were protesting against its use	5	10
I would like to find out more how to protect my privacy	49	64
I do not oppose it at all	35	13
NA	-	2
Total	100	100

Table 7: Challenging the use of the technology for security purposes

Active avoidance is a relevant question only with regards to SLT (Table 8). The most common method of “avoidance” is when citizens consider whether to take their mobile with them or leave it at home specifically because of SLT. Others told how they defend themselves against SLT by frequently changing their mobile phone. Another possible method of avoidance – mentioned by the participants – was not to switch to a smart from the traditional phone, or not to use a mobile phone at all.

Changing the behaviour because of mass surveillance characterised only a few people: 5-7 percent of citizens (Table 8).

smart CCTV (N=201)		smartphone location tracking (N=198)	
Percentages			
I would never go into areas where smart CCTV is used	1	I would not use a smartphone because of SLT	6
I would avoid going into areas where smart CCTV is used	2	I would avoid using a smartphone because of SLT	15
I would change my behaviour in areas where smart CCTV is used	7	I would change how I behave because of SLT	5
I do not think I would change my behaviour because of it	40	I do not think I would change my behaviour because of SLT	36
I would definitely not change my behaviour because of it	49	I would definitely not change my behaviour because of SLT	35
NA	1	NA	3
Total	100	Total	100

Table 8: Active avoidance of the technology

Resolute opposers, avoiders and behaviour-changers often belong to those who have more prior knowledge about the discussed topics, thus, presumably are more aware of the “dark sides” of these technologies, and consequently worry about their effect on privacy more.

4.2.7 Risk-balance (Trade-off)

Participants evaluated both SOSTs along two dimensions: usefulness and intrusiveness. This, so-called “Risk-balance (Trade-off)” variable intended to weight whether respondents rely on the trade-off model, when they assess security technologies. The currently prevalent, but by this research challenged, Trade-off model assumes that the lay public understand privacy and security as interchangeable, which can be increased only at the expense of each other, thus citizens are expected to sacrifice or – using the wording of the variable – trade a part of their privacy for higher security.

Based on earlier exploratory analysis²⁶, it was revealed that the question of such kind of trade-off is relevant only if citizens perceive SOSTs both security enhancing and privacy infringing. If an individual regards an SOST as beneficial but not privacy infringing, it is not the trade-off that stands behind the acceptance. Similarly, if someone regards a security technology as ineffective but highly intrusive, it makes no sense to sacrifice even the smallest piece of privacy in order to enhance security. And finally, if a surveillance technology is regarded useless to increase security and harmless to privacy, again the trade-off frame has no relevance to describe their thinking about these topics.

The trade-off context applied to assessing SOSTs for every second participant in case of SLT and significantly less, only for one-third of citizens with regard to smart CCTV. They were those, who considered the SOST as useful in terms of security, but risky in terms of privacy. Close to 40 percent of participants regarded SLT as useful but not very intrusive, and 63 percent of participants had the same opinion about smart CCTV (see Figure 11).

The rate of those who considered these SOSTs as useless but highly intrusive was below 10 percent. Although the model defines four segments of citizens, it seems that only three are relevant in Hungary with regards to the discussed two SOSTs, because the rate of those who perceived these technologies as useless and not very intrusive is insignificant (see Figure 11).

²⁶ <http://www.prise.oeaw.ac.at/>

Smartphone location tracking (N=201)

	Useful	Useless
Highly intrusive	53%	9%
Not very intrusive	38%	1%

Smart CCTV (N=190)

	Useful	Useless
Highly intrusive	31%	5%
Not very intrusive	63%	1%

Figure: 11: Risk-benefit balance²⁷

Taking SLT and smart CCTV into account, we can observe some factors, which influence the trade-off between security and privacy:

- Sacrificing privacy is more acceptable if identity is not strongly linked to the data that is gathered about a person – SLT is directly linked, while smart CCTV is not
- Sacrificing privacy is less acceptable if the information gathered is more private (e.g. surveillance at the workplace, following every movement of citizen)
- If the surveillance can be “switched off” by the citizen, it becomes more acceptable (e.g. some younger citizens leave their smartphone at home when they go to participate in a political event)
- If surveillance is carried out in a public place (e.g. smart CCTV on the street, banks, shops, public events, etc.) it is more acceptable, as citizens feel it less intrusive, while if surveillance is made in private places (e.g. at home, in the citizen’s garden), it makes it less acceptable, thus the trade-off has less relevance.
- If citizens see obvious links between the technology and its effectiveness to enhance objective and subjective security, this makes the usage of the technology more acceptable even if it is regarded as intrusive to some extent, as in case of smart CCTV.
- Having more information about data protection and regulation would make surveillance technologies more acceptable for citizens even if they were aware that the measure might have negative effect on their privacy.

4.2.8 General attitudes towards technology to foster security

Two-thirds of citizens did not doubt that surveillance-oriented security technologies themselves are effective in a way that they are able to contribute to the improvement of the national security. However, opinions were strongly divided with regards to the appropriate deployment and use of these technologies.

Perhaps this can be a reason for the fact that a part of even those who regarded these technologies as security fostering, did not think that these technologies should be automatically used by the national governments if they were available.

The opinion that “if you have done nothing wrong, you do not have to worry about these technologies” was rather prevalent: two thirds of the participants shared this opinion (see Table 9).

²⁷ The rate of those who selected the “don’t know/don’t want to answer” was 2 percent in case of both SOSTs. They are not included in Figure 11.

	N	Strongly agree/ Agree	Neither, nor	Disagree/ Strongly disagree	NA	Total
Positive attitude variables		<i>Percentages</i>				
<i>"The use of surveillance-oriented security technologies improves national security"</i>	196	72	19	8	1	100
<i>"If surveillance-oriented security technology is available, national governments might as well make use of it"</i>	195	48	26	20	6	100
<i>"If you have done nothing wrong you do not have to worry about surveillance-oriented security technologies"</i>	196	63	18	18	1	100
Negative attitude variables						
<i>"Surveillance-oriented security technologies are only used to show that something is being done to fight crime"</i>	201	27	30	42	1	100
<i>"Once surveillance-oriented security technologies are in place they are likely to be abused"</i>	201	32	28	37	3	100

Table 9: General attitudes towards SOSTs

Cluster analysis was completed based on the five questions about general attitudes towards technology to foster security. The intention was to produce a variable, which told us who were the technology supporters and who were the detractors. However, the situation was not so simple, because in our case, the advantages (whether technology really fosters security) is often difficult to measure, and at the same time, the associated risks are indirectly present. The reason for this is that, when evaluating the risk, actually the negative effect of mass surveillance should be evaluated, which is strongly connected to the user of the technology.

Because of this, based on cluster analysis, not two but three well-defined segments of citizens took shape:

- **Doubtless supporters (38%):** who strongly believed in the security improving effect of these systems, as well as tended to trust both in the perfect operation of the system and in the users of these systems.
- **Self-convincing individualists (33%):** who were the most sceptical with regards to the use of the system, and tended to believe that SOSTs were only used to show that something was done to fight crime. However, because they felt secure from the negative effect of these systems by convincing themselves that "I have nothing to hide", they could be counted among supporters of SOSTs.
- **Mistrustful detractors (29%):** who did not trust in the authorities responsible for the operation of these systems, and were strongly against their automatic deployment and use.

4.2.9 Information privacy concerns

Individual concerns about organisational privacy practices are called "Concerns for Information Privacy" (CFIP). It was weighted along four dimensions:

- Collection: concerns because of the excessive quantity of personal data and information
- Unauthorised secondary use
- Improper access

- Errors: anxieties about accidental errors in personal data due to poor data handling, inaccurate records

The level of information privacy concerns, similarly to privacy concerns, is comparatively low in Hungary. This attitude, which can be difficult to explain, is also confirmed by other comparative international studies. According to "Special Eurobarometer 359 - Attitudes on data protection and electronic identity"²⁸, Hungary is among the countries where citizens are less concerned about privacy issues and tend to protect their privacy the least. An explanation can be that, although Hungary was a surveillance society before 1990, with the abolishment of the surveillance- and spy-based, oppressive political system, people tended towards the other extreme, and a kind of negligence and carelessness started to develop with regard to personal data and privacy. It is highly likely that lack of awareness is also a serious problem behind the relatively considerable indifference towards surveillance and towards the infringement of privacy.

The biggest information privacy concern that people are concerned about is the unauthorised secondary use of their personal data (Table 10). Actually, this is what they commonly encounter in their everyday life e.g. receiving spams, junk mails, not required advertisements.

	N	Strongly agree/ Agree	Neither, nor	Disagree/ Strongly disagree	NA	Total
Collection		Percentages				
"I am concerned that too much information is collected about me"	198	43	21	39	-	100
Unauthorised secondary use						
"I am concerned that my personal information may be shared without my permission"	196	77	11	12	1	100
Improper access						
"I am concerned that my personal information may be used against me"	197	45	28	27	-	100
Errors						
"I am concerned information held about me may be inaccurate"	192	33	23	42	3	100

Table 10: Information privacy concerns

Information privacy concerns have an effect on the acceptability of the SOSTs, however, the effect depends on the nature of the SOST we examine. For example, fear of "improper access" or "errors" influence the acceptability of smart CCTV only, while concerns with regards to "unauthorised secondary use" have an effect only on the acceptability of smartphone location tracking²⁹.

4.2.10 Proximity

Proximity of the technology has an effect on the risk perceptions associated with new technologies, and, through this, it influences the acceptability of a particular SOST. In our case, this "risk" is the privacy endangering effect of the particular SOSTs, which is slightly special compared to other technology assessment processes. Because of this, the usually weighted dimensions of proximity in technology assessment studies, the social, temporal and spatial proximity had to be adjusted to the speciality of our topic.

²⁸ http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

²⁹ Chi-square test was completed on a 0.01 significance level.

Social proximity

Increases the acceptability of the SOST, if surveillance focuses on criminals and not on common citizens. This positively affects the acceptability especially in terms of smartphone location tracking (see Figure: 12), which is a device connected directly to persons, while (smart) CCTV is connected to space, thus, even if it tends to follow only criminals, it is not possible for ordinary people to avoid it completely.

Temporal proximity

Worrying about the future development of these two technologies was the lowest in Hungary. This is a consequence of the generally lower level of privacy concerns, which is partly a cultural difference between Hungary and the other countries in the sample of the project.

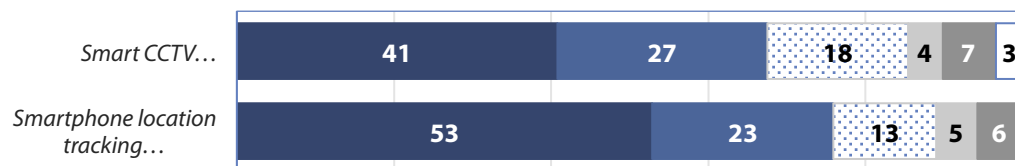
Spatial proximity

Spatial proximity refers to the individual-collective aspect of the evaluation. Hungarian culture is rather individualistic³⁰, consequently it is not surprising that there is an exceptionally high rate of those who only worry about smartphone location tracking if it hurts their own interest: every second Hungarian agreed that SLT was bothering only if their phone was tracked, while this rate was only 36 percent in the total sample of the six countries who discussed this technology.

The same cultural aspect invoked a very different result with regard to smart CCTV. This surveillance measure was not disturbing for the Hungarian citizens. They saw a lot of individual advantages in their use, and, at the same time, the associated risk of privacy infringement was perceived as low, thus video surveillance was welcomed by the Hungarian citizens especially in the areas where they live and work (see Figure 12).

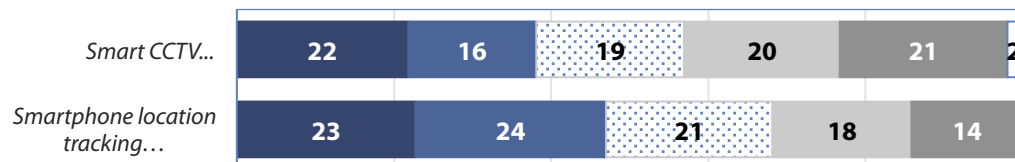
Dimension 1: Social proximity

"...does not bother me as long as it only targets criminals"



Dimension 2: Temporal proximity

"I worry about how the use of ... could develop in the future"



Dimension 3: Spatial proximity

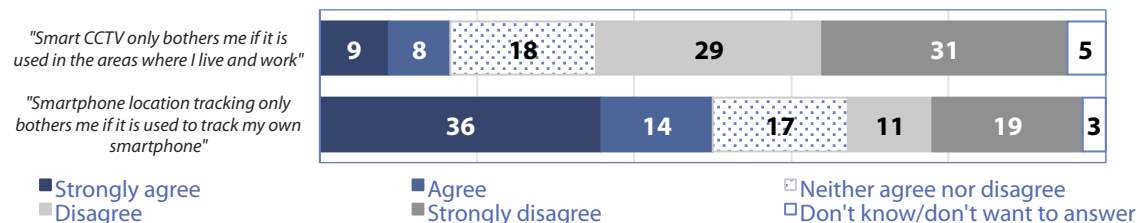


Figure: 12: Proximity (percentage)

³⁰ <http://geert-hofstede.com/hungary.html>

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

4.3.1 Institutional trustworthiness

Overall institutional trustworthiness can be seen as the result of the perceived integrity, ability and benevolence of the evaluated authorities, in our case the security agencies. “Integrity” means that the institution acts in good faith, variable “ability” stands for the perception that the institution is able to do what it sets out to do, and “benevolence” covers how much the institution is perceived to be concerned about the welfare of citizens.

Answers to the institutional trustworthiness questions did not vary significantly according to SOST. The competence of these authorities was generally respected or at least not criticized by the great majority of the citizens. At the same time, at least every third participant was concerned about that these authorities might abuse their power ((see Figure 13)

The high rate of those who selected the “neither/nor” answer possibilities may be attributable to a lack of direct knowledge about the operation of these institutions, as well as a culturally inherited fear of publicly expressing something negative about authorities.

Compared to other countries, Hungarian citizens trust in security agencies slightly more when they use (smart) CCTV, and slightly less when they use smartphone location tracking.

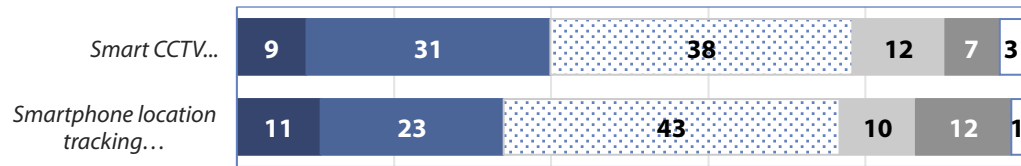
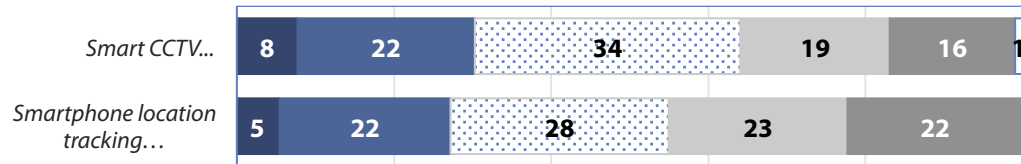
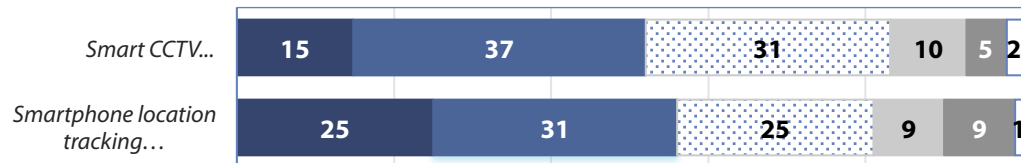
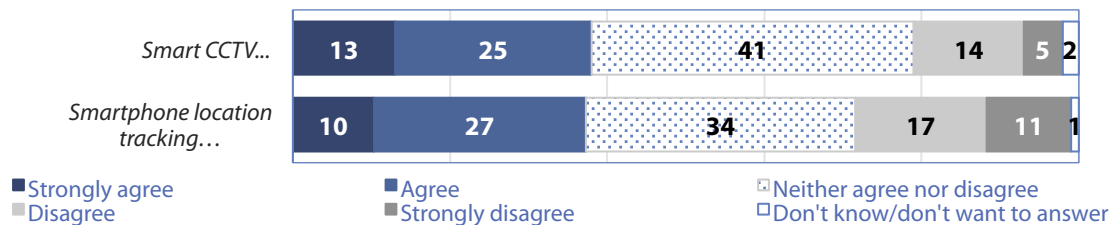
Dimension 1: Overall trustworthiness*"Security agencies which use ... are trustworthy"***Dimension 2: Integrity***"Security agencies which use ... do not abuse their power"***Dimension 3: Ability***"Security agencies which use ... are competent at what they do"***Dimension 4: Benevolence***"Security agencies which use ... are concerned about the welfare of citizens as well as national security"*

Figure: 13: Institutional trustworthiness (percentage)

4.3.2 Alternative security approaches

Two-fifths of citizens would give a higher priority to alternative approaches, which do not involve surveillance-oriented security technologies, and only a small minority, less than 10 percent, voted on the preference of the surveillance-based technological solutions. The deliberation process brought no significant change in this respect (Table 11).

		N	Strongly agree Agree	Neither, nor	Disagree/ Strongly disagree	NA	Total
		Percentages					
<i>"Alternative approaches to security, which do not involve surveillance-oriented security technologies should be given higher priority"</i>	Before the event	207	58	31	9	2	100
	After the event	194	60	31	7	2	100

Table 11: Opinions on alternative security approaches

While the support of alternative solutions was high, there were only few spontaneous suggestions for particular alternative solutions. Perhaps the "strong" opinions expressed a desire to avoid mass surveillance rather than keeping some feasible solutions in mind.

The most common alternative suggestion that emerged during table debates was the request of more police, although there were people who saw this as an unrealistic solution because of its financial implications on the government.

"There should stand a policeman on each corner, but this is unrealistic."

The question of the number of police also emerged in the context that surveillance-oriented solutions are not able to replace police. There were participants who expressed concern that these technologies might result in a decrease in the number of police.

"The use of more cameras must not result in less policemen."

Another alternative solution was raised in the context of the necessity of surveillance cameras especially in smaller communities, where people pay greater attention to each other, even when not required. This may be referred to as spontaneous neighbour watch.

"My neighbour, Mary, has a much sharper eye than the camera."

Preventive and socially more sensitive solutions were also formulated as alternative possibilities, such as:

- strengthening local communities
- crime prevention by paying more attention to raising the youth
- paying more attention to the integration of criminals into society in a way that provides them with special education as well creating possibilities to socialize

These humanistic attitudes, compared to the technocratic approach, included the wish that, instead of increasing control, society should be changed in a way that sees classical moral values such as the Ten Commandments regain meaning. The behaviour and attitudes of people should be changed if we want to live in a more secure environment and this would also have the benefit of fewer underprivileged children turning to crime.

“There is no surveillance-oriented security technology that would give us maximal security. We would be better off if we changed people’s behaviour and attitudes”

With regard to these last suggestions, we have to remark that petty crime is a major security problem in Hungary, especially in areas where unemployment is high.

The quantitative analysis supports the idea that perceptions of the advantages and risks of SOSTs have an impact on opinions of alternative solutions. Those who perceived these technologies as useful, and thus supported their increased use, tended to suggest alternative solutions less. Similarly, those who were more concerned about their effect on privacy, tended to prefer alternatives more.

When talking about alternatives, we have to keep in mind the characteristics of modern urban life, which can be characterized with alienation that can result in a decrease in social morals. At the same time, we can still observe the power of local communities in this area in smaller towns and villages.

There are two possible ways in which to fight against the negative effects of alienation on security:

- Increasing the level of control on what citizens do – SOSTs are the tools of this control. This route is based on external control and punishment.
- Maintaining social morals by strengthening local communities. This alternative raises the level of trust among people inside the society and strengthens the identity of local communities, which can lead to a decreasing level of crime, as citizens pay more attention to each other.

The second alternative is already working in some smaller cities and villages, where citizens express a less obvious need for increasing the level of control by using SOSTs – while citizens living in bigger towns or in the capital miss the strength of local communities and, in parallel, can more easily accept the increasing level of control by using SOSTs.

4.4 Citizens’ recommendations to policy makers³¹

Despite of the deliberative discussion methodology, participants predicated a less important role to citizens as being able to influence the decisions of politicians. They did not believe that they really could have an influence on politics, they saw their own role as citizens as being more reactive in this respect, and therefore tried to avoid putting any of the issues discussed into a political context.

There were differences between the groups of citizens in how easily they could find a common recommendation to policy makers. Although it was an aim to work with heterogeneous groups of citizens (age, education, place of living, etc.), groups were not the same in this respect. More homogeneous groups found it much easier to pronounce their common opinion, while groups with larger age differences or with participants living in very different areas found this much more difficult.

Most recommendations of citizens to policymakers reflected the three major problems they saw in connection with the usage of surveillance-oriented security technologies:

- Low level of trust in security authorities, regulation and control
- Lack of Information about SOSTs and about the related regulation and control
- The negative effect of surveillance on privacy

³¹ See the complete list of the recommendations formulated by the Hungarian citizens at the end of the summit, in the Appendix.

4.4.1 Recommendations with regards to regulations and control

The far most important recommendation of citizens was that it is necessary to build much more strict regulation in connection with data protection and control – this could have a favourable effect on the acceptance of surveillance-oriented security technologies in general.

It is important to control who can use the collected data (only Hungarian, or also foreign authorities?), and for what purposes (e.g. certain offices – such as the tax office –, and politicians should not be allowed to use the data; it should be forbidden to sell it for business purposes).

Citizens felt it necessary that this regulation be made, or also made internationally, on the level of the European Union.

Another important issue related to regulation is that a (politically) independent and professional organization should be delegated to control surveillance, data collection, and that human rights (mainly privacy) should not be harmed. It also emerged that civil organisations would have to undertake this role.

It would be important that regulation is not always behind the development of security technologies: the European Union should invest more in coping with this development.

4.4.2 Recommendations to enhancing information and transparency

Citizens in general reported low levels of information about surveillance-oriented security technologies. They thought that the information magazine of this project had helped them a lot, but that there was no such material available in Hungary for those who did not participate in this research.

It would be necessary to inform citizens about surveillance-oriented security technologies with regard to the following questions:

- What kinds of technologies are used in Hungary?
- How do they work?
- For what purposes are they used?
- How is the collected data protected and controlled?
- How long is the data stored for?

To preclude avoidance and resistance, it is useful to show certain cases in mass media when these technologies helped to prevent crime or find criminals.

It is also important to inform citizens about their rights in connection with surveillance, and their possibilities to protect their privacy.

Citizens were so involved in this topic, that they even made recommendations about the channels that would be suitable to use to inform different groups of citizens:

- Mass media: TV ads, short informational programmes on TV, informational brochures

“There is a need for informational programmes, where they talk about this topic in a way that’s easy to understand.”

- Teaching students in schools by, for example, policemen about surveillance, security and privacy, and citizens’ rights in this respect (“similarly to the way citizens learn traffic rules”).

4.4.3 Recommendations how to protect privacy

It is a common fear of citizens that the uses of surveillance-oriented security technologies have a strong negative effect on citizens' privacy. Thus it was an important topic among their recommendations to policymakers to help to protect the privacy of "innocent" citizens.

For this purpose, the first important step to make is to define what privacy means and establish its limits (e.g. most citizens consider their own flat and own garden to be private places, and email messages and phone call conversations are also considered private).

A general expectation from citizens was, that without the permission or information of the citizen, surveillance should not be performed: e.g. when using smart CCTV, it is important that a sign is placed in a visible place; in connection with SLT, the permission should not only be a sentence with small letters in the contract with the service provider, but more visible and understandable for citizens. Information on these topics should be given by companies to their customers when they buy a smartphone.

It was also an often-mentioned topic that citizens wanted to have the right to check the data collected about them. They imagined a webpage, where citizens could log in and check their personal data collected.

Many citizens mentioned that it would also be important to give the right to mobile phone users to switch the different ways of location tracking off. But it is important to mention that this recommendation evoked debates, because others were afraid that this would enhance security risk as criminals could switch these functions off as well.

An interesting issue here is the private usage of different surveillance-oriented security technologies: e.g. private usage of CCTV. Citizens would not forbid this, but feel it very important to develop strict rules behind this usage to prevent citizens from encroaching on each other's private lives.

4.4.4 Topics evoking debates

Although most of the final individual recommendations were rather similar at a particular table, and citizens could rather easily agree in their common recommendation, there were two topics, which evoked more debate:

- Using more CCTV in public places vs. not increasing the numbers of CCTV cameras
- Investing in the development of CCTVs' "intelligent" features vs. using more traditional (not smart) CCTV systems

4.4.4.1 Debate on the increase of video-surveillance

It was mainly those citizens who lived in large cities who felt it important to use more CCTV in public places, as this was seen as a good solution to reduce crime, and to reconstruct accidents.

"It is important to further develop these systems because there are more and more criminals, and they can only be forced back with this. Although it infringes our privacy, this is the only way to protect ourselves."

They would welcome more CCTV in dangerous districts of cities and not only in public places but also in public institutions such as hospitals, schools, etc.. They also felt it important to enhance the links between CCTV cameras and police stations³².

Other citizens were more afraid of CCTV's negative effects on privacy, and so they preferred to recommend alternative solutions³³.

³² Citizens talked a lot about experiences that the camera is there but it is not connected to a viewing room, it does not film anything.

³³ See alternative suggestions summarised in Chapter 4.3.2.

4.4.4.2 Debate on whether to invest in smart or traditional CCTVs

This argument partly stemmed from the fact that many citizens did not really understand the way smart CCTV works, and did not see the possible advantages of this over regular CCTV usage.

Some citizens believed that an algorithm (imagined like a “machine”) can never be more intelligent than a human being, while other citizens had the opinion that operators behind the screens might make bad and rather subjective decisions, and this is why the smart version should be given priority.

Another argument against the smart cameras was that it would increase unemployment, because it would replace real people.

5 Summary and Conclusions

The matter of surveillance and privacy is currently a rather marginal concern in Hungary. This fact was also evident from the comparative analysis of the empirical data, because the rather strong concerns about privacy were the most modest in Hungary among the nine countries that were included in the research. This, let us say, relatively careless attitude of Hungarians with regard to personal data and privacy is also supported by other comparative studies such as the Eurobarometer surveys.

A cultural reason for the lack of debates on privacy issues is that the democratic development in Hungary was not organic, and the mass base of social movements is missing, the civil sphere is weak. Another reason is that the issue of privacy is dwarfed by the growing economic and financial problems of the people. A further explanation can be that, although Hungary was a totalitarian surveillance society before 1990, the freedom that citizens received with the change of the regime resulted in people moving to the opposite extreme, and a kind of negligence and carelessness started to develop with regard to personal data and privacy.

It is highly likely that the lack of awareness is also a serious problem behind the relatively considerable indifference towards surveillance and towards the infringement of privacy. This fact was reinforced during the citizens' summit, where a great number of the recommendations demanded more information as well as technical education with regard to these technologies, their regulation and control in schools, and programmes targeted specifically at adults through the public media and other channels.

While privacy concerns were the lowest in Hungary, Hungarians seemed to have the largest concerns about safety. People in this country fear burglary and theft the most. The number of these kinds of crimes is continuously growing with the worsening economic situation. These fears strongly contribute to the high support of smart and traditional CCTV cameras. Negative attitudes towards video surveillance cameras came not primarily from their possible intrusive effect, but rather from their often weak performance in preventing crime. These personal or indirect negative experiences resulted in positive attitudes towards more intelligent smart cameras, which are often seen as more effective variants of this technology.

With regard to smartphone location tracking (SLT), people saw the advantages more in terms of personal security and convenience and not from the side of the national security. This technology is not seen as a tool that can prevent crime, consequently it has a much weaker effect on the perception of personal security. At the same time, citizens saw a lot of drawbacks: e.g. its unfavourable effect on the human rights, as it is suitable to use for political aims and can reveal information that is not intended to be shared like political views, sexual orientation, religion, etc.

While worries about private and public security were the highest in Hungary, Hungarians worry because of internet security the least out of the nine countries. A reason behind this fact can be that Hungary lags behind Western European countries in internet use: internet penetration is low as is the use of internet in managing everyday activities; internet shopping is also significantly behind the levels seen in Western European countries. In addition, Hungarians feel less well informed about the risk of cybercrime according to the most recent Eurobarometer on cyber security, meaning that a lack of information can be mentioned among the reasons.

An unexpected connection could be observed between the perception of security and the fear of privacy infringement. Those who felt safe in their daily life tended to worry about privacy less; in other words, those who felt generally safe, also felt safer from surveillance. This connection was even stronger in the context of online security: those who worried about security when they were online were particularly concerned about the effect of SOSTs on their privacy. People feared surveillance not just because it could possibly damage their privacy, but because they feared that data collected about them could be abused and harm could be caused to them.

These results might support the hypothesis that the trade-off model oversimplifies the situation of real life. The reason behind the feeling of insecurity might also be due to the effect of mass surveillance. If this is the case, sacrificing privacy for more security will make no sense. According to the empirical research, the trade-off context applies to assessing SOSTs for every second Hungarian citizen in case of

SLT, and significantly less, only for one third of citizens with regards to smart CCTV. There are those, who consider the SOST as useful in terms of security, but risky in terms of privacy. The others regarded the SOSTs as not useful and/or not intrusive.

Worrying about the future development of these two technologies was the lowest in Hungary. This is a consequence of the generally lower level of privacy concerns, which is partly a cultural difference between Hungary and Western European countries in the sample of the project.

Hungarian culture is rather individualistic, consequently it is not surprising to see the exceptionally high rate of those who only worry about smartphone location tracking if it hurts their own interests.

The same cultural aspect invoked a very different result with regards to smart CCTV. This surveillance measure was not disturbing for Hungarian citizens. They saw a lot of individual advantages in their use, and at the same time, the associated risk of privacy infringement was perceived as low, thus video surveillance was welcomed by Hungarian citizens especially in bigger cities, where the alienation of the people is high and the social cohesion is low.

Compared to other countries, Hungarian citizens trusted in security agencies slightly more when they use CCTV, and slightly less when they use SLT. Similarly to other countries, a great number of people were afraid that authorities using SOSTs tend to abuse their power. When citizens supported these technologies despite of significant concerns about their privacy and about that authorities abuse their power, their respect was often for the technology itself and its possible use as a national security tool. Compared to other technology assessments, in case of SOSTs, the advantages is difficult to weight on national level. At the same time, the associated risk, i.e. the negative effect of mass surveillance is connected to the measure not directly but through the user, i.e. through the political power, which – in addition – is subjected to continuous change. As a consequence, the latter is also difficult to take into consideration.

Perhaps this is the reason behind the high support of alternative, non-surveillance-based solutions despite the high acceptability of the two discussed technologies, especially (smart) CCTV. Only a very small minority, less than 10 percent of citizens would give preference to SOSTs against alternatives.

The most common alternative suggestion that emerged during table debates was the request of more police. There were participants who expressed worries that these technologies might result in the decrease of the number of police, because they felt that these solutions were not able to substitute the police.

Another alternative solution was raised in the context of surveillance cameras especially in smaller communities, where people pay attention to each other more, and this kind of spontaneous neighbour watch makes the cameras completely useless.

Preventive and socially more sensitive solutions also were formulated as alternative possibilities, such as:

- Strengthening local communities
- Crime prevention by paying more attention to raising the youth
- Paying more attention to the integration of criminals into the society in a way that provides them with special education as well as possibilities to socialize

These humanistic attitudes, compared to the technocratic approach, included the wish that instead of increasing the control, society should be changed in a way that sees classical moral values regain their meaning.

Most recommendations of citizens to policymakers reflected the three major problems they saw in connection with the usage of surveillance-oriented security technologies:

- Low level of trust in security authorities, regulation and control
- Lack of information about SOSTs and about the related regulation and control
- The negative effect of surveillance on privacy

Hungary was the only new democracy, the only country from outside Western European, the only country using a non-Indo-European language in the sample of the nine countries, i.e. this country significantly differed from the others culturally. These cultural differences are responsible for the fact that the Hungarian results are often significantly different from that of the other countries in the sample of the research. However, if we consider the recommendations and messages addressed to the local and European politicians, the demands of the Hungarian people is rather in line with that of the other countries.

6 Bibliography

Act C of 2003 on the Electronic Communication

http://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A0300100.TV&timeshift=0

Act LXIII of 1992 on the Protection of Personal Data and the Disclosure of Information of Public Interest

[http://www.haea.gov.hu/web/v2/portal.nsf/att_files/jogszabalyok/\\$File/actLXIII.pdf?OpenElement](http://www.haea.gov.hu/web/v2/portal.nsf/att_files/jogszabalyok/$File/actLXIII.pdf?OpenElement)

Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information

http://www.naih.hu/files/Privacy_Act-CXII-of-2011_EN_201310.pdf

Evaluation report on the Data Retention Directive (Directive 2006/24/EC), (2011) Report from the Commission to the Council and the European parliament

<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011DC0225:EN:HTML>

Jacobi A., Holst, M. *Interview Meetings on Security Technologies and Privacy* (2008) D5.8 Synthesis Report, PriSe Project, <http://www.priSe.oEaw.ac.at/>

Hungary's National Strategy (2012) Ministry of Foreign Affairs of Hungary

Pavone, V., Degli Esposti, S., Santiago, E. (2013) *Draft Report on Key Factors*, D2.2 of Surprise Project, <http://surprise-project.eu/>

Population Census 2011, volume 4: *Demographic data*, (2013) Budapest, Central Statistical office.

Population Census 2011, volume 7: *Educational data*, (2013), Budapest, Central Statistical office.

Report on the activity of the commissioner in 2010 (2011) Office of the Data Protection Commissioner.

Report on the activity of the National Authority for Data Protection and Freedom of Information in 2013, (2014) National Authority for Data Protection and Freedom, Budapest

Report on the situation of fundamental rights: standards and practices in Hungary (pursuant to the European Parliament resolution of 16 February 2012) (2012) Committee on Civil Liberties, Justice and Home Affairs.

Special Eurobarometer 404 - *Cyber security* (2013) European Commission.

Special Eurobarometer 390 - *Cyber security* (2012) European Commission.

Special Eurobarometer 371 - *Internal security* (2011) European Commission.

Special Eurobarometer 359 - *Attitudes on Data Protection and Electronic Identity in the European Union* (2011) European Commission.

7 List of Figures

Figure: 1: „I have gained new insight by participating in the citizen summit” (percentage, N=193).....	9
Figure: 2: „I believe the citizen summit has generated valuable knowledge for the politicians”(percentage, N=196)	9
Figure: 3: Has this experience changed your attitudes regarding security oriented surveillance technology? (percentage, N=206).....	9
Figure: 4: Before reading the SurPRISE information booklet how would you rate your knowledge of surveillance-oriented security technologies? (percentage, N=203)	11
Figure: 5: Knowledge about how the technology works (percentage).....	15
Figure: 6: The extent to which someone is getting “in touch” with the technology in daily life (percentage)	15
Figure: 7: Perceived effectiveness (percentage)	18
Figure: 8: Perceived intrusiveness (percentage)	19
Figure: 9: Substantive privacy concerns (percentage)	20
Figure: 10: Acceptability of smart CCTV and Smartphone location tracking (percentage)	21
Figure: 11: Risk-benefit balance	24
Figure: 12: Proximity (percentage).....	27
Figure: 13: Institutional trustworthiness (percentage)	29

8 List of Tables

Table 1: Socio-demographic structure of participants (percentage).....	8
Table 2: General attitudes on security.....	10
Table 3: Prior knowledge on surveillance-oriented security technologies according the gender	11
Table 4: Prior knowledge on surveillance-oriented security technologies according the age	11
Table 5: General attitudes on privacy with respects to intrusiveness of surveillance-oriented security technologies	13
Table 6: Connection between perceived private security, online security and privacy	14
Table 7: Challenging the use of the technology for security purposes	22
Table 8: Active avoidance of the technology	23
Table 9: General attitudes towards SOSTs	25
Table 10: Information privacy concerns	26
Table 11: Opinions on alternative security approaches	30

9 List of Abbreviations

Abbreviation	Definition
BKV	Budapesti Közlekedési Vállalat ("Budapest Transport Company")
CCTV	Closed circuit television
CFIP	Concerns for Information Privacy
CV	Curriculum Vitae
DPI	Deep Packet Inspection
EC	European Commission
EU	European Union
GDR	German Democratic Republic (East Germany)
HR	Human resource
NATO	North Atlantic Treaty Organization
NGO	Non Governmental Organisation
SOST	Surveillance-oriented security technology
STL	Smartphone location tracking
TEK	Terrorelhárítási Központ ("Counterterrorism Centre")

10.1 Table recommendations

Template for recommendation round

Mi a lényegi mondanivalója az asztaluk javaslatának?

Mi a javaslat háttere? // Mi a probléma?

Az Önök javaslata // Mit kellene tenni? // Hogyan lehet a problémát kezelni?

surprise

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?
CCTV cameras can be set up anywhere, but data processing must be regulated more severely	Establish an office where recommendations can be submitted.	Recorded images should be filtered
People should be informed if they are potentially exposed to surveillance cameras. The data subject must be notified about the use of their recorded information and information must be accessible for them	Surveillance activity and information processing is unknown	When purchasing devices suitable for surveillance purposes, informed consent must be obtained. Areas with security cameras should be visibly designated. Data subjects must have access to information recorded about them by surveillance technology. Notification about surveillance activity in all cases. The reasons and methods of surveillance should be made transparent. Strict legal regulation and protection of personal data or of data of personal nature.

35 Translated from Hungarian

Stricter and precise legislation, calling attention to surveillance activities (with special regard to privacy and to the public good (not in the private interest of corporations). Individual cases should be investigated by experts in the most confidential manner and use those for security purposes only and not for controlling the data subjects. The data should never be used for political purposes.	We are worried that these technological devices severely violate rights to personality, since a lot of data not wished to be shared with the public can be accessed by strangers. These technological devices are also harmful for the young as they increase alienation	There should be an independent body (representing legality) independent of political parties and consisting of experts. Stricter and precise legal regulation and compliance with them. Respecting human rights is crucial but never at the expense of legality and society. There should be a balance between security and privacy. Our recommendations should be evaluated according to humane considerations
Transparent and controllable legislation that are accessible for everyone in order to protect privacy	The violation of rights to personality due to lack of legislation	An independent social organization should control and handle data and information
If strict laws are in place, these technologies are acceptable. It is important to define who, when and for what purposes uses them and who supervises and controls surveillance	There is a potential danger of the misuse of data.	An independent judicial organization must be granted with the power of data gathering and data use. To filter dangerous threats, besides maintaining privacy, this body should regulate data gathering and data use.
Data gathered on individual persons should only be used with their informed consent.	People are entirely vulnerable to the unauthorized use and manipulation of their data-	EU recommendations can serve as a basis for member states to enact laws
To maintain our security is a top priority. These technologies should never violate human rights. The security and controllability of recorded data is important. Citizens should be informed about the use of their recorded data.	Citizens should have a better insight into the work of those who conduct surveillance. Currently they are deprived of adequate information on who can have access to these data and what they exactly do with them.	Constant monitoring is needed in order to prevent the retention of data. The controllability of the system should be solved with the assistance of a body that is independent even of the state. Legislation should keep up with the development of technology.
Legal guarantees should safeguard citizens' rights in the entire EU region.	See the questions	1. A body at an EU-level must give out licenses to set up surveillance cameras, oversee accountability, and protection of personal data. 2. A bill on criminal liability. 3. Who can buy surveillance devices and for what reasons, rules on licensing and control, 4. Launch information campaigns targeted at average citizens
More wide-scale and extensive information campaigns to be launched about CCTV cameras through different communication channels	Shortage of information on the use of these technologies most people. Lack of adequate legislation	Description of the legislations in EU languages (in shortened versions). Introduction and description of the data management process for the public

The localization ability of smart phones worry us, but we perceive a lot of advantages in the case of CCTV cameras	They make decisions without our will, our consent and without our asking	As far as smart phone users are concerned "only" informed consent can entitle "non-authorized persons" for conducting surveillance on them. The user of smart phones should be enabled to decide the applications' settings on their devices
On the condition of appropriate and non-technical, comprehensible legislation, the table accepts the raison d'être of the examined functions of CCTV cameras and of smart phone localization. Monitoring compliance with human rights, such as the freedom of assembly and fundamental human rights is particularly important	Users receive a lot of unrequested information packages, which suggests that there is an inadequate compliance with legislation or a lack of relevant regulations related to data processing	Competent authorities should take data protection seriously and comply with legislations
The access route of data should be disclosed to data subjects and neither unauthorized persons nor politicians should have access to their records	In Hungary there is no sharp boundary between politics and privacy.	Laws should be enacted, but politicians will not constrain themselves by laws anyway
Data recorded on data subjects can be disclosed to an official authority or to a person authorized by the data subjects, but only in due justification	It should not violate fundamental human rights, be more efficient and should not be used for advertisement and marketing purposes.	The people of the environment should be consulted on where surveillance cameras should be set up. The recorded images must be made accessible for data subjects if they request to view them.
We recommend the tightening of the legislation with both surveillance technologies (CCTV cameras and smart phone localization). The overwhelming of smart phone users with data packages should be restricted	Human fallibility, corruption, elimination of misuse	Monitoring compliance with the legislation. Improving the quality of recorded images or making sure that the existing cameras work properly, people and vehicles should be connected (if a criminal drives a stolen car, there is a possibility of a criminal offence). With smart phone there should be an opt-in choice for localization, data users must gain the informed consent of data subjects
The average citizen should have a say in and gain a better insight into how their personal data are being used	Lack of knowledge, ordinary citizens do not gain an adequate insight into these matters	A public online access to images recorded by the CCTV cameras. Citizens and companies must strictly adhere to relevant laws
A legislation should be in place that guarantees the security and use of citizens' data	Lack of sufficient legislation and of sufficient information	There should be a forum, where anyone can be informed about relevant legislations. To know where the recorded personal data can be accessed and looked at. More attention should be made on information campaigns (through films, flyers, TV ads)
Although CCTV cameras, programs and applications running on our smart	There is a lack of transparent review and control mechanism of	There is a need for a uniform legislation not only on a European, but on a global scale as well. Unauthorized persons should not

phones make our lives easier and enhance our security, these devices also allow for misuse of personal data by different interest groups (economic, political or criminal)	surveillance technology's data managers. A more uniform data protection legislation is required on a global level.	have access to our data. Adequate legislation within the EU is insufficient. "Information" is a problem to be handled globally. All information can be accessed anywhere on the world wide web (smart phones' GPS-based localization tracking should be disabled at users' will, and the manufacturer or the software developer should be required by law to solve that).
We fundamentally agree with and deem the application of these technologies and their use for national security necessary. But we also believe that the use of these surveillance technologies must be monitored strictly and misuse must be avoided.	We wish to live in security without any infringement on our privacy.	There should be a body that guarantees that these technologies do not infringe on civil rights. The police force should be considerably expanded - in the countryside and in smaller villages particularly. Surveillance technologies by themselves should not be regarded as a solution to the problem of public security only as a means to enhance it and the operation of authorities responsible for national security.
Personal data must be stored at the appropriate places by the appropriate authorities.	Non-authorized use of security technology, problems with public security	We recommend the prevention of crime besides the legislation on law enforcement. Children from a young age should be taught about that shift in perspective. Hungarian legislation should be harmonized with EU legislations. More money must be invested in technological development in order to recruit better experts. In the subjects discussed (smart phone, CCTV), there must be a striving for their de-politicization.
Recorded data must be used consciously and in accordance with moral principles.	Authorities have too much license	Better quality, more money, transparency, public scrutiny
Restriction and regulation of access to information and data, gathered from surveillance activities	It is not only the judicial authorities that can have access to the data	Only national security and law enforcement agencies should have access to recorded data, as provided by the laws. An agency should be set up, whose members include a judiciary expert, the President, and a data protection expert. This authority should monitor parties' compliance with the law.
When preparing the legislation, they should take into consideration as many aspects as possible	The legislation is deficient, and the whole process is hardly transparent: personal data are vulnerable from the point of data handling to data use	Information dissemination, trainings for all target groups that are concerned. There should be a preliminary investigation of the violation of rights. Monitoring. Compliance with adequate legislation.
Creating an uniform European data protection legislation and the national Data Protection Authorities must be overseen by a central supervisory	Not enough information is provided to the public about the background of data management, and the processes of data management and data	1. The creation of a uniform European data processing regulatory system. 2. The setting up of a uniform independent European supervisory authority (with sanctioning power) 3. Financing and organizing a wide-scale campaign to raise

organization. There is a need for an independent supervisory body that stands above national administrations. These powerful bodies should strive at eliminating people's concerns about data processing.	transfer are not transparent. Everybody should receive adequate information. A strengthened control is necessary of the private sector's economic and marketing data processing. Let's have a uniform European Directive!	awareness on data protection and data processing. Incorporate education on data protection and data security in school curriculum.
People should be educated and informed about mobile phone localization. As far CCTV is concerned, citizens should be informed if surveillance cameras are installed in their environment and they should know who is watching them. People must be allowed to view the recorded images.	Lack of information campaigns and messages through media on surveillance technologies. Insufficient information and communication among people.	More information distribution, the improvement of information flow, more messages for people. When subscribing to the service, the salesperson should inform the customer about the concept and about the fact of localization.
We have a positive opinion of intelligent surveillance cameras to prevent crime provided that it is regulated by appropriate legislation. In the case of smart phones, opinions are more divided. (it is the road to the future, but trigger anxieties nonetheless)	It restricts privacy but quickens and facilitates the investigation of accidents, as it transfers useful information. It can be advantageous in business (prevention of crime, marketing)	Legislation should be publicly controlled (intelligible for citizens not only existing in legal paragraphs) employees should be notified if cameras are installed in their buildings at their workplaces. There must be visible signs in order to prevent data misuse. Information transfer should be made transparent as well. A competent and authorized person of the organization with sufficient education level should install and handle the cameras.
Unauthorized persons should not be allowed to view the records. A trade-off between privacy and security should be established in a sensible manner. And a new law should be passed on that.	Technologies were not created by ordinary people's will. People wield no influence and have no leverage on their use, they are only victims of these technologies. People have no other option than to live with these technologies, but they also need to use them.	Spying on e-mails, voice messages, telephone services, text messages should be banned and that should be codified in law, so that private persons have something to refer to if they suffer a violation of their privacy. With laws in place, there must be law enforcement, but currently the professional conditions for it are lacking. Only the law enforcement authorities should be allowed to use the data and the records and only for what they were designated, and solely in due justification. Commercial use should be banned. A person should be entitled to request guarded and retained records on themselves, and check whether these data are correct. Educating the young (under the age of 18) is important and teaching about surveillance technologies in schools is important. Authorities should continue to apply and develop traditional alternative (non-technological) surveillance methods,

		which must not be neglected.
We accept the necessity of these technologies, but their use should be monitored.	There is a room for improvement regarding the accountability of the system.	Surveillance technology must remain in the hands of public bodies, and managed by highly qualified, well-selected experts. Before introducing new technologies, authorities should assess the dangers and the possibilities of privacy violations in as many social classes as possible and prepare laws in that light more prudently. There should be quick regulatory reactions to ethical problems emerging during their operation.
There is a need for better information campaigns about these new technologies.	People should be informed more extensively both about new technologies and on current technologies that are already in use.	These informational campaigns could be realized on TV, in the media, in the form of documentaries, articles, in intelligible language. It would also be advantageous if the device itself would inform the user and the service provider. Clear signs should inform citizens about CCTV operating. When purchasing devices (e.g. mobile phones) the customer must be informed about the surveillance risks of the device, and certain privacy settings should be changed immediately.
Legal provisions about the boundaries of privacy	The law on the one hand raises people's awareness about of existence of data protection and on the other hand they learn that information cannot be disclosed to third parties	People on the one hand should be "developed" and educated, and on the other they must be regularly offered the possibility to revise their privacy settings. People must be allowed to track down who stores their records and in what form. Besides that, people should be entitled to view and check their records.
EU-level regulation. Protecting the right to personality, and severe sanctions in the case of violation of rights. Regular controlling of intended use.	Technology is rudimentary, modernization is necessary.	There should be as many modern cameras as possible. Establishing an EU body (with supervisory and sanctioning power) More extensive information campaigns. More extensive data provision about the use of cell phones: users should have a say about the transfer of their data to 3 rd parties.
It's not the camera that must be intelligent but the person who handles it. To teach about the appropriate and conscious use of the devices (smart phone localization system, CCTV). Intelligent devices are not suitable for serious crime prevention. Misuse of data should be fought against, data users must be controlled and monitored.	Security technologies do not alter human nature, but can help in prevention. It is a useful tool with the prevention of smaller criminal offences, but does not help against severe criminal acts. It can be useful for investigating a crime, but it also brings about a new type of criminal offence: informational crime (data abuse, identity theft, etc.) The processing and storage of data is not safe.	Data must be stored with an appropriate level of safety, data must not be accessed from outside the system. The staff of data processing bodies must be qualified, so the recruitment process is crucial to ensure expertise. Transparency: people living in the given area must be able to view their recorded data. Establishing an independent non-state controlling agency consisting of independent experts working for the public good. Reducing the dependence on the intelligent systems. Cameras are necessary, but intelligent security cameras are not. The cameras must be set up in public places (in streets, parks) and in public institutions (e.g.: school, but NOT in

		hospitals) and ONLY with the informed consent of the parties concerned (those who live there). Cameras must not record the inside of the apartments.
We should profit from technology to enhance our security	We feel the advantages of current technological devices and hope that further development will eliminate current problems: traffic jams, supervision of the health of the elderly, CCTV – based on the example of London.	Technology should not replace human supervision. Criminals should be permanently controlled by judicial supervision.
Improve efficiency, restrict licenses.	Not sufficiently worked out. Data regulation (storage and use of data) is not transparent.	Law enforcement bodies should have access to data, but private companies should not. CCTV cameras should have a high resolution in order to have precise images.

Template

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

---

Recommendations to European Policy makers
I recommend that a higher proportion of smart cameras be used within the circle of security cameras. Cameras with low resolution, producing unrecognizable images do more harm than good. With the help of smart cameras, the travel behaviour of people could be analysed and (technical) security can be developed based on that. Legislation is necessary to regulate penalties based on the recorded images of security cameras (e.g. the hazard warning signal or the disabled parking permit is not visible)
In a rule of law, within a system of democratic checks and balances both systems can be supported besides sufficient monitoring as long as a common data protection authority within the framework of a uniform EU legal system and nongovernmental organizations monitor and sanction the member states.
People are not born criminals. These technologies cost a lot of money. More attention should be paid to the prevention of crime. More attention should be paid to the education of children so that they do not become criminals. If the ethical sense of everyone is developed, there will be no criminals. Everybody should be given the opportunity to work. Workplaces should be established instead of distributing dole money. Criminals can be rehabilitated.
Users must be provided with the option to disable the GPS-based location tracking on their smart phones.

Country report Hungary

Both the device manufacturers and the software developers must be required by law to enable users to switch off that app. Hence, location tracking based on grid information remains available only. Software developers should also be required by law to allow users to block grid information from the softwares. Users should be able to regulate that separately with each software.
Although the summit was about smartphones, cameras and the internet, a law would be necessary to assure individuals that no (harmful) content can be broadcasted about them in television or on the radio without their informed consent. E.g. reality shows, talent shows, film footages of passers by on the street, etc. An ordinary citizen does not have an insight into the operation of the media and can easily fall victim to it. I recommend a stronger legal protection for the participants in such programs.
I recommend the population, especially children and they young be prepared to the dangers of the internet and of modern technologies, and also to encourage parents to monitor their children's activities on the internet. I can say about people in general that they are not aware of the risks involved in the use of the networks, but to be honest, of their inherent possibilities either. It would be advantageous to offer them courses and trainings to make them realize these possibilities and dangers.
• They should provide a legislative background and sufficient information with regard to security cameras and smart phones.   • They should make sure that the organizations using security technologies and their operations are transparent and their accountability is guaranteed.   • Monitoring should be obligatory   • Citizens' rights to personality and the protection of privacy   • Developments   • Regulation of the use of surveillance results, elimination of biases and of risks of making mistakes
• Strict monitoring (of the use of surveillance)   • EU harmonization of the possible uses   • Prevent their use for political or business purposes
There are two important points: legislation and information. First, conditions of data gathering must be defined: who, where, when, for what purposes can record data; how long and how they can store those data; who and under what conditions can access those data. Everybody should be enabled to access their own personal data recorded by these technologies. The population must be informed about all these - in a passive form (via leaflets, TV ads, etc.) and in active forms (the citizen actively seeks the information - a separate, transparent and intelligible webpage particularly created for that purpose)
What must be done is prevention and not surveillance. Such model behaviour forms must be shown as examples that are not dangerous to society. The media play a huge role in that. That should be focused on even to the extent of censoring if necessary. People's value system must be transformed. By transforming the media, news and films on violence should be banned or at least reduced to the minimum.
• applying the principle of prevention when making a legislation   • weighted consideration of rights to personality   • presumption of innocence until the presentation of evidence
Security cameras are not always put in the right places. They are useful, but their placement must be carefully considered so that they do not make people feel uneasy, in parks for instance. People should not feel that wherever they go, they are being watched.
Discuss deep packet inspection!   More information and awareness raising programs about the use and the reliability of security technologies!   Thank you for listening to our opinions!
Deep packet inspection would have been the most interesting, as this is the most dangerous for people. It's a pity that we didn't discuss that   They must not ignore the classical criminal activities.   Intelligent cameras cannot replace normal security cameras.