



"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 2.4 – Key factors affecting public acceptance and acceptability of SOSTs

Lead Beneficiary: CSIC

Author: Vincenzo Pavone (CSIC), Sara Degli-Esposti (OU), Elvira Santiago (CSIC)

Due Date: October 2014

Submission Date: January 2015

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 orientated 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

About SurPRISE	i
Executive Summary	ii
1 The SurPRISE project: background and general aims	1
1.1 The security/privacy dilemma and the need of overcoming the limits of the trade-off approach	2
1.2 Framing the assessment.....	4
2 Security, surveillance and technology: trends and issues	6
2.1 State of the art and relevant literatures	9
2.2 Securitization.....	10
2.3 The Risk Society thesis.....	13
2.4 Surveillance studies.....	17
2.5 Security technology, neoliberalism and the competition state.....	20
3 Security, technology and democracy:	25
3.1 Introduction	25
3.2 Security, technology and democracy before 9/11	25
3.3 Security, technology and democracy after 9/11.....	28
3.4 Pre-emptive security and the trade-off between security and liberty: the EU security strategy (2003-2010).....	32
3.5 Security, technology and democracy: national developments and public debates.....	38
3.6 Implications and conclusive remarks	41
4 Drivers of technology acceptability.....	44
4.1 Introduction	44
4.2 Public assessment of science and technology	44
4.3 Acceptability of security technologies from a risk analysis perspective.....	51
4.4 Acceptability of surveillance-orientated security technologies	58
4.5 Acceptance of security technologies in Europe: insights from the national reports	69
4.6 Summary of potential factors.....	77
5 Towards a theoretical model to explain acceptability of SOSTs.....	78
5.1 Introduction	78
5.2 Understanding public acceptance and acceptability of SOSTs	78
5.3 Factors influencing public acceptability of SOSTs	81
5.4 Theoretical model with directionality of relationships	95
6 Criteria and factors determining acceptability of security technologies in Europe	98
6.1 Introduction	98
6.2 Constructs measured in the questionnaire	104
6.3 Factors influencing acceptability of SOST.....	132
6.4 Factors and criteria emerging from the analysis of qualitative data.....	142

6.5 Criteria	146
7 Conclusion	152
8 Bibliography	156
9 List of Figures	170
10 List of Tables	172
11 List of Abbreviations	173
12 Annex	174
12.1 Statistical techniques applied in testing the hypotheses	174
12.2 Tables of results	176

About SurPRISE

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

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

The work in the SurPRISE project is organised in eight¹ technical work packages. WP1 supports research activities by developing and establishing common project methodologies. WP2 develops a theoretical framing of criteria and factors influencing the acceptance and acceptability of security technologies, to be evaluated and tested in the empirical work done later in the project. WP3 identifies and elaborates options to shape security measures to comply with ethical and privacy requirements from a technical, legal and social perspective. WP4 combines the output of WP2 and WP3. It translates them into a testable empirical model, applied in large-scale participatory activities. WP4 develops the overall structure of the questionnaire and the supporting information material. WP5 organises and conducts large-scale participatory technology assessment events in nine European countries. These "Citizen Summits" involved on average about 200 citizens per country. Citizen summits are full day events with alternating phases of receiving information, discussing emerging issues in small groups, electronic voting on general aspects of the relation between surveillance and security and on specific surveillance technologies, and of developing recommendations from the citizens to policymakers. WP6 analyses the qualitative and quantitative data in depth and synthesises them to conclusions and recommendations, combining expert knowledge and citizens perspectives. WP7 applies the results and methods of the citizen summits to develop a decision support system, allowing the involvement of citizens in decision-making on security technologies and measures in small-scale participatory events. WP8 is devoted to dissemination to ensure information flows from the project to relevant bodies, interest groups, decision makers and the general public.

This report elaborates the theoretical model of criteria and factors and summarises the results from testing it on basis of the data gathered at the participatory events conducted in nine European countries within work package 5.

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

Executive Summary

SurPRISE aims at empirically investigating criteria and factors likely to affect public acceptance and acceptability of Surveillance-Orientated Security Technologies (SOSTs). A central premise that drives SurPRISE is the idea that framing the relationship between privacy and security in terms of a trade-off is not only one among several potential interpretative frames, but also that, empirically speaking, it may not be the most common way used by European citizens to assess security measures. To investigate the issue, SurPRISE adopts an innovative methodology inspired by the citizen summit participatory method. The SurPRISE citizen summit method is a technology assessment exercise that gathers both qualitative and quantitative data on the base of a rigorous research design. The method ensures that citizens not only have a chance to express preferences among a set of predetermined options (an electronic questionnaire), they also have an opportunity to voice their own views, ideas, knowledge and proposals during table discussion rounds. SurPRISE provides two types of outcome: (1) a deep scientific understanding of the rationale behind rejection or acceptance of SOSTs; and (2) guidelines for security experts, providers, policy makers and regulators to increase the appropriateness and effectiveness of security measures embedded in complex social realities.

The present report, entitled “Key factors and criteria affecting public acceptance and acceptability of Surveillance-Orientated Security Technologies (SOSTs)”, makes a contribution to the achievement of SurPRISE overall project objectives by offering a detailed recognition of those parameters likely to affect the way in which security measures are assessed by lay people. By gathering insights from relevant studies in the security and technology assessment fields, this report outlines how contextual elements, such as perceived trustworthiness of institutions and operators managing SOSTs, specific features of the technology under study, such as the level of perceived intrusiveness or effectiveness of a given SOST, as well as personal concerns, such as privacy concerns, and individual opinions about the necessity of relying on technological solutions to solve security problems, may affect the probability of considering a given security measure acceptable by citizens.

The report is structured into seven chapters. The **Introductory Chapter** explains what role this deliverable plays in achieving overall project aims, as previously stated. A brief summary of the remaining six chapters is here provided.

Chapter Two presents the security debate through different theoretical lenses, from securitization approaches to surveillance studies. Security is a highly contested concept whose definitions change in scope and depth as we write. While during the 1990s the focus was on *human* security, which emphasised the role of an integrated, global system of international intervention to complement the effort of so called “failed states” in securing their citizens, since 2001 the war on terrorism has encouraged a re-evaluation of *homeland* security in tackling new global threats. In spite of changing emphasis and definitions, security has become a policy priority for both the EU and the national states belonging to it. The rapid expansion of the conceptual scope and relevance of security issues, principles and values, need to be explored in order to understand the proliferation of surveillance-orientated devices meant to address security problems. By calling for a new approach to security strategy, EU documents, like the European Security Strategy, bear witness to a changing understanding of security agenda and strategy in the Union, which is no longer meant to be based on balance of power rationality but on the active management of largely unknown and unpredictable risks, which are global in nature but geographically dispersed and temporally undetermined.

The emphasis on risk management and prevention has changed the way security issues and priorities have been conceived. Security threats have been increasingly framed in such a way that (a) technology makes always sense as a solution, and (b) surveillance is the only and inevitable way to increase security levels. The expansion of security into new policy domains and the progressive inclusion of several social and political issues under its policy agenda are also provoking a gradual erosion of the boundaries between public and private domains. Within this context, the introduction of new technologies to foster

security is increasingly perceived as a socially problematic and scientifically uncertain option. As a result, public participation in technology assessment exercises represents a way forward and it is introduced as part of a new endeavour that tries to use both scientific and non-scientific knowledge as reliable bases for decision-making. The final outcome is a pragmatically oriented policy-making strategy that introduces new technologies to enhance security while engaging citizens in technology assessment exercises to foster public dialogue and democratic accountability. As a result of this process, over the past 20 years and especially after 9/11, security has become a) broadly inclusive, b) largely reliant on surveillance technologies, c) situated on blurred boundaries between public and private domains, d) pro-active and pre-emptive and e) often associated with recurrent technology assessment exercises aiming at exploring public opinions. Each of these salient features of the changing nature of security has been addressed by different sociological and political science academic literatures.

Securitization theories, for instance, address the gradual expansion of security agendas in Europe and all over the globe, focusing on the social construction of security and on the implications of securitizing social, economic and political subjects into the political debate. This perspective is especially helpful not only to understand how is securitization performed and under which conditions it succeeds, but also to better understand how this is accomplished through EU security policies and what the implications for our society and democracies are. *The Risk Society thesis*, on the other hand, outlines and discusses how security has changed, both in conceptual and in practical terms. It casts light on the dynamics that have shifted security from “means-ends” rationality towards a risk management and risk assessment approach and it also provides interesting conceptual tools to account for the gradual transformation of security into a pre-emptive and pro-active endeavour, which no longer aims at protecting and responding to threats, but actively look for potential threats and operate beforehand to deactivate the sources of menaces. *Surveillance Studies* squarely address the growing reliance on surveillance technologies, which are likely to constitute a serious threat not only for our privacy; however the latter is understood, but also, and perhaps mainly, for our residual chances to enjoy our civil and political rights. These studies are extremely useful to understand the variety of forms and modalities under which surveillance practices may operate, the variety of technologies that have been employed and with what implications. Surveillance studies, finally, shed light on the relationship between modern liberal societies and surveillance practices, showing the intrinsic nature of this relationship but also its potential intended and unintended consequences. The blurring boundaries between public and private, military and civil security have been originally addressed by *Science and Technology Studies* and by a critical stream of economic geographers, who have recently explored the relationship between neoliberalism, the knowledge society and the so-called competition state.

Despite the different approaches, these streams of literature seem to converge on one main issue: the steady and progressive entanglement of security and surveillance technologies. Though looking at different types of implications and consequences, they address the controversial and complex relation between this progressive entanglement of security and technology and the ways in which democracy and liberty are being affected. In other words, the key issue at stake seems to be how come that security is increasingly associated with the implementation of new surveillance technologies and what the main implications of this phenomenon for our democracy and our liberty are.

The Third Chapter, therefore, analyses in more details the relationship between security, privacy and surveillance from a policy perspective, with a special emphasis on the trajectory of the European security policy and on the rise and implications of the trade-off between liberty/privacy and security. Security is a term that nowadays seems to be ubiquitous. A brief search on almost any policy document of the European Union contains at least one or two reference to security. The contemporary ubiquity of the term security should not, however, mislead. The term was widely used well before the end of the Cold War or the terrorist attack to the Twin Towers. For a long time, though, it was a term mostly associated with theories of international relations usually underpinned by realist perspectives emphasizing national integrity and sovereignty. During the Cold War, due to the relatively stable international context and blocks, these theories looked exhaustive and comprehensive enough to account for both relevant international political changes and foreign policy developments. With the collapse of the Berlin Wall, however, the debate about the meaning and implications of security was gradually dominated by a new, emerging definition of security: the “human security”: The concept was

initially formulated as an extension of the human development approach that had been, in the meanwhile, elaborated by the United Nations Development Programme (UNDP). 'Human security' was explicitly concerned with the security of persons as opposed to the security of states. It also openly affirmed that state security could be legitimate only if it was based on, and consistent with, the security of individuals.

During the 1980s and the 1990s, the relationship between security and technology, and its implications for democracy and liberty, not only had not been theorized; it had remained almost completely undetected. In the multiple scenarios emerged during the 1990s, new threats materialized as a result of the combination between objective factors, such as the trans-national nature of new agents and phenomena, and subjective factors, which relate to the social construction of certain events as risky and the changing public understanding of security. For instance, the NATO Strategic Concept suggested that security strategy should focus on the active management of risks, while the EU security strategy called for a new security approach based on threat and conflict prevention. Both US and EU security strategies acknowledge the global and unpredictable nature of security threats but seek to control and dominate risks through preventive actions which rely heavily on the implementation of new technological devices, from biometrics to IT technologies.

Upon these premises, with a view of taking action against the demise of the military-industrial complex, and of effectively addressing what were the considered new types of threats and challenges defying the traditional distinction between internal and external security, the EU began to develop a new security strategy. This new focus found a better and more articulated expression in the Group of Personalities final report, entitled *"Research for a Secure Europe"*, published in 2004 as well as in its first security strategy document, the 2003 *"A secure Europe in a better world"*. In these documents security is considered impossible without technology. Obviously, military technology had always been an important component of national security, and even during the debates on human security, technological tools and instruments had never disappeared.

Yet, never before had technology been conceived as a conceptually central component of security. These documents also affirmed that security constituted a shared platform where of civil and defence strategies converged to become one security strategy, not only because the type of security threats no longer respected national borders or predefined settings, but also because civil, security and defence applications increasingly draw on the same technological basis. Moreover, in these documents, two main concepts make their way in the first pages: the indissoluble link between internal and external security and the relationship between global integration, increased dependence and, thus, increasing vulnerability. In this context, security becomes a precondition for development: if infrastructures, energy, information and transportation are increasingly interconnected, this interconnection increases their vulnerability and increasing vulnerability jeopardizes development.

The 2011 document on internal security strategy constitutes the final stage of a trajectory characterised by five main trends. First of all, an expansion of security threats and domains, which implies a further advance in the process of securitization of policy domains that, traditionally, fell under the competence of ordinary political, democratic debates. Second, these domains, re-framed with urgency and exceptionality, get subjected to a new approach that emphasizes threat anticipation. In this context, risk-assessment and risk management emerge as the dominant approaches to security analysis. Third, from the perspective of threat anticipation and risk-assessment, the monitoring and surveillance of people's movements, actions, communications and transactions become a crucial component of security responses, which, in turn, makes surveillance technologies a necessary tool of such security responses. Expansion of the security agenda, the securitization of several societal domains, threat anticipation and pre-emptive action, massive use of SOSTs and risk-orientated analysis and responses emerge, therefore, as key elements of the new European security model formulated in the European internal security strategy. The combination of these trends makes the trade-off between liberty and security almost inescapable.

This is, in a way, a security paradox that lies at the heart of the new concept of security and is further aggravated by the new emphasis on risk assessment and risk management. The attempt to prevent a security threat from materializing needs the deployment of a powerful and ever expanding intelligence service being able to gather massive amount of information in order to assess the risk and manage its possible manifestation. In this perspective, all citizens can be subjected to surveillance and be assigned

a security label on the basis of the level of risk they pose to the system. Needless to say, these tasks cannot be performed, at least in the terms in which they have been conceived, without the massive deployment of surveillance-orientated security technologies. A higher emphasis on surveillance technology often implies a lower emphasis on the social and economic determinants of crime and restricts focus only on those aspects of security that can actually be addressed by a technology. Thanks to surveillance studies, we are today aware of social sorting, ethnic discrimination and self-censorship practices usually associated with SOSTs.

As a result, citizens are increasingly asked to renounce to part of their liberty and civil rights in exchange for an increased level of security. Security, the national and European security strategy documents suggest, is a precondition for development, or for democracy. Without security, as they say, democracy would simply not be possible. However, as the EU chart of rights acknowledges, security and liberty are both essential elements of our liberal democracy. Citizens cannot be free unless they are safe. However, they cannot be safe unless they are free, or they would no longer be citizens. SurPRISE aims, thus, at a new endeavour: the elaboration of a new theoretical model where the criteria and factors influencing public acceptability of new security measures – be they surveillance orientated or not, technology based or not – do not necessarily proceed from a frame where security and liberty stand at odd with each other. It also aims at something more: the elaboration of new engagement process where citizens are not asked how much liberty are they willing to trade in exchange for more security, an engagement process where they have a chance to set the rules and the boundaries, without having to choose from a path of predefined options.

Bearing in mind these debates, and drawing insights from technology assessment studies rooted in the Public Engagement with Science tradition as well as in Risk Analysis studies, Chapter Four offers an overview of all those factors and criteria that are most likely to influence public acceptance and acceptability of surveillance-orientated security technologies (SOSTs). On the basis of their own societal and experiential knowledge, citizens have often come to question the need, the appropriateness and the actual impact of prospective or recently implemented technologies. The end of that unconditional support to science and technology, which characterised the years of reconstruction after World War II, led an increasing number of scholars to criticise the linear model of innovation, which considered that citizens accept technological breakthrough under the premise that this would bring prosperity and wealth. Addressing public perception and assessment of science and technologies, theorists have, thus, adopted a different perspective. From the deficit model, which attributes opposition toward technology to a lack of scientific knowledge; through contextual approaches, in which different socio cultural variables must be taken into account to understand acceptance or rejection of technology; to the most recent public-engagement-in-science proposals, which emphasise the need to involve citizens in the decision-making process as a way to democratise science and increase acceptance of technological developments.

Whilst earlier studies, inspired by the so-called ‘deficit model’, used the level of scientific knowledge (or the lack of knowledge) as independent variable and considered the level of support for science and technology as the dependent variable, contextual approaches have focused on more institutional and contextual variables, such as trust in public institutions or scientists, or technology operators. Considering that citizens and lay public possess societal and experiential knowledge that is potentially very relevant to assess the risks and benefits of new technologies, more recent approaches have instead tried to involve citizens and civil society organisations in participatory technology assessment exercises, such as citizens summits and consensus conferences, in order to promote Public Engagement with Science (PES).

Radical approaches within PES have proposed to address public participation in, and public engagement with, science under a radically different light. In fact, they aim at asking new questions about the relationship between science, politics and society. The reasons and the ways in which certain issues, and not others, have become objects of public policy; how and as a result of whose action has this happened; and what kind of society are we trying to achieve through current innovation directions and priorities emerge as key questions that deserve attention well before single technologies can be assessed. As long technology assessment keeps focusing on the reaction, and/or opinion, of the wider

public in risk assessment exercises associated with the development and introduction of new technologies, these questions will remain unaddressed.

In conclusion, the complexity and uncertainty surrounding the development and implementation of new technologies affects public attitudes towards them and, clearly, the deficit model is not sufficient to explain public acceptability or rejection of these technologies. New approaches have been, thus, developed, which have emphasized the importance of socio cultural factors, like trust, and the need to take into account lay knowledge as a relevant type of knowledge. The experience of citizens in the decisions process about the directions of science and technology is necessary to guarantee socially robust and publically shared development of new technologies.

In general, these studies have highlighted the importance of risks and benefits analysis and on the impact of risk perception on the way citizens assess technologies. Another important stream research community has therefore looked at risk perception in close details. The concept of 'risk' has gained significance in public and academic debates in particular after WWII. It was mainly linked to the development of new technologies, such as nuclear energy applications. Nowadays the concept of risk is relevant to many scientific disciplines, but despite its current development and growing interest, the social sciences have not been able to establish a coherent theory that can structure this field of work and interconnect the multiple research results of risk problems. In this section, we are going to review three conceptions of the acceptability of technology from a risk perspective, taking into account the three frames existing in the literature.

First, the technical approach insists on the possibility of obtaining a scientific and objective measure of the risks related to each technology. A second, psychological approach focuses on the individuals and includes subjective and contextual factors in the acceptability of risk, using a psychometric test. According to this approach, it would be possible to talk about objective risk only when sufficient data exist for a solid statistical calculus of probability. As this is rarely the case, in the absence of such data, only the subjective estimation of risks made by experts or by the lay people could really be considered. As a result, the psychological approach reduces the distinction between objective and subjective risk to the differences between two sources of subjective risk, ones from the experts and ones from lay people. A third approach, therefore, takes distance from the technological or psychological approaches, and focuses on the importance of social structures and cultural behaviours, among which trust in institutions is a central point.

As we restrict our focus on Surveillance-Orientated Security Technologies, the issue of privacy becomes fundamental and needs to be addressed in this context. Privacy, which is sometimes referring to the safeguard of a person's intimate spatial or social space, represents a complex idea that has been investigated and discussed from many different perspectives and over many years without finding any conclusive answer. Privacy can be conceived (1) as a moral value, if seen from an ethical perspective; (2) as a commodity, if seen from an economic perspective; and, (3) as a psychological state when interpreted from a psychological or socio-psychological stand.

Socio-psychological approaches underline the necessity in social life for moments of withdraw from social interaction or concealment of intimate matters from public gaze, which is necessary to safeguard one's own emotional and mental integrity. Thus, privacy seems to work as a mechanism that allows people to set boundaries between themselves, other people and the overall society. These boundaries are necessary for people to establish, nurture and protect their identity and their valuable relations with what and whom they consider important in their life. Moreover, they represent a protection against misuse of information and power abuses. This idea of privacy, however, is being challenged by the introduction of new ICT technologies. The digital and the physical world are so increasingly intertwined to challenge the appropriateness and validity of old and well established ideas, such as the distinction between what we deemed private or public. For this reason we need a model of privacy able to reconcile the digital and the physical world, to follow people in semi-public spaces, and to face the challenges posed by advanced tracking technologies. We propose to work with a concept of privacy characterised by only four dimensions, as Westin suggests. We consider adopting Westin's terminology while extending the scope of each category to include not just psychological states but real life situations, informed by current technological innovations.

We start from defining *general privacy* as the state of being free from unauthorised intrusion and observation and we distinguish between physical and information privacy. While by *information privacy*

we mean individual control over personal information, according to mainstream literature, we define *physical privacy* as the safeguard of an individual's space, which can refer equally to an individual's body, geographical location, or social environment. These dimensions are also identified in the deliverable D3.2.² We use the same terminology used by Westin, but extend and change the definition of each category to take into account not just psychological states, but also sociological aspects like the relationship between the individual and the physical, relational space.

As a consequence, physical privacy is partitioned into three dimensions: *intimacy* of the body and close personal relationships; geographical and spatial *solitude*; and *anonymity* of behaviour and association. *Intimacy* refers to the integrity of the human body, conceived as encounter of biological tissues and emotional states. It not only reflects the sacredness of the physical self, but also the need of respecting the most intimate relationships, like the ones between lovers, family members or close friends. *Solitude* concerns the right to move freely in the physical space, either to stay isolated and escape, or to go to places we like, without having to worry about being tracked or monitored. *Anonymity* represents a way of protecting individual behaviour from collective pressure and expectations. The possibility of detaching one's identity from behaviour, or to lose one's identity to be part of a crowd, helps people develop themselves through positive and negative experiences.

With regards to the communicative space and the freedom of producing and sharing information about oneself, the dimension called by Westin *reserve* will map all those concerns related to information privacy. Reserve, in fact, is about being in control of one's expressive power through any form of communicative media. Four additional sub-dimensions help us map this concept, these are: concerns related to massive data gathering; concerns related to unauthorised secondary use and access to the information; presence of inaccurate and erroneous data.

Chapter Five articulates the distinction between acceptance and acceptability, factors and criteria and explains each factor in further detail by presenting findings of previous empirical studies assessing public perception of SOSTs. The chapter ends with the elaboration of a general theoretical model envisioning how factors and criteria may influence public acceptability of SOSTs. We say that a technology is acceptable when it is capable or worthy of being accepted, which means that it is received favourably or with approval, and also capable of being endured, because it is tolerable, adequate, and conforms to approved standards. In policy documents and in the academic literature, the construct most widely preferred is *public acceptance*. It is important, though, to clarify the distinction between 'acceptance' and 'acceptability'. First of all, there is often a discrepancy between behaviours and attitudes. People's behaviour is often influenced by a number of different factors which constrain citizens. As a result, it is more instructive to address their attitudes, which reveal what they actually think and would do if they could freely choose. Whilst 'acceptance' mainly addresses people's behaviour, people attitudes are better captured by the concept of 'acceptability'. Given that SOSTs are usually imposed by public authorities on the citizens without the latter having really any choice on whether to adopt them or not, we consider more accurate to focus on *acceptability*, rather than on *acceptance*, within the context of this study. We also consider more accurate to use *acceptability*, because we are more interested in investigating those factors and criteria that make SOSTs acceptable, rather than describing what percentage of the population find SOSTs acceptable.

It is also important to distinguish between factors and criteria. While a *factor* is *one of the elements contributing to a particular result or situation*, a *criterion* is *a standard on which a judgment or decision may be based*. Within the context of this study, criteria are those arguments consciously used by citizens to explain their position vis-à-vis the acceptability of SOSTs. In contrast, factors represent those elements that influence people's opinions, but that people do not explicitly state or that they recognise only partially. Factors may be addressed by means of quantitative methods, while criteria can be better assessed qualitatively through table discussions and focus groups.

Having clarified these distinctions, it is now possible to build upon the revision of the literature previously carried out, and to identify those variables that are more likely to influence public

² Porcedda, M.G., M. Vermeulen et al. (2013). Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy. Deliverable 3.2, SurPRISE Project. Florence, European University Institute.

acceptability of SOSTs. Three groups of variables emerge, which proceed from social studies of science and technology, the risk perspective, and privacy and security studies, respectively. These variables are: 'Familiarity with SOSTs' and 'General attitude towards SOSTs: Technology Detractors vs. Supporters', coming from the Science and Technology studies literature; 'Perceived Intrusiveness and Perceived Effectiveness', 'Temporal, Spatial and Social Proximity', 'Perceived Level of Security Threat', and the variable 'security-privacy balance, from the Risk perspective; 'Institutional Trustworthiness', from both the contextual approaches in public engagement with science and the socio-cultural perspective in Risk studies; 'Substantive Privacy Concern (which refers to both physical and information privacy)' inferred from privacy studies. The theoretical model at the end of chapter summarises the relationships among these variables.

Finally, Chapter 6 provides a detailed overview of the results, highlighting and discussing the factors and criteria that, according to both quantitative and qualitative analysis, appear to influence acceptability of SOSTs. Confirming most of the results proceeding from the contextual approaches to public engagement in science as well as the socio-cultural approach to risk analysis, Institutional Trustworthiness is a key factor determining the acceptability of SOSTs, and it shows that, besides what citizens may think, or know, about security technologies, the degree of trust that security agencies and political institutions enjoy is a crucial element that citizens do take into account when assessing the acceptability of security technologies. Interestingly, the perceived level of threat has a limited effect on the acceptability of SOSTs, whilst Social Proximity has a strong impact on it, confirming that security technologies that operate blanket surveillance are considered significantly less acceptable than security technologies carefully focusing on specific targets. Both effectiveness and intrusiveness emerge as highly relevant factors in explaining the level of acceptability of SOSTs. Moreover, whilst much of the security technology discourses insists that security technologies need to be intrusive to be effective, citizens argue that the more a technology is considered intrusive, the less it might be considered to be effective.

This result questions the general idea that SOSTs need to be intrusive to be effective, and, consequently, radically questions the trade-off approach. Moreover, our analysis shows that the security-privacy balance, a factor inspired by the trade-off approach, does not generally influence acceptability, except in the case of DPI. Finally, we found out that age is positively correlated with acceptability; a result that radically questions the general belief that the digital natives generation, due to their familiarity with ICTs and SOSTs, would be less concerned with privacy issues. Some of the most interesting results of this study proceed also from the qualitative analysis and suggest that factors like the type of crime targeted, the risk of function creep, the clarity and transparency of the operational functions of SOSTs, the contribution of the human factor and the public-private partnership emerge as very relevant when citizens assess the acceptability of SOSTs. Finally, citizens suggested that acceptable technologies should primarily address the types of crime they consider a priority, such as crime streets and political corruption and financial crimes. Last but not least, our study has identified a list of criteria suggesting that acceptable technologies are those that a) operate under an international legislative framework, monitored by a data protection authority with sufficient powers at the European level; b) are operated by transparent, accountable public agencies that inform citizens about their purposes and functions; c) are cost-effective and allow citizens to access and control the data they retrieve and store; d) always target the least sensitive data, only in public spaces, whenever possible and be specifically orientated towards suspects and criminal activities; e) are deployed only after significant evidences have been collected and only after judicial authorities grant permission f) incorporate Privacy-by-Design mechanisms and principles and g) do not replace but complement human intervention, as part of a broader, socially informed, security strategy that addresses also the social and economic causes of crime and violence. These last findings are summarised in the following table (Tab.1).

SOSTs are more acceptable if:

...operating within a European regulatory framework and under the control of a European regulatory body.

...operating in a context where transparency about the procedures, information about both data protection rights and principles and about the purposes and the scopes of security actions as well as accountability of security operators is ensured at all times.

...operated only by public authorities and only for public benefits. The participation of private actors in security operations, such as when security agencies acquire banking data or Facebook data or when security functions are outsourced to private operators, therefore, must be strictly regulated.

...their benefits largely outweigh their costs, especially in comparison to other non-technological, less intrusive, alternatives.

...their operation can be regulated through an opt-in approach. Whenever this is not possible, their operation need to be communicated to targeted individuals.

...they allow monitored individuals to access, modify and delete data about themselves.

...they target less sensitive data and spaces, whenever possible, according to criteria and purposes known to the public.

...they not operate blanket surveillance. After reasonable evidences are gathered, they address specific targets, in specific times and spaces and for specific purposes. Whilst their purposes may change, these changes need to be explicitly discussed and publicly approved.

...they work and operate in combination with non-technological measures and social strategies addressing the social and economic causes of insecurity. SOSTs are not alternatives but complementary to human resources and social policies.

...they incorporate privacy-by-design protocols and mechanisms.

Table 1. Criteria for the development of more acceptable surveillance-orientated security technologies.

1 The SurPRISE project: background and general aims

SurPRISE examines factors and criteria taken into account by citizens in assessing surveillance-orientated security technologies (SOSTs). SurPRISE aims at empirically investigating the impact of technological, individual, institutional, social and contextual factors on citizens' assessment of Surveillance Orientated Security Technologies (SOSTs). More specifically, the SurPRISE project focuses on the criteria and factors likely to affect public acceptance and acceptability of surveillance-orientated security technologies. This deliverable, therefore, will not focus on key factors that may be affecting public acceptance and acceptability of all sorts of technologies that may infringe on privacy or allegedly enhance our security. There exist security technologies that are not surveillance orientated, such as fire alarms or motion sensitive lights, and there exist surveillance technologies that are not necessarily orientated towards security, which is how basically operate all social networks. Social media like Facebook collect huge amount of personal data, which are normally used for business and marketing purposes. They do constitute an instance of surveillance, but their primary task is not to gather information for security purposes, although it is nonetheless possible to use these data in these terms. The key issue, for SurPRISE to engage in detailed investigation, thus, is that the selected technologies need to be surveillance-orientated and explicitly implemented for security purposes at the same time.

A central premise that drives SurPRISE is the idea that framing the relationship between privacy and security in terms of a trade-off is not only one among several potential interpretative frames, but also that, empirically speaking, it may not be the most common way of approaching the security issue among European citizens. Nevertheless, policy debates about security in the EU and member states concerning the acceptability of the effects of security on civil liberties, particularly privacy, have been framed in terms of a mutually exclusive relationship between security and liberty. The outcomes of the project, thus, also need to contribute to develop a decision-support approach that may enable end users throughout Europe to assess the degree of acceptability of new SOSTs in a more sophisticated and complex way, which goes beyond that of a simple trade-off between privacy and security.

The security-liberty trade-off is problematic for at least three reasons. First, liberty and security are presented as abstract categories, instead of enacted social practices emerging from the interaction between people and their social and institutional context.³ Second, the debate on security and liberty is framed as a zero-sum game, in which the trade-off acts as a rhetorical device to reduce public opposition to a mere problem of making the necessary sacrifice for the sake of national security.⁴ Third, studies adopting the trade-off approach are empirically narrow, because they require citizens to assess the introduction of new security technologies using a predetermined conceptual approach, which frames security and privacy as interchangeable goods right from the start.⁵

SURPRISE has the potential to challenge common understanding of privacy and security issues. In order to achieve this, SurPRISE is developing an innovative research design, which features a combination of citizen consultations, multimedia information material and a questionnaire. Through this research design, SurPRISE will explore whether citizens consider the acceptability of given security solutions in terms of a trade-off between their security and their privacy, or whether they prefer to rely on different interpretative frameworks. Crucially, SurPRISE will identify and explore the alternative factors that citizens take into consideration when performing an assessment of SOSTs.

³ Dourish, P. and Anderson, K. (2006) "Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena," *Human-Computer Interaction* 21(3): 319–42.

⁴ Monahan, T. ed. (2006) *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York: Routledge. Tsoukala, A. (2006) "Democracy in the Light of Security: British and French Political Discourses on Domestic Counter-terrorism Policies," *Political Studies* 54(3): 607–27.

⁵ Pavone, V. and Degli Esposti, S. (2012). "Public assessment of new surveillance-orientated security technologies: Beyond the trade-off between privacy and security " *Public Understanding of Science* 21(July): 556-572.

Citizens will be engaged in the assessment process in quality of experts of their everyday realities: citizens will add their own societal and experiential knowledge to integrate the technical knowledge traditionally employed by policy-makers and experts when assessing security technologies. In SurPRISE, citizens will also be provided the technical expertise, experience and information about future scenarios needed to ensure neutrality and completeness of vision at the time of evaluating the consequences of SOSTs.

SurPRISE adopts an innovative, original methodology, which is reflected in its research design and data gathering procedures. It is a technology assessment exercise that uses qualitative and quantitative methods to ensure that citizens not only have a chance to express preferences among a set of predetermined options, they also have an opportunity to voice their own views, ideas, knowledge and proposals. It is not an issue of asking citizens questions in order to understand to what extent they know what it is already believed to be solid knowledge, but rather to ask questions in order to solicit a societal knowledge that experts and scientists do not know, do not possess and can't even imagine at this stage. Only in this way it may become possible to get from citizens ideas and arguments that make experts, scientists and policy-makers think differently as formulate new questions. SurPRISE does not only aims at soliciting answers and responses that may be at odds with current beliefs and predominant perspectives, it also aims at providing a space for citizens to be able to reshape the debate in order not only to provide different answers to already pre-determined questions, but also to be able to ask different questions.

For instance, instead of asking how we can prevent violence from striking, it may be more suggestive to ask why and how violence is generated. Instead of focusing merely on how can citizens be protected, it may also be useful to ask how can citizens and institutions cooperate and engage together to protect their society. Instead of restricting European research to the development of new technologies to stop crime, new research directions may explore new combination of social and technical innovation processes that may make the upsurge of violence less likely.

European countries are striving to find a way to elaborate security policies that can simultaneously strengthen security and protect civil liberties and individual privacy. In order to do so, it is clearly not sufficient to search for different answers to long-standing questions; it is rather crucial to be able to ask novel questions. SurPRISE considers this latter endeavour as one of its main goals.

1.1 The security/privacy dilemma and the need of overcoming the limits of the trade-off approach

Over the past ten years, in the face of global terrorism, nuclear proliferation, and transnational organized crime, new approaches to safeguard national and personal security have emerged.⁶ As a result of the spatial and temporal unpredictability of criminal actions and of their global repercussions, a safer society is often pursued through the implementation of security policies that increasingly rely on the deployment of SOSTs⁷ and interconnected data exchange systems in order to transform unknown threats into predictable events.⁸ However, while any real improvement of security is yet to be demonstrated,⁹ several SOSTs are subjecting ordinary citizens to such a level of monitoring and control¹⁰ that some authors speak of a *surveillance society*¹¹. Addressing the potential implications of this

⁶ Rasmussen, M.V. (2006) *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century*. Cambridge: Cambridge University Press

⁷ Pavone, V. and Degli Esposti, S. (2012) *op.cit.*

⁸ Zureik, E. and Salter, M.B. (2005) *Global Surveillance and Policy: Borders, Security, Identity*. Cullompton: Willan Publishing.

⁹ Webb, M. (2007) *Illusions of Security: Global Surveillance and Democracy in the Post-9/11 World*. San Francisco, CA: City Lights Books.

¹⁰ Monahan, T. ed. (2006) *op. cit.*

¹¹ Surveillance Studies Network (2006) "Report on Surveillance society, 2006", available at Surveillance Studies Network (2006), Report on Surveillance society, 2006 available at: www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_public

paradox a variety perceptions and opinions studies have been realized in Europe to understand to what extent and under what conditions, European citizens are willing to trade part of their privacy/liberty in exchange for increased security.¹²

Like the security policy approaches from which they stem, most of these perception and opinion studies, with few relevant exceptions (e.g. PRISE) have also been inspired by a trade-off approach and, thus, tend to take it for granted.¹³ In these studies, privacy is generally defined as the right of the individual to have one's personal information protected from the undue prying eyes of government and private organizations seeking to use such personal information either for security purposes or for trade and profit, without the consent of the individual, apart from where exceptional circumstances dictated by the law apply.¹⁴ The definition of security, however, is more controversial and it might refer to the right and duty of national governments to protect their geopolitical and economic integrity or to the right and duty of national governments to ensure citizens' personal safety.¹⁵ According to these studies, new SOSTs not only force governments to make a clear distinction between those liberties that can be sacrificed to security needs and those that cannot be included in the trade-off, they also encourage citizens to trade part of their privacy in exchange for enhanced security.

On the one hand, the trade-off has been used to justify a growing series of surveillance orientated, privacy infringing security technologies and practices. On the other hand, people tend to approach new technologies along a trade-off model only when they consider these technologies as risky and useful at the same time,¹⁶ which, applied to SOSTs, means that only those who consider new SOSTs as both privacy infringing and security enhancing do face a trade-off. Alternative approaches, therefore, do exist and are strongly influenced by demographic, institutional and cultural factors, which implies that the acceptance of SOSTs is context-dependent.¹⁷ For instance, if trust in institutions depends on the type of technology in use, trust in technology also depends on citizens' confidence in the institutions using the technology¹⁸. As a consequence, from a more socially embedded perspective, several authors have pointed out how the emphasis of the trade-off approach purposively obscures a number of ethical, social and political implications increasingly associated with the introduction of new SOSTs¹⁹.

In fact, current studies generally focus on first order social, ethical and political implications, which refer to the implications *directly* associated with a given technology, such as, in the case of biometric information, for instance, the risk that, once in the database, not only do the data no longer belong entirely to the physical holders, but they can also be stolen, commercialized or used for political purposes. Given the actual flow of data among EU countries and the lack of a common juridical protection, biometric technologies constitute a serious challenge to current norms of democratic accountability.²⁰

_discussion_document_06.pdf. See also Lodge, J. (2005) "e-Justice, Security and Biometrics: The EU's Proximity Paradox," *European Journal of Crime, Criminal Law and Criminal Justice* 13(4): 533–64.

¹² Strickland, L.S. and Hunt, L.E. (2005) "Technology, Security, and Individual Privacy: New Tools, New Threats, and the New Public Perceptions," *Journal of the American Society for Information Science and Technology* 56(3): 221–34.

¹³ Riley, T.B. (2007) "Security vs. Privacy: A Comparative Analysis of Canada, the United Kingdom, and the United States," *Journal of Business and Public Policy* 1(2): 1–21.

¹⁴ Ibid. p. 2.

¹⁵ Amoore, L. (2006) "Biometric Borders: Governing Mobilities in the War on Terror," *Political Geography* 25(3): 336–51. Manners, I. (2006) "Normative Power Europe Reconsidered: Beyond the Crossroads," *Journal of European Public Policy* 13(2): 182–99.

¹⁶ Gaskell, G., Allum, N., Wagner, W., Kronberger, N., Torgersen, H., Hampel, J. and Bardes, J. (2004) "GM Foods and the Misperception of Risk Perception," *Risk Analysis* 24(1): 185–94.

¹⁷ Davis, D.W. and Silver, B.D. (2004) "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America," *American Journal of Political Science* 48(1): 28–46.

¹⁸ Knights, D., Noble, F., Vurdubakis, T. and Willmott, H. (2001) "Chasing Shadows: Control, Virtuality and the Production of Trust," *Organization Studies* 22(2): 311–36.

¹⁹ Muller, B.J. (2008) "Securing the Political Imagination: Popular Culture, the Security Dispositif and the Biometric State," *Security Dialogue* 39(2–3): 199–220.

²⁰ Lodge, J. (2007) "Freedom, Security and Justice: The Thin End of the Wedge for Biometrics?" *Annali Istituto Superiore Sanità* 43(1): 20–6.

New security policies based on SOSTs, however, also have important *second order* social, ethical and political implications, which relate to the implications of *framing* a given security problem in such a way that a given technology emerges as an appropriate solution. This is, for instance, the case of security technologies employed at national borders. By framing security hazards as a function of given ethnic, social and religious characteristics, security policies based on new SOSTs are endorsing a discriminating process of risk profiling, a procedure through which all monitored citizens are encoded with a risk profile, turning people into low risk “trusted travellers” or high risk suspicious immigrants.²¹

To address second order socio-ethical implications, which refer to the wider social and political changes encouraged by the introduction of new sociotechnical practices, studies aimed at understanding public assessment of technologies need to incorporate frame analysis. Frames, in the social sciences, are “principles of selection, emphasis and presentation composed of little tacit theories about what exists, what happens, and what matters”²². Frame analysis provides a better understanding of the frames used to make sense of a given problem and it helps identifying not only the mechanisms through which problems that have social, economic or political causes are addressed in terms of given technological “solutions” but also potential or existing alternative frames that may take into account these social, ethical and political aspects in a more effective way.

Public assessment of privacy and security issues associated with the introduction of new SOSTs not only is more complex than the trade-off assumes, it is also largely affected by a variety of factors, which relate to how these technologies address social priorities and to the social and institutional context of implementation. In general, a hypothesis can be that a higher trust in public institutions makes it more likely for security to become a priority, reducing concern over privacy implications, while a low level of trust makes it more likely for privacy to become a priority, encouraging citizens to raise doubts about the way in which security as an issue is constructed, and question its appropriateness. The trade-off approach might obscure the fact that a deeper line of demarcation could exist, running along the dilemma between two broad political attitudes, trust and concern, of which the divide between privacy and security may only be a by-product.

For instance, in any given society, where sceptical and critical attitudes prevail there might actually be a short circuit of trust, that cannot be effectively addressed simply by improving the amount of information people receive through institutional communications. The adoption of a trusting attitude may also have negative effects because, while it indicates a high level of trust towards the institutional context of implementation of SOSTs, it may encourage security actors to underestimate that technologies not only provide solutions, they also create new problems.

Therefore, security technologies need to be assessed not only on the basis of technical effectiveness, but also on the basis of how, when, where, and by whom these technologies are going to be implemented. As a consequence, it becomes necessary to explore not only citizens’ opinions towards technology and institutions, but also the actual social, economic and political context in which these technologies, and possible alternatives, are likely to be implemented.

1.2 Framing the assessment

Combining frame analysis and context analysis, within a European-wide technology assessment exercise, the SurPRISE project may not only constitute a crucial step forward to cast light on whether citizens do actually employ a trade-off approach to assess the introduction of new security technologies, but it may also provide a much-needed understanding of the main factors behind over-acceptance and over-rejection of SOSTs. In a context of rising security concerns, expanding definitions of risk and growing governmental monitoring activities, this project may yield important results to shed some light on the persisting gap between the governmental and the lay public perceptions of the security agenda, as well as on the political implications of the new public discourse on security. In this respect, SurPRISE will provide support to the development of a decision support system providing insights into the *pros* and *cons* of specific security measures compared to a set of alternatives taking into

²¹ Côté-Boucher, K. (2008) “The Diffuse Border: Intelligence-Sharing, Control and Confinement along Canada’s Smart Border,” *Surveillance and Society* 5(2): 142–65.

²² Jasanoff, S. (2003) “Technology of humility: citizen participation in governing science,” *Minerva* 41:223–24.

account a wider societal context. SurPRISE will include and discuss wider societal alternatives going beyond traditional approaches to meet security threats by addressing root causes of insecurity and emerging security threats. In doing so, the interplay between human and technological aspects related to the implementation of a particular security measure will be taken into consideration.

In line with this objective, this Deliverable has a special interest to study the way in which the problem-solution framework is (a) constructed by the citizens and (b) affected by the implementation of security policies based on the introduction of new surveillance orientated security technology. After having selected a number of key pairs of security challenges together with their sociotechnical measures, across different domains of security policy within the European Union, as part of Deliverables 2.1 and 2.3, this Deliverable identifies those social, cultural and political factors that are likely to affect, or are perceived as likely to affect, citizens' acceptance and acceptability of surveillance-orientated security measures.

This Deliverable also aims at identifying potential implications of SOSTs and to incorporate the societal dimension into the technology assessment exercises by means of frame and context analyses. Frames, in the social sciences, are 'principles of selection, emphasis and presentation composed of little tacit theories about what exists, what happens, and what matters. Framing is active at all times and is a function of our desire to control and master events that look complex at first sight. Frames help the analysts to order their experiences of reality into patterns of causes and effects so that a given problem can be understood and addressed. As a consequence, frame analysis should constitute a fundamental tool of policy studies and policy making because a better understanding of the frames used to make sense of a given problem is essential to evaluate the solution suggested to solve that problem. It can, for example, help to identify when the proposed solution suffers from a "technological fix", through which problems that have social, economic or political causes are framed and addressed in terms of a technological "solution". Such a solution claims to address unwanted effects but leaves untouched their non-technical origins.

D2.4 tries to gather, outline and discuss factors and criteria are likely to affect public acceptance and acceptability of SOSTs. To achieve these goals, D2.4 gathers insights about how (a) individual characteristics (e.g. citizenship status, ethnicity, income, age, education, etc.), (b) elements of the institutional context, (c) social and cultural factors, and (d) the specific features of the technology under study (novelty, intrusiveness, safeness, etc.), affect the probability of considering a security measure as either risky and useless, which provokes a rejection of the technology, or harmless and useful, which engenders an unproblematic interpretation of the technology.

D2.4 aims also at identifying and analysing the social and political frames (such as the widely adopted trade-off model between privacy and security) that are normally used to frame the relationship between security privacy and surveillance, in those policy and regulatory documents, as well as academic literature, that presents, promotes and encourages the selected key pairs of security challenges and related sociotechnical measures.

The present deliverable, thus, is meant to substantially contribute to the development of a theoretical framework to guide the empirical analysis of those factors most likely to influence acceptance and acceptability of SOSTs. The set of conceptual tools developed here will also contribute to a critical assessment of both EU and national security policy responses, taking into account national and cross-national differences and reflecting different cultural and social backgrounds.

Finally, on the basis of this initial exploratory and conceptual work, it also aims at elaborating a new model of the relations between surveillance, security and privacy, that may be better equipped to study, through the testing of clearly identified set of dependent and independent variables, the social, cultural and political factors affecting public acceptance and acceptability of existing and emerging SOSTs and compare them with their technological and non-technological alternatives. As a result, this Deliverable, together with D3.1, D3.2, D3.3 and D3.4, constitutes the theoretical foundations of SurPRISE.

2 Security, surveillance and technology: trends and issues

*Security is 'the condition of being protected from or not exposed to danger; [...] a feeling of safety or freedom from or absence of danger'.*²³

*"Technology itself cannot guarantee security, but security without the support of technology is impossible. [...] In other words: technology is a key 'force enabler' for a more secure Europe".*²⁴

*"Striking the right balance between security and freedom will be a permanent challenge while respecting the highest ethical principles".*²⁵

As it is clear from the above introduction, our project faces a number of different issues that are nonetheless deeply intertwined. First of all, SurPRISE is a response to a great expansion of security measures, technologies and policies, both in terms of security research and in terms of security technologies. Security is highly contested concept whose definitions change in scope and depth as we write. While this issue is discussed in details in the next chapter, here it is important to anticipate that, while during the 1990s security had increasingly focused on *human* security, emphasizing the role of an integrated, global system of international intervention to complement the effort of so called "failed states" in securing their citizens, the war on terrorism seems to have encouraged an explicit re-evaluation of *homeland* security into the new global context²⁶. In spite of changing emphasis and definitions, security has become a policy priority for both the EU and the national states belonging to it. The EU has, for instance, elaborated several policy documents on security strategy, ranging from the European Security Strategy in 2003, to the most recent Internal Security Strategy in 2011. Meanwhile, security has also become a focus of European R&D strategy, as first the Preparatory Action on Security Research and then the current FP7 on Security Research demonstrate.

The rapid rise of security as a political and economic topic and as a policy priority in the EU is a relatively recent phenomenon, which in its current form, began at the end of the 1990s, with the widespread debate on how to reconfigure the defence industry and strategy. Until then, in general, defence research and policy strategy were considered as essentially belonging to the military domain. As a result of the end of the Cold War, during the 1990s a rapid reconversion of military industry and research to security technologies and solutions for civil purposes was first envisioned and then properly developed²⁷. Partially in response to a decline of military needs and military industry perspectives, partially in response to the on-going development of multipurpose technologies that could also be deployed in border control and internal crime control, such as CCTV or biometrics, a new perspective emerged.

According to this new approach, on the one hand, it was time to take advantage of the potentialities of emerging technologies for matters of internal security and for the fight against organized crime, on the other hand, it also made sense to give impulse and support the rising industry of security technologies, which was partially proceeding from reconversion of military industry and partially proceeding from the gradual convergence of ICTs towards surveillance purposes and functions. Effectively, in a very short time span, a solid, blooming market was set and put in motion. Private companies, public authorities, academia and business interests were effectively mobilized towards the development, implementation and diffusion of new security technologies.

²³ European Commission "A Secure Europe in a Better World: European Security Strategy", Brussels, 12th December 2003, available at: <http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf>

²⁴ Burkard Schmitt et al. (2004) "Research for a Secure Europe " Luxembourg: Office for Official Publications of the European Communities p. 12.

²⁵ Ibid. p.11.

²⁶ Duffield, M. and Waddell, N. (2006) "Securing Humans in a Dangerous World" *International Politics* 43(1): 1-23.

²⁷ Hayes, B., Rowlands, M. and Buxton, N. (2009) *Neoonopticon: The EU security-industrial complex*. Transnational Institute.

Traditional macroeconomic arguments were then used, such as the usual lagging-behind-the-US argument that is often present in European Policy documents dealing with the emergence and development of new promising markets and technologies.²⁸ However, it was not just an issue of market construction, for the expansion of the security industry, the consolidation of a security technology market and the rise of security concerns and issues among the top priorities of the EU and national agendas, are also due to a changing understanding of security. In other words, these policy and industry changes were influenced by, and influenced in turn, a gradual expansion of the list of social and political items that could be considered as, and approached by, a security perspective. To put it differently, social and political issues, such as documented and undocumented migration, social deviance and micro-criminality, financial crimes and illegal economic activities, became progressively framed and approached as an issue of security. As a consequence, principles, priorities, values and arguments normally used in security discourses became applied to an increasingly wider range of social and political phenomena.

The rise of security in the policy agenda, both in economic and political terms, accompanied by the rapid expansion of the conceptual scope and relevance of security issues, principles and values are two intertwined phenomena, which are of great relevance to the research concerns of SurPRISE, which specifically aims at studying the criteria and factors affecting public assessment of surveillance-orientated security technologies. Yet they are certainly not the only ones. Both phenomena have wider social and political implications that also need to be placed under the analytical gaze of SurPRISE. The rise and expansion of security concerns and discourses has been accomplished in specific ways that are loaded with serious social and political implications.

First of all, the rise and expansion of security discourses and practices has been often accomplished through the development and implementation of surveillance technologies, which have been, in turn, accompanied by the relevant legal and political changes, often curbing civil liberties and infringing basic human rights and individual privacy. In what is now common conceptual framework in Science and Technology Studies (STS), this mutually constitutive process, where technology and social order co-construct each other, is known as *coproduction*.²⁹ Co-production, though, should not be merely understood in the sense that science and society influence each other. This is certainly true, but co-production implies something more than that, for it suggests that science and social order are *co-produced*, in the sense that they jointly come to life and evolve through the constant making of new identities, institutions, discourses and representations.³⁰

Second, the overwhelming emphasis on surveillance and technology has changed the way security issues and priorities have been conceived. Security threats have been increasingly framed in such a way that (a) technology makes always sense as a solution and (b) surveillance is the only and inevitable way to increase security levels (whether in real terms or merely through the increase of the feeling of being secure is yet another issue). Security policies, in other words, have increasingly adopted a conceptual approach to security problems that is strongly solution-driven and tends to neglect the variety and complexity of social, economic, technical and political factors that may have caused the emergence of those security problems in the first place. In this situation, technological progress is *per se* one of the main driving forces behind the 'technologization' of security policies and strategies. Many of these technologies, as a matter of fact, are ready-made solutions in search of problems, which in turn get framed and approached in terms that make these technologies effectively look like the long sought solutions³¹.

Third, the expansion of security and the progressive inclusion of several social and political phenomena under its policy agenda are also provoking a gradual erosion of the boundaries between public and private domains. Not only are military technologies and approaches being applied to civil domains and

²⁸ European Commission (2004): "Research for a secure Europe: Report of the Group of Personalities in the Field of Security Research," Luxembourg Office for Official Publication of the European Communities

²⁹ Jasanoff, S. (2005) *Designs on nature: Science and Democracy in Europe and the United States*. Princeton, NJ: Princeton University Press.

³⁰ Jasanoff, S. (2004) *States of Knowledge: The Co-Production of Science and the Social Order*. London: Routledge.

³¹ Zureik, E. and Hindle, K. (2004) "Governance, Security and Technology: The Case of Biometrics," *Studies in Political Economy* 73(Spring/Summer): 113–38.

practices, but also private companies and public institutions more and more often cooperate, exchange data, run and operate the same technologies and it is increasingly difficult for a citizen to identify the boundaries between these two domains. The SWIFT case is one example: private companies, i.e. the banks operating the SWIFT technological system, made available their customers' data to public authorities.³² Sometimes the opposite may occur, which is that personal data retrieved by public authorities are then entrusted and analysed by private companies, as it was the case in Canada with Accenture.³³ The overlap between private and public is also due to the gradual shift of security from the exclusive domain of the Ministry of Defence and Foreign and Commonwealth Office to the actual situation where responsibility and action in security are shared with the Ministry of Home Affairs. It is not by chance that the EU has recently elaborated an Internal Security Strategy at the Union level (2011), while, until very recently, internal security was considered to be the exclusive responsibility of the individual nation states. In a Report on Security Research commissioned by the EU to a Group of Personalities is stated: *'Facing these changes and (security) challenges, there is both a need and an opportunity for the EU to develop a comprehensive approach that links the external and internal dimensions of security and can combine the use of civil and military means'*³⁴

Fourth, calling for a new approach to security strategy, EU documents such as the European Security Strategy³⁵ also bear witness to a changing understanding of security agenda and strategy in the Union, which is no longer meant to be based on balance of power rationality but on the active management of largely unknown and unpredictable risks, geographically dispersed, temporally undetermined and global in nature. More specifically, the new security agenda is switching from the pursuit of well-defined ends to the *management of risks* that are perceived as multifaceted and multi-directional and therefore hard to assess and predict:

*'We live in a world that holds brighter prospects but also greater threats than we have known. The future will depend partly on our actions. We need both to think globally and to act locally [...]. In an era of globalization, distant threats may be as much a concern as those that are near at hand [...]. The first line of defence will be often abroad. Conflict prevention and threat prevention cannot start too early.'*³⁶

While future scenarios constitute the new basis for the construction of risks, economic, environmental and social crises are now constructed as matters of security³⁷. These recent changes have, in turn, encouraged two main trends: (a) the introduction of legal provisions restrictive of civic rights and freedom and (b) the adoption of anticipatory intervention and precautionary measures. As we have seen, in both cases, the concrete proposals elaborated by Western states have consistently relied on the development and implementation of new security technologies.

Fifth, in accordance with the cognitive revolution that Beck defines as reflexive modernity,³⁸ the security solutions provided by the introduction of new technology are increasingly perceived as socially problematic and scientifically uncertain. In turn, public participation in technology assessment is introduced as part of a new endeavour that tries to use both scientific and non-scientific knowledge as reliable bases for decision-making. In fact, the rapid progress in the development of communication technologies, biometrics, sensor technologies and data storage and analysis capabilities are perceived as causing constant pressure on the fundamental right to privacy for both economic and security reasons. The final outcome is a pragmatically orientated policy-making that introduces new

³² De Goede, M. (2012) "The SWIFT affair and the global politics of European security" *JCMS: Journal of Common Market Studies*.

³³ Maki, K. (2011) "Neoliberal Deviants and Surveillance: Welfare Recipients under the watchful eye of Ontario Works," *Surveillance & Society* 9(1/2): 47-63.

³⁴ European Commission (2004) *op. cit.*

³⁵ European Commission (2003) *op. cit.*

³⁶ *Ibid.* p. 6

³⁷ Rasmussen, M.V. (2001) *op. cit.*

³⁸ Beck, U. (1992) *Risk Society: Towards a New Modernity*. London: Sage. Beck, U. and Lau, C. (2005) "Second Modernity as a research agenda: theoretical and empirical explorations in the meta-change of modern society," *British Journal of Sociology* 56(4): 525-557.

technologies to enhance security while engaging in technology assessment exercises with a view to enhancing public trust and dialogue and strengthen democratic accountability.

There is a question related to what extent was this process inevitable. To what extent security needed to be expanded to address an increased range of social and political phenomena? Was it necessary to enhance security mainly through the introduction of new technological devices? To what extent was it necessary to develop security technologies aiming at surveillance? The security of whom are these new policies and technologies enhancing? Although this is how the security trajectory has mainly evolved so far, with resistance, alternatives and setbacks, this report consider these issues as open questions and tries to problematize the dominant narrative, trying to show not only its contingent and negotiated nature, but also the existence, resistance and often failure of alternative narratives.

Before moving to empirical stage, where SurPRISE will explore the social, political, ethical and economic factors that influence citizens' acceptance and acceptability of security solutions, there is a need to understand how and why several technology assessment exercises and current policy documents predominantly frame the relationship between security and privacy in terms of a trade-off. When the privacy infringement produced by surveillance orientated security technologies is presented as a necessary consequence of their capability of enhancing security, the conceptual process that made security expand and evolve as a function of new technologies, which are predominantly surveillance orientated, is completely black-boxed, taken for granted and removed from the critical gaze.

So far, we have identified five main trends related to the evolution of and changes in the concept and practices of security. Over the past 15 years, and especially after 9/11, security has become (a) broadly inclusive, (b) largely reliant on surveillance technologies, (c) situated on blurred boundaries between public and private domains, (d) pro-active and pre-emptive and (e) usually associated with recurrent technology assessment exercises aiming at exploring public consensus and opinions. Each of these salient features of the changing concept and practices of security has been specifically addressed by different sociological and politological academic literatures. These academic studies have raised interesting issues and debates and need to be at least briefly revised before we can move on into an empirical discourse analysis of the key security policy texts of the EU (Chapter 3), and into an informed review of the main contributions so far delivered by the empirical studies on the public assessment of security technologies (Chapter 4).

The expansion and broadening of the scope and influence of security discourses, values and principles has been extensively theorized and discussed by the Copenhagen School with the *securitization thesis*. The gradual shift from power rationality to risk management and pre-emptive, proactive security has been discussed by a relatively small group of international relations scholars, who find inspiration in a set of theoretical concepts elaborated since 1992 by Ulrich Beck and followers, known as the *risk society thesis*. The blurring boundaries between public and private, military and civil security has not been the exclusive topic of any specific literature, but could be usefully addressed through, on the one side, the conceptual tools provided Sheila Jasanoff's theory of co-production, and, on the other side, by a critical stream of economic geographers³⁹, who have recently explored the relationship between neoliberalism, the knowledge society and the so-called competition state.

For this reason, in the next section, we will provide a reconstruction and problematization of the conceptual (and empirical) process that not only made security become broadly inclusive and reliant on surveillance technologies but also gave rise to the dominant approach that frames security and privacy/liberty into a trade-off.

2.1 State of the art and relevant literatures

In this section, we review four main streams of literature dealing with security and surveillance from different perspectives. By presenting securitization theories and the theses of the Copenhagen School, we will try to address the gradual expansion of security agendas in Europe and all over the globe,

³⁹ Peck, J. and Tickell, A. (2002) "Neoliberalizing Space," *Antipode* 34(3). Benner, M., and Löfgren, H. (2007) "The Bio-economy and the Competition State: Transcending the Dichotomy between Coordinated and Liberal Market Economies" *New Political Science* 29(1): 77-95.

focusing on the social construction of security and on the implications of securitizing social, economic and political subjects into the political debate. This perspective will demonstrate to be especially helpful not only to understand how securitization is performed and under which conditions it succeeds, but also to better understand how this is accomplished through EU security policies and what the implications for our society and democracies are.

The risk society thesis, on the other hand, will help us to grasp how security has changed, both in conceptual and in practical terms. It will cast light on the dynamics that have shifted security from “means-ends” rationality towards a risk management and risk assessment approach. It will also provide interesting conceptual tools to account for the gradual transformation of security into a pre-emptive and pro-active endeavour, which no longer aims at protecting and responding to threats, but actively look for potential threats and operates beforehand to deactivate the sources of menaces. The risk society thesis will also help us to consider the broader social and political implications of this shift, with the background of reflexive modernity.

Surveillance studies will demonstrate to be highly relevant, too. One of the major changes in security theories, policies and practices is the growing reliance on surveillance technologies, which are likely to constitute a serious threat not only for our privacy, however this is understood, but also, and perhaps mainly, for our residual chances to enjoy our civil and political rights. These studies are extremely useful to understand the variety of forms and modalities under which surveillance practices may operate, the variety of technologies that have been employed and with what implications. Surveillance studies, finally, will shed light on the relationship between modern liberal societies and surveillance practices, showing the intrinsic nature of this relationship but also its potential intended and unintended consequences.

The impact of surveillance-orientated security technologies on citizens’ privacy and civil rights has also been the ground upon which more and more public consultations searching for acceptability criteria have been organized. An increasing number of studies focusing on SOSTs⁴⁰ have been carried out within the vast stream of research known as Science, Technology and Society (STS) studies, especially within Public Understanding of Science or, in its more reflexive evolution, Public Engagement with Science.⁴¹ This literature, which goes back more than 30 years now, can help us to understand and get familiar with a variety of social, cultural, economic and political factors that have been considered likely to influence public opinion on scientific practices and technologies. A number of very different technologies, from nuclear energy⁴² to synthetic biology, have been studied from an STS perspective.⁴³ Some of these studies have focused on security technologies, too.⁴⁴ However, given the specific relevance of this literature vis-à-vis the selection of the factors more likely to affect public acceptance and acceptability of SOSTs, it will be dealt with in details in the next chapter.

All these streams of literature contribute—each in its own way and from its own angle—to cast light on the evolution of security technologies and policies over the last 20 years. In this chapter we briefly present their main works, arguments and contributions, as a propaedeutic introduction to the discussions unfolding in following chapters.

2.2 Securitization

The extension and growing scope of security agendas over the past decades is a phenomenon that has not remained unperceived by international relations analysts. In the field of security studies, some

⁴⁰ See Chapter 4.

⁴¹ Felt, U. and Wynne, B. (2007) *Taking European knowledge society seriously*. Luxembourg: DG for Research

⁴² Wynne, B. (1992) "Misunderstood misunderstanding: social identities and public uptake of science," *Public Understanding of Science* 1(3): 281-304.

⁴³ Kronberger, N., Holtz, P. and Wolfgang Wagner, W. (2012) "Consequences of media information uptake and deliberation: focus groups, symbolic coping with synthetic biology," *Public Understanding of Science* 21(2):174-87.

⁴⁴ Bowyer, K.W. (2004) "Face Recognition Technology: Security versus Privacy," *IEEE Technology and Society Magazine* 23(1): 9–19. Strickland Lee S. and Hunt, L. E. (2005,) *op.ci.*; Pavone, V. and Degli Esposti. S. (2012), *op. cit.*

scholars, such as Ole Waever, Barry Buzan and Jaap de Wilde⁴⁵, have tried to capture and analyse this phenomenon, elaborating a conceptual framework that tries to address the social construction of security. In their work, securitization emerges a conceptual framework that tries to show how new topics, areas and phenomena get framed and addressed in security terms, and what the conditions are that have to be met for this process to occur. In their own terms, this process can be defined as *securitization*.⁴⁶ Since their first contributions in the mid-1990s, securitization theory has come to a position of great relevance in the field of security studies. In international relations, it has been, perhaps, the most influential theory challenging, on constructivist grounds, the traditional realist and neorealist schools. It is also a distinctively European theoretical contribution to international relations theory in general and security studies in particular.

It has been developed by what is now considered the Copenhagen School, and is largely seen as synthesis of constructivist and classical political realism in its approach to international security⁴⁷. In contrast to materialist approaches of classical security studies, securitization is a process-orientated conception of security. In other words, while classical approaches of security focus on the material dispositions of the threat including distribution of power, military capabilities, and polarity, securitization examines how an actor transforms a certain issue into a matter of security. Securitization theory, thus, is empirically concerned with the shifting agendas of security and theoretically with the social construction of security.

According to securitization theory, any actor can transform any issue in a matter of security through what they define 'speech acts'. In other words, through the effective and coordinated deployment of a series of speech acts, several issues can be reconstructed as matters of security. This process can be applied to an almost unlimited variety of subjects, some of them well beyond the military security of the territorial state.

Yet, what does securitize mean? And how is this accomplished? To securitize an issue, the theory suggests, is to consider a given subject at risk from an essential threat, which allegedly puts its existence at stake. When the very survival of this subject is constructed as in grave danger, the security clause is applied, suspending the ordinary rules of political and democratic confrontation and invoking the urgent application of extraordinary and dramatic actions. Securitization, therefore, is a deeply political act, which suspends ordinary democratic debates and warranties and translates the management of a subject onto a different political plane, that of urgency and survival. Any issue can be securitized if it can be intensified to the point where it is presented and accepted as at risk from an existential threat⁴⁸.

If a subject is successfully securitized, then it is possible to legitimize extraordinary means to solve a perceived problem. This could include declaring a state of emergency or martial law, mobilizing the military or attacking another country. Furthermore, if something is successfully labelled as a security problem, then the subject can be considered to be an illegitimate subject for political or academic debate. I quote: 'By labelling it as security an agent claims a need for and a right to treat it by extraordinary means'⁴⁹. Securitization, thus, marks a decision, a breaking free of rules and the suspension of normal politics.

Securitization is a radical version of politicization that enables the use of extraordinary means in the name of security. For the securitizing act to be successful, it must be accepted by the audience, therefore securitization studies aim to understand who securitizes (securitizing actor), on what issues (threats), for whom (referent object), why, with what results, and not least, under what conditions. Basic components of a securitization speech act, thus, are: (a) a securitizing actor/agent: an entity that makes the securitizing move/statement, (b) a referent object: the object that is being threatened and needs to be protected and (c) an audience: the target of the securitization act that needs to be persuaded and

⁴⁵ Buzan, B., Wæver, O. and de Wilde, J. (1998) *Security: a new framework for analysis*. Boulder: Lynne Rienner.

⁴⁶ Taureck, R. (2006), "Securitization theory and securitization studies," *Journal of International Relations and Development* 9(1): 53-61; Waever, O. (2007) "Securitization and desecuritization," *International Security*, 66

⁴⁷ Williams, M.C. (2003) "Words, Images, Enemies: Securitization and International Politics", *International Studies Quarterly* 47(4): 511-531.

⁴⁸ Ibid.

⁴⁹ Buzan, B., Wæver, O. and de Wilde, J. (1998) *op. cit.*

accept the issue as a security threat.

Although in principle all societal actors may securitize a great variety of subjects, in practice not all claims are socially effective, and not all actors are equally powerful. As a consequence, securitization may also fail and the opposite may well occur, that is a subject may be successfully desecuritized. Desecuritization is an equally important political act, for it ends the state of exception, which had been called upon a given subject through a previous act of securitization, and brings the subject back to the ordinary and democratic political debate.

The securitization of a given subject or domain does not imply that such domain is objectively vital for the survival of a given state; it rather means that it has been successfully constructed as such, and that the management of its social, economic and political dynamics have been configured as a problem of security. In principle, anyone can construct something as a security problem through given speech acts. The ability to effectively securitize a given subject is, however, highly dependent on both the status of a given actor, and on whether similar issues are generally perceived to be security threats. In general, a securitization act has been successful when three elements concur: an existential threat has been successfully mobilized, emergency actions have been implemented and the breaking free of the ordinary rules has been successfully accomplished.

In *Security: A New Framework for Analysis*⁵⁰, Barry Buzan, Ole Wæver and Jaap de Wilde suggested that, apart from the military sector, there exist four socio-political domains in which securitization trends have been taking place, i.e. the political, the economic, the society and the environment. When military security is at stake, subjects can be securitized by constructing them in relation to an existential threat to the territorial integrity of the state. In political terms, subjects can be securitized through their social construction in relation to an existential threat to political legitimacy. Constructing them as constituting an existential threat to an equally constructed national identity, for instance, has often securitized migration and cultural diversity. Securitization processes, though, could easily involve more than one of these sectors at the same time. If we consider the case of the 2003 Invasion of Iraq, the conflict was securitized militarily for the weapons of mass destruction were officially the reason for the invasion. However, the war was also securitized as a societal problem as human rights in Saddam's regime were also mentioned in the public rationale. Another example proceeds from immigration policies in both the US and the EU, where concerns of terrorist infiltration are regularly cited as grounds for the tight control of borders. As a consequence, there has been a gradual and tighter association of illegal migration with security threats and concerns, which, in turn, has taken attention away from the social, political and economic factors that have always been at play in international migration. Similar trends could be observed when we focus on financial and economic transactions and movements, which have been increasingly presented as vulnerable to criminal attacks, and, therefore, ideal subjects for security policies. The economic prosperity of a country or of an economic sector is increasingly framed in terms of a (technological) improvement of dedicated security measures.

Securitization theory is first, and foremost, a theoretical account of how security expands and evolves over time. It is a theory that explores the social construction of security and tries to understand how this act of construction is accomplished, under what conditions, by whom and for what purposes. It is not, in principle, a normative theory for it aims at studying how security is constructed and not how it should be constructed. Yet, it warns us of the potentially problematic implications of the untamed expansion of security agendas and discourses, because every time a subject is successfully securitized, it is then removed from ordinary democratic politics, placed under the emergency umbrella provided by the security label and addressed by extraordinary measures and actions. For this reason, many authors drawing inspiration from the Copenhagen School suggest that it is necessary to de-securitize issues like ethnic diversity and migration in order to bring them back to the realm of public political discourse and normal political dispute and accommodation.

Securitization theory has been criticized on several grounds, from both realist and constructivist point of view. Realist scholars have suggested that social constructivism does not give proper account of the actual and major issues in security studies, while some social constructivists have suggested that it is an oversimplified account of security that does not take into account the role of security analysts in

⁵⁰ Ibid.

participating and reinforcing existing securitization trends even when as they analyse securitization processes.⁵¹ It has also been criticized on ethical grounds, for it may occasionally seem to endorse realist practices of security actions and because it may be black boxing complex social phenomena such as social identities and ethnic integration⁵². Yet, it is important to distinguish between securitization theory, which tries to elaborate a set of conceptual tools that may help to study and understand the process of securitization and securitization practices, which successfully securitize more and more social and political subjects and foster the expansion of security agendas⁵³. Insofar as security technologies are concerned, securitization, however, makes an important contribution for it provides interesting and versatile set of conceptual tools to interpret and discuss a phenomenon that, though complex it may be, is certainly central to the continuing expansion of security technologies across different policy fields.

2.3 The Risk Society thesis

Inspired by what is known as the risk society thesis, some authors have focused on a redefinition of security studies along risk management approaches. Their work suggests that the redefinition of the security agenda has been largely provoked by the emergence of a variety of multi-faceted, sparsely located sources of threats, ranging from nuclear proliferation to trans-national organized crime, and from terrorist networks to financial speculations.

They explicitly draw from recent works published by Beck⁵⁴, who takes into account the changing security context after 9/11. In its initial account, however, Beck emphasized that emergence of new risks increasingly visible in some evolving trends in the natural and human environment, increasingly affected by contamination, pollution and depletion of natural and energy resources as well as radical changes in biosphere mechanisms and climate changes⁵⁵. In his view, these new threats were not only quantitatively but also qualitatively different from those menacing human societies in pre-modern and early modern times. First of all, they were the result of human manufacture, by-products of technological innovation and developments. Second, they defied territorial and temporal localization while carrying an intrinsic level of uncertainty that also defies calculation and prediction. As a result, these phenomena resist any attempt to turn them into quantifiable and predictable risks, preventing the elaboration and implementation of traditional means-ends rationality responses.

In Beck's narrative, this shift was a by-product of a broader transition from rational modernity, as presented in the works of Weber, to a self-reflexive modernity, that is a modernity constantly facing the effects of risk produced by the industrial society but cannot be dealt with according to its current standards.

Self-reflexive modernity, in other words, is a product of a *radicalization* of the modernization process, which has produced a gulf between the world of quantifiable risks in which we were used to acting and the world of non-quantifiable global risks associated with environmental changes, financial markets and terrorist threats that this process of transformation is creating⁵⁶. As a result, modern institutions – like the nation state, the welfare system and the nuclear family – and basic modern principles – such as the very idea of control and security, the binomial connection between science and rationality and the

⁵¹ Jackson, N.J. (2006) "International organizations, security dichotomies and the trafficking of persons and narcotics in post-Soviet Central Asia: a critique of the securitization framework." *Security Dialogue* 37(3): 299-317. Stritzel, H. (2007) "Towards a theory of securitization: Copenhagen and beyond," *European Journal of International Relations* 13(3): 357-83. Knudsen, O.F. (2001) "Post-Copenhagen security studies: desecuritizing securitization," *Security Dialogue* 32(3): 355-68.

⁵² Williams, M.C. (2003) *op. cit.* Taureck, R. (2006) *op. cit.*

⁵³ Taureck, R. (2006) *op. cit.*

⁵⁴ Beck, U. (2002) "The Terrorist Threat: World Risk Society Revisited" *Theory, Culture and Society* 19(4): 39-55; Beck U., Bonss, W. and Lau, C. (2003) "The Theory of Reflexive Modernization – Problematic, Hypotheses and Research Programme" *Theory, Culture and Society* 20(2): 1-33; Beck, U. and Lau, C. (2005) "Second Modernity as a research agenda: theoretical and empirical explorations in the meta-change of modern society," *British Journal of Sociology*, 56(4): 525-557

⁵⁵ Beck, U. (1992), *op. cit.*

⁵⁶ Beck, U. (2002) *op. cit.*

exploitation of nature as recipient of external resources – are increasingly questioned by the expansion of globalization and the intensification of individualization.

The generation of manufactured risks exceeds the regulatory power of the nation state because contemporary risks cross international borders as a result of globalization processes. In more specific terms, current globalization processes seem to be increasingly characterized by the emergence of equally global risks, which materialize as a result of the interaction between objective factors, such as the transnational nature of political and economic agents and technological tools involved, and subjective factors, which are related to the social construction of certain events as risky and the changing general public understanding of security.

While globalization is producing a vanishing of borders and the re-evaluation of the role and limits of the nation state, the radicalized process of individualization is not only challenging the very foundations of the welfare state system but also producing an erosion of the several patterns of collective life. At the same time, the gradual acknowledgement of the scarcity of basic natural resources and of the devastating impact of pollution and human exploitation has generated the perception of a global ecological crisis, which is shaping a new understanding of nature as part and parcel of society. These fields and institutions are permanently being redefined and restructured in a context where traditional distinctions, like we/others, nature/society, global/local, war/peace or public/private, experience a permanent process of blurring boundaries⁵⁷.

Among all the risks generated by the transition from first to second modernity, Beck paid special attention to the dynamics of risks and risk perception triggered by the global terrorist threat following 9/11 (2002). This event produced a twofold reaction, which set in motion new narratives and practices related to security and democracy. On the one hand, it materialized a global threat, external to Western society in philosophical terms but internal in structural, social and political terms. In other words, the enemy was clearly identified in abstract terms as 'alien' to Western culture but physically placed everywhere, within national borders, among all citizens, in a potentially unlimited setting that defies spatial and temporal localization⁵⁸. The walls between innocents and guilty collapsed, extending suspicion to all citizens, without exception: *"Under conditions of a universalized perception of terrorist threats all individuals are potentially suspects and all individual rights constitute potential risks to the state"*⁵⁹. Vulnerability and fear are, thus, normalized, ceasing to be problematized⁶⁰. Along these lines, the very concept of freedom has been redesigned to accommodate the risk approach, shifting to a new 'freedom from insecurity.'⁶¹

Echoing some of the arguments set forward by securitization studies, some recent studies inspired by the risk society thesis considered that these recent changes are likely to encourage the introduction of legal provisions restrictive of civic rights and freedom and the adoption of anticipatory intervention and precautionary measures. In both cases, the concrete proposals elaborated by western states have consistently relied on the development and implementation of new security technologies. The interaction between risk management responses and technological outcomes has produced a new narrative of security that seem to substantially confirm Beck's suggestion of an overlapping between first and second modernity⁶².

While the global and unpredictable nature of terrorist threats is readily acknowledged, the solution keeps being offered following the modern rationality approach, which seeks to control and dominate problems through the implementation of new technological devices, from biometrics to IT technologies, within and across the territorial boundaries of the nation state⁶³. Detection and identification of risks through enhanced technological devices somewhat suggest that these risks cannot be autonomously observed by ordinary citizens. In a risk society, citizens are made aware of

⁵⁷ Beck, U., Bonss, W. and Lau, C. (2003) *op. cit.*

⁵⁸ Beck, U. (2002) *op. cit.* p. 44.

⁵⁹ Beck, U., Bonss, W. and Lau, C. (2003) *op. cit.* p.12.

⁶⁰ Spence, K. (2005) "World Risk Society and War Against Terror," *Political Studies* 53(2): 284-302.

⁶¹ Mythen, G. and Walklate, S. (2006) *Beyond the 'Risk Society': Critical Reflections on Risk and Human Security*. London: McGraw-Hill.

⁶² Beck, U. and Lau, C. (2005) *op. cit.*

⁶³ Beck, U. and Lau, C. (2005) *op. cit.* Duffield, M. and Waddell, N. (2006) *op. cit.*

these risks through the experts, the media or the political debate⁶⁴. Global systemic risks are set and defined by governments and then presented to the public through the media. While governments claim to be the only actors entitled to decide when, where and to what extent there is a security threat, surveillance technologies emerge as the privileged instruments to enhance national and international security.

Technological developments play a constitutive role in Beck's narrative of the transition from traditional modernity into self-reflexive modernity, both as drivers of emerging global risks and of (problematic) global management responses. Along the same lines, the new security technologies are increasingly becoming a cornerstone of both security research agenda and national and international security policy. Although extensively discussing, from a constructivist point of view, the various social and political dynamics associated with the emergence of new security agendas and strategies, risk society security studies have surprisingly paid little attention to technological changes.

Drawing on the theoretical framework of a risk society, and inspired by its most intriguing questions on the relationship between risk, technology and politics in the transition from the first to the second modernity, however, some studies aimed at exploring in deeper empirical details the following research questions: has global terrorism made the public highly sensitive to the issue of security and, if so, what are the security threats they perceive as most urgent and compelling?

The complex interaction between technology, security and risk in the European society after 9/11 has been extensively discussed by Levi and Wall, who argued not only that the re-securitisation of society and politics began before the Twin Towers collapsed but also that recent security technologies have been introduced to integrate already existing security measures, within the boundaries of an already existing legal framework. Although it is true that these events paved the way to those proposals that previously would not have been found politically acceptable, the implementation of new security technologies is currently facing two major challenges. First, they are gathering poor quality data that are difficult to integrate and produce little improvement in terms of the reduction of crime risks. Second, they are *de facto* encouraging new forms of crimes that settle outside the monitored reality, such as identity theft, illegal navigation through the flaws of software systems and underground economic and financial transactions⁶⁵.

The increasing reliance on security technologies in the attempt of anticipating and managing security threats and risks has caused preoccupation about the potential authoritarian implications. Angela Liberatore, on the one hand, acknowledges the growing implementation of security technologies in the EU, but, on the other hand, she argues that this new emphasis on security and technology is accompanied by significant attempts at further democratising the EU, through the growing role played by public participation and scrutiny. In the end, she argues that the existence of a plurality of actors involved in the policy making processes on security enhancement provides a relatively safety net against totalitarian outcomes, while it also ensures the gradual emergence of the EU as a new security actor and as a supranational democratic polity⁶⁶. While Shearing wonders whether the new emphasis on risk-focused technologies is triggering the emergence of a new form of justice, less centred on individual punishment⁶⁷, Elia Zureik explored the social, political and economic dynamics leading western governments to promote biometrics and surveillance technologies. In her work, it comes to the fore how the political exploitation of public fear, the lobbying effort of the industry and the tight connection between economic and political interests made technology uptake a crucial factor of security policies across the globe.⁶⁸ Some studies seem to confirm Zureik claims as they did find relatively high rates of anxiety and PTSD (Post-Traumatic Syndrome Disorder) symptomatology in

⁶⁴ Beck, U. (2006) *Cosmopolitan Vision*. Cambridge: Polity Press.

⁶⁵ Levi, M. and Wall, D. (2004) "Technologies, Security, and Privacy in the Post 9/11 European Information Society," *Journal of Law and Society* 31(2): 194-220.

⁶⁶ Liberatore, A. (2007) "Balancing security and democracy, and the role of expertise: Biometrics politics in the European Union" *European Journal of Criminal Policy* 13: 109-137.

⁶⁷ Shearing, C. and Johnston, L. (2005) "Justice in the risk society" *The Australian and New Zealand Journal of Criminology* 38(1): 25-38.

⁶⁸ Zureik, E. and Hindle, K. (2004) *op. cit.*

persons only indirectly exposed to the 9/11 attacks through the media.⁶⁹

By the same token, some research has empirically looked at the impact of a growing sense of vulnerability and fear on people's willingness to accept new SOSTs and to give away part of their civil liberties. It was well known, already before 9/11, that fear of terrorism promotes intolerance and a willingness to forego basic civil liberties.⁷⁰ Yet, some studies following 9/11 demonstrated that the experience of terrorist attacks makes people more sensitive to the issue of security and security threats.⁷¹ In some cases, this higher sensitivity, however, did not lead people to accept or adopt new security technologies.⁷² Other studies suggested that face recognition technology, and security technologies in general, are likely to force us to renounce to some of our liberties to enhance security⁷³ (Bowyer 2004). Provided that security technologies are effective in delivering the benefits claimed, which is controversial⁷⁴, they are likely to force us to make a clear distinction between those liberties that need to be sacrificed to security needs and those that indeed, cannot be included in the trade-off⁷⁵ (See D3.2).

To be fair, though, the risk society approach has also been criticised extensively, during the past decade. Gabe Mythen and Sandra Walklate have clearly pointed out how Beck's theory, as it is formulated⁷⁶, escapes empirical validation and over-simplifies the nature of dangers, which cannot be reduced to the natural/manufactured dichotomy. Beck's narrative of modernity, which is eminently Eurocentric, also oversimplifies the various stages of human history, separating in clear-cut stages the transition from pre-modernity to present days. Criticisms have also been raised against Beck's claim on the classless nature of global risks: both theoretical⁷⁷ and empirical works⁷⁸ have demonstrated that distribution of, and exposure to, risks reinforce social inequality. Moreover, while cultural understanding of risk cannot be generalized, risks may also imply beneficial outcomes⁷⁹.

Criticism against the risk society thesis has also emerged from a different approach, which relies on the concept of governmentality and draws explicitly from Foucault. The literature on Governmentality and risk refers to Foucault's concept of a new style of governance in modernity. According to the governmentality approach, risk is mainly understood as a concept that is entirely the product of social construction. There is no outer world, which forces society to respond to risk. Quite to the contrary, risk is understood as a specific way, or better-said *dispositif*, to shape and control populations and to govern societies. O'Malley⁸⁰ suggested that risk was to be one of the central technologies of government in terms of which the analytical framework was developed. Donzelot's 1979 paper on risk is the first

⁶⁹ Marshall, R.D., Bryant, R.A., Amsel, L., Suh, E.J., Cook, J.M. and Neria, Y. (2007) "The psychology of ongoing threat: relative risk appraisal, the September 11 attacks, and terrorism-related fears." *American Psychologist; American Psychologist* 62(4):304.

⁷⁰ Doty, R. M., Peterson, B. E. and Winter, D.G. (1991) "Threat and authoritarianism in the United States, 1978-1987," *Journal of Personality and Social Psychology* 61(4): 629.

⁷¹ Huddy, L., Feldman, S., Capelos, T. and Provost, C. (2002) "The consequences of Terrorism: Disentangling the effects of personal and national threat." *Political Psychology* 23(3): 485-509.

⁷² Lee, J.K., and Rao, H.R. (2007) "Perceived risks, counter-beliefs, and intentions to use anti-/counter-terrorism websites: An exploratory study of government-citizens online interactions in a turbulent environment," *Decision Support Systems* 43(4): 1431-49.

⁷³ Bowyer, K.W. (2004) "Face Recognition Technology: Security versus Privacy," *IEEE Technology and Society Magazine* 23(1): 9-19.

⁷⁴ Jain A. K., Ross, A. and Uludag, U. (2005) "Biometric Template Security: Challenges and Solutions" available at <http://biometrics.cse.msu.edu>, last accessed June 2008.

⁷⁵ Porcedda, M.G., M. Vermeulen et al. (2013). Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy. Deliverable 3.2, SurPRISE Project. Florence, European University Institute.

⁷⁶ Mythen, G. (2004) *Ulrich Beck: A Critical Introduction to the Risk Society*. London: Pluto Press. Mythen, G. and Walklate, S (2006) *op.cit.*

⁷⁷ Mythen, G. (2004) *op.cit.*

⁷⁸ Cooper, M. (2008) "The inequality of security: Winners and losers in the risk society," *Human Relations* 61(9): 1229-1258.

⁷⁹ Sustain, C.R. (2007) *Worst-case scenarios*. Harvard University Press.

⁸⁰ O'Malley, P. (2009) Governmentality and Risk, in J. Zinn ed., "Social Theories of risk and uncertainty", working paper, available at <http://www.papers.ssrn.com>

example in which a governmentality approach (or a 'governmental analytic') was developed, at least in English. While Ewald's *L'Etat Providence*, focusing on risk as a central technology in the welfare state, was never translated, the publication in 1991 of *The Foucault Effect Studies in Governmentality* brought this body of work to the attention of Anglophone sociology.⁸¹ In particular, the papers by Ewald, Defert and Castels explored risk in terms of this emerging analytical framework, the first two dealing with insurance, the latter with psychiatry.

In the perspective of governmentality, power is not just understood as the prerogative of authorities. Rather it is constituted in practices as well as in knowledge; that is the ways in which people think and act about an issue. Applying this perspective, research studies on governmentality use the concepts such as 'truth programmes', 'power strategies' and 'technologies of the self' in order to show how risk is used in societal games of power and control. This approach is criticised in a socio-cultural perspective for its generalised model of the self, which would underestimate the possibilities and different responses to social risk demands.⁸²

Arguing that the risk society thesis problematically views risk within a macro-sociological narrative of modernity, Aradau and van Munster suggested that governing terrorism through risk involves a permanent adjustment of traditional forms of risk management. Deploying the Foucauldian notion of 'dispositif', they explore precautionary risk and risk analysis as conceptual tools that can shed light on the heterogeneous practices that are defined as the 'war on terror'.⁸³

In the governmentality approach, O'Malley⁸⁴ has recently suggested not to focus only on the constructions of risks (and the transformation of uncertainty into risk) but also on the management of uncertainties as governmental strategies. Given that most problems are not constructed purely as risk problems but, rather, as problems of unsolvable uncertainty, and that uncertainty cannot be solved by objective strategies alone, from a governmentality perspective, moral and political aspects become even more important.

Though criticisms against the risk society thesis have been successful to bring to the fore the limits of considering risk merely from a dialectical view of modernity and post-modernity, these studies have in a way reinforced the idea that risk and risk management constitute a crucial element in contemporary societies, especially when new technologies are introduced and security is at stake.

2.4 Surveillance studies

A growing body of literature has taken surveillance as its core object in the past 20 years or so. In the words of one of the main authors in this field, David Lyon, surveillance studies can be '*described as a cross-disciplinary initiative to understand the rapidly increasing ways in which personal details are collected, stored, transmitted, checked, and used as means of influencing and managing people and populations*'⁸⁵. Surveillance studies, therefore, is a vast body of works that focuses on the collection, use and exploitation of personal information and data across many different social areas and fields, ranging from business practices to migration and political movements.

One the main areas of study, though, is the relationship between security, technology and surveillance. The reason behind this specific interest is, in a way, self-evident. As security policies and strategies increasingly grow on the implementation of new security technologies, the amount of personal data

⁸¹ Foucault, M. (1991) "Governmentality," in G. Burchell, C. Gordon and P. Miller (eds.), *The Foucault Effect: Studies in Governmentality*. London: Harvester Wheatsheaf. pp. 87-104. Burchell, G., Gordon, C. and Miller, P. (eds) (1991) *The Foucault Effect: Studies in Governmentality*. Chicago: University of Chicago Press. Barry, A., Osborne, T. and Rose, N. (eds.) (1996) *Foucault and political reason: liberalism, neo-liberalism and rationalities of government*. London: UCL Press. Dean, M. (1999) *Governmentality: Power and Rule in Modern Society*. London: Sage. O'Malley, P. (2004) *Risk, Uncertainty and Government*. London: Glasshouse Press.

⁸² Lupton, D. (1999) *Risk*. London: Routledge.

⁸³ Aradau, C. and R. Van Munster. (2007) "Governing terrorism through risk: Taking precautions, (un) knowing the future." *European Journal of International Relations* 13(1):89-115.

⁸⁴ O'Malley, P. (2004) op cit

⁸⁵ Lyon, D. (2002) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London and New York: Routledge.

and information grows exponentially, paving the way for a proliferation of surveillance practices. In turn, surveillance practices are also shaping the way we understand and conceptualize security. In other words, as security extends its agenda and becomes more pro-active and pre-emptive, adopting a risk assessment approach, the collection and exploitation of personal information and data become a constitutive element of security strategies.

A first body of works, in surveillance studies, was largely influenced by the works of Foucault on the Panopticon, which was a concept borrowed from Bentham. In some of his works, such as *Discipline and Punish*, Foucault commented upon this Panopticon, stressing the ability to monitor all the inmates of a prison from a single, central position, which was invisible to the inmates but enabled a full vision of all that happened inside the prison. This first conceptualization of surveillance emphasized the hierarchical, vertical and authoritarian aspects of a political device that aimed at monitoring individual behaviour to the point that the subjects under surveillance would interiorize the monitoring gaze and behave according to a given set of rules, *regardless of whether they were actually monitored or not*. The scope of the Panopticon, thus, was to promote the interiorisation of the surveilling gaze and substitute punishment for self-discipline. Surveillance, therefore, is essentially a disciplining practice, which looks for a gradual interiorization of power, rules and authorities. This process, especially if applied to security, can be described as a process of *normalization*, which somewhat suggests that human behaviour is best regulated from within the subjects rather than from external rules and authorities, outside and above the subjects. For some authors, living in surveillance societies implies that individuals are subjected to this disciplinary rationality, although the latter may be evolving along with the use of a range of new surveillance technologies. David Lyon, for instance, speaks of an electronic Panopticon.

However, taking distance from the Orwellian image of a Big Brother watching everyone and everywhere, more recent contributions in surveillance studies have shifted away from this vertical and centralistic view of surveillance, emphasizing the rhizomatic nature of surveillance⁸⁶, or, in other words, the diffuse, horizontal, shared and heterogeneous forms of surveillance. Rather than holding a central position from which a central authority can monitor everything, these new contributions emphasize the distributed nature of surveillants and surveilled, as well as the focused, narrow and limited scope of the surveilling gaze. Rather than panoptica, surveillance is oligoptica⁸⁷. Other works have focused on lateral, mutual and bottom-up forms of surveillance⁸⁸.

Haggerty and Ericson⁸⁹ for instance, speak of surveillance assemblages. They emphasize the heterogeneity and instability of a variety of forms of surveillance, explicitly questioning the hierarchical model and showing the assembled nature of surveillance. Inspired by Actor Network theory, they describe surveillance as an assemblage of different and heterogeneous components, both human and non-human. In their work, a more distributed, more fragile and negotiated concept of surveillance emerges.

Whether in their hierarchical and centralized version or in the more horizontal, rhizomatic variety, everyday surveillance is endemic to modern, liberal societies⁹⁰. Surveillance, it is important to notice, is focused, systematic and deliberate and it is by no means confined to some exceptional cases of occasional monitoring. In modern societies in a way, as David Lyon suggests, surveillance is routine⁹¹.

Moreover, surveillance is driven by prescriptions about normal and abnormal behaviours and how these behaviours have to be steered. It relates therefore to the activity of governing and works through the establishment and promotion of given categories of behaviours and profiles, and the repression or

⁸⁶ Haggerty, K.D. and Ericson, R.V. (2000) "The Surveillant Assemblage" *British Journal of Sociology* 51(4): 605-622.

⁸⁷ Gad, C. and Lauritsen, P. (2009) "Situated surveillance: an ethnographic study of fisheries inspection in Denmark". *Science & Society*, 7(1): 49-57.

⁸⁸ Andrejevic, M. (2002) "The work of watching one another: Lateral surveillance, risk, and governance," *Surveillance & Society* 2(4). Lyon, D. ed. (2006) *Theorizing Surveillance: the Panopticon and Beyond*. Cullompton, Devon (UK): Willan Publishing.

⁸⁹ Haggerty, K.D. and Ericson, R.V. (2000) *op.cit.*

⁹⁰ Lyon, D. (2007) "Surveillance Security and Social Sorting: Emerging Research Priorities," *International Criminal Justice Review* 17(3): 161-70.

⁹¹ Ibid.

discouragement of other behaviours and profiles⁹². Recent works in surveillance studies have addressed the relationship between security and surveillance drawing inspiration from some later works of Foucault, where security was described as a technology of power operating through liberties, through statistical reasoning as well as through risk analysis and profiling. More specifically, Foucault made a distinction between three technologies of power: *sovereignty*, which operated through mainly external interventions legitimized by a political authority, *discipline*, which operated through the previously described process of normalization, and *security*, which was different for it works through specific arrangements of ordinary life, for it aimed at controlling populations without disrupting the natural processes characterizing them.⁹³ Valverde and Mopas⁹⁴ have, for instance, spoken of a 'dream of targeted governance', i.e. the increasing reliance on risk assessment and risk management techniques to govern what are considered deviant populations.

An interesting and especially relevant group of works has addressed surveillance with a specific focus on our societies increasing reliance on electronic data. A pioneer among these authors was Roger Clarke⁹⁵, who coined the terms 'dataveillance' back in 1988. The proliferation of personal data, mostly in digital forms but not only, seems to be giving a new and most problematic twist to surveillance practices. This is especially due to the huge possibilities of social sorting that these technologies, practices and data enable. This is called phenetic fix by David Lyon: "What I call the '*phenetic fix*' describes this trend – to capture personal data triggered by human bodies and to use these abstractions to place people in new social classes of income, attributes, habits, preferences, or offences, in order to influence, manage, or control them"⁹⁶

Social sorting, the categorization of individuals, is constantly being performed not just for security purposes through public agencies, but also for commercial purposes by private agencies. In both cases, the retrieval and processing of huge flows of personal data lead to vast and detailed practices of social sorting, which then enable targeted actions. Social sorting and individual profiling has therefore become a key element of pre-emptive and pro-active security policies.⁹⁷

Finally, other works have emphasized practices of lateral surveillance, which are based on the enrolment of individuals and social networks, calling for peer-to-peer monitoring, or voluntary surveillance or self-surveillance.⁹⁸ Social networks, for instance, have turned surveillance into a daily practice, a generalized and familiar activity that naturally reinforces a synoptic logic. Other examples of self-surveillance or mutual surveillance come from web cameras and voyeurism, the "quantified self movement", or the GPS-based apps through smartphones.

Although sometimes surveillance studies quite often restrict their focus to individual privacy and freedom, which somewhat diverts attention from the broader social consequences of surveillance practices, their continued and extended work on social sorting, individual profiling and the public-private overlaps that usually come along with surveillance has raised awareness about the changing nature of social and political relations, as well as about the deep and disquieting implications of a closer association between surveillance and security.

⁹² Friedewald, M. and Bellanova, R. (2012) *Deliverable 1.1. Smart Surveillance – State of the Art*. SAPIENT Project. Available in www.sapientsproject.eu.

⁹³ Ibid

⁹⁴ Valverde, M. and Mopas, M.S. (2004) "Insecurity and the Dream of Targeted Governance" in Wendy Larner and William Walters (eds.) *Global Governmentality*. New York: Routledge, pp. 233-250.

⁹⁵ Clarke, R. (1988) "Information technology and dataveillance" *Communications of the ACM* 31(5): 498-512.

⁹⁶ Lyon, D. (2002) *op. cit.*

⁹⁷ Council of the European Union "Draft Internal Security Strategy for the European Union: Towards a European Security Model" (Brussels, DG H, 7120/10), p. 20.

⁹⁸ Friedewald, M. and Bellanova, R. (2012) *op. cit.* p. 6.

2.5 Security technology, neoliberalism and the competition state

The increasing reliance of European internal and external security strategies on the development and implementation of new security, often surveillance-orientated, technologies can also be fruitful addressed and analysed from a different perspective, which does not emphasize the securitization dynamics, the risk assessment perspectives or the surveillance implications but rather focuses on the mutually constitutive relationship between science and social order in general, and science and the neoliberal governance regimes, in particular.

In this section, therefore, we will try to shift our focus to the economic drivers behind security technology and to some of the frames recently adopted by international organization like the OECD, when they talk, for instance, of a security economy⁹⁹. We will do so drawing from Science and technologies studies approaches that have been recently shown how the trajectories followed by some new technologies, such as GMOs or genetic engineering well illustrate how science and social order are the outcome of a process of co-construction where neoliberal ideas and principles have played a constitutive role. Although these approaches have turned their attention to security technologies only recently, they help us to understand better the relations between technological advances, neoliberal governance regimes and security approaches. The neoliberal shift endorsing technological framing and individualisation – which has encouraged the adoption of GMOs to address world hunger and the depletion of natural resources or the shift towards personalised medicine and genetic testing in public health care – has also affected European and US security policies. Neoliberal politics, have, for instance, consistently supported a decreased responsibility of the State for social security, social welfare and social integration. In turn, this has encouraged the adoption of a new emphasis on surveillance and on the anticipation of violence and crime, whenever possible, and towards more repressive measures when that was not possible. As a consequence, this shift has made new forms of security, i.e. pre-emptive and precautionary security, necessarily more relevant. In addition, the increasing social unrest as a consequence of neo-liberal economic policies has also reinforced this trend, which eventually attributes to surveillance-orientated security technologies a crucial role in crime prevention and repression.

Increasingly prominent in Science and Technology Studies, the theoretical perspective emphasising the mutually constitutive relationship between science and social order, has been gradually applied to the study and analysis of several emerging technologies, from GM crops and ICTs to biomedical technologies. This theoretical approach, which is known as co-production or co-construction, suggests that the traditional STS views that emphasized the social construction of technology did not take into due consideration that the opposite was equally relevant, that is the technological construction of the social. In other words, Sheila Jasanoff argued that both society and science are the outcomes of a process of simultaneous co-production, which implies that it would not be possible to understand a given technological development or a given social order unless they are both studied simultaneously in their joint process of co-construction¹⁰⁰.

As Sheila Jasanoff puts it, *'The reality of human experience emerges as the joint achievements of scientific, technical and social enterprise: science and society are co-produced, each underwriting the other's existence'*¹⁰¹. From a co-production perspective, therefore, the emergence and consolidation of the reproductive bioeconomy, therefore, is a complex process whose extent and implications go well beyond the mere impact of new biomedical technologies on existing social, ethical and legal practices. It is a process in which technological developments, research practices, economic interests and culturally embedded values systems constantly engage in four well-documented pathways of coproduction of science and social order, through the making of new identities, institutions, discourses and representations¹⁰². Through this process of co-production, scientific advances, technological artefacts and economic, socio-political norms are co-constructed. As Swedlow puts it, *'The concept of*

⁹⁹ OECD (2004) "The Security Economy", Paris: OECD Press

¹⁰⁰ Jasanoff, S. (2004) *op. cit.*

¹⁰¹ *Ibid.* p. 33.

¹⁰² *Ibid.* p. 38-39.

*coproduction helps us understand how knowledge and its production shape and sustain social and political identities and give them power and meaning*¹⁰³

In a recent contribution, Swedlow uses the co-production approach to illustrate the production of four different ways of constructing 'nature'. From a co-production perspective, other works have addressed, for instance, the emergence and consolidation of governance regulatory regimes in the area of biomedicine. In a recent article, Salter and Faulkner¹⁰⁴ have shown how different governance of innovation regimes in biomedicine can be successfully studied as the outcomes of a multilayer co-production process between three points of tensions: science, the society and the market. Governance regimes, as they argue, are co-produced through the interactions between the different institutional and cultural settings present in each of these elements in any single political space. Even small differences in how science is organized, conducted and financed, or in how the society perceives, uses and understand the process and outcomes of science or, finally, in how the market functions and operates may result in very different national and supranational governance regimes. In their model, each point of tension is a multilayer domain where different actors have different resources to make their way up to the policy process and back down to the implementation level. This asymmetric set of both vertical and horizontal relations often engenders conflicts between different political cultures and different value systems.

Inspired by co-production perspective, some recent works have been revisiting the emergence of biotechnologies with a focus on their relationship with neoliberal regimes of knowledge production and governance. Melinda Cooper's '*Life as surplus*'¹⁰⁵, for instance, reconstructs the emergence of biotechnology through a genealogy that goes back to the collapse of Bretton Woods and the publication the 1972 report, *Limits to Growth*. In her work, the neoliberal policies of the 1980s and, in a revised version, of the 1990s played a constitutive role in the emergence of both biotechnologies and intellectual property regimes. The potential contribution of the new biotechnologies towards national economic growth made the US reduce public spending on healthcare and social welfare services but dramatically increased public spending on science and technology¹⁰⁶. This new phase that Peck and Tickell¹⁰⁷ captured with the term "roll out" neoliberalism, did not simply imply a return of the state as a major source of public funding for science and technology. It also implied a number of relevant changes in how science and technology was being conducted, implemented and commercialized but also on how technology assessment and regulation was to be set to operate. It also changed the very nature of the state, favouring a shift from a Keynesian welfare state, mainly intervening on through demand side measures, into a post-neoliberal *competition state*, now intervening essentially through supply-side measures¹⁰⁸.

These relevant changes took place in what Benner and Löfgren define as education policies, appropriation policies and ethical (regulatory) policies¹⁰⁹. Educational measures related mainly to the R&D policies, the support of public-private partnership, and the alignment of public research priorities with business interests and expectations and have been mentioned before. These measures, however, were not going to be successful unless private investments and effort could be involved in the new biotech revolution, and this could only be accomplished by making the new technological products and applications very profitable. In the 1980s, when these policies were about to be elaborated and formulated, it was considered that the long span of time which any of these biotech innovations needed before they could make it to the market would have scared off private investors unless the profit eventually made could be protected for a sufficient amount of time. This gave rise to an increasingly broader

¹⁰³ Swedlow, B. (2011) "Cultural Coproduction of Four States of Knowledge," *Science, Technology & Human Values*.

¹⁰⁴ Salter, B. and Faulkner, A. (2011) "State strategies of governance in biomedical innovation: Aligning conceptual approaches for understanding rising powers in the global context", *Globalization and Health* 7(11).

¹⁰⁵ Cooper, M. (2008) *op. cit.*

¹⁰⁶ Ibid. p. 27.

¹⁰⁷ Peck, J.A. and Tickell, A. (2002) *op. cit.*

¹⁰⁸ Benner, M., and Löfgren, H. (2007) "The Bio-economy and the Competition State: Transcending the Dichotomy between Coordinated and Liberal Market Economies" *New Political Science* 29(1): 77-95.

¹⁰⁹ Ibid. p. 81-84.

interpretation of the scope of patenting and of the actual duration of it¹¹⁰. Intellectual property rights and patenting became therefore the core of new appropriation policies, in which also not only private companies but also universities and public research centres were encouraged to patent their results and give birth to spin-off to commercialize their products and applications.

The third pillar of the competition state, at least in relation to the emerging biotechnologies, was the development of appropriate regulatory frameworks that could maintain citizens' trust in science and the public system without, however, hindering the development and progress of innovation. The US and Europe, as we know today, adopted different strategies in relation to GMOs, with Europe adopting the precautionary principles and endorsing more public consultations than the US, but the overall strategy on other biotechnologies, especially medical ones, was essentially convergent and is nicely captured by the word 'governance'. Although there exist hundreds of different definitions of governance, the term governance essentially serves to capture a shift from direct, top-down governmental regulatory interventions to a more shared, horizontal and diffused form of management and regulation of new technological products and processes in which many stakeholders are involved and in which constant negotiations are the usual practices adopted in the decision-making process¹¹¹. Though it has been noticed that governance mechanisms are more inclusive than strict, top-down governmental regulations, for they involve different stakeholders, with their relative expertise and interests, it must also be considered that the forms of governance introduced usually do not take into account the often enormous difference in economic and power status of these stakeholders and tend to favour market-based forms of regulations. Sensitive issues like human genetic data, human tissues or natural biological resources belonging to the biodiversity reservoirs of developing countries, are therefore left to the market forces to decide their fate, often under the notions of individual consensus, patient choice or reproductive autonomy, which in turn leave less powerful groups, individuals, countries and populations in a position of enhanced vulnerability and exploitability.

The history of ICT and security technologies can also be analysed against this political and economic background. During the late 1990s, what was first a vision of economic growth, competitiveness and technological innovation and then full-fledged political project, capable of transforming not only scientific policies and the research agenda, but actually the whole neoliberal understanding of the state of the public sector, and of science, innovation and regulation, had already blossomed in ICTs.

The interesting contribution of these studies is their emphasis on how neoliberal regimes of knowledge production and governance and the new technologies co-produced each other, changing our way of understanding both technology and capitalism. One main contribution, for instance, is the emphasis on the fact the knowledge economy is not 'out there', and that their successful development is at least in part functional to the advance and success of a global political project. The latter proposes the development and implementation of a set of emerging technologies to tackle the main world problems and envisions a set of future economic, social and political arrangements yet to be set to work in order to allow these technologies to operate as expected. In this political project, security technologies also can only come to life as a result of a complex process of enactment that implies much more than the mere technical development of appropriate biotechnologies.

This process of enactment normally follows five steps, which are not necessarily chronologically ordered and often overlap. In a first stage, the problems and issues at stake are framed in such a way that given technologies make sense as a solution. This approach, which as elsewhere presented as a technological fix tends to focus exclusively on the solution side of a given problem¹¹², shifting away the attention from the causes and narrowing down the debate to the great opportunities provided by emerging technologies to solve the problem. It generally aims at depoliticizing controversial issues, through an apparently uncontroversial emphasis on the cost-effective nature of the selected technologies. An

¹¹⁰ Birch, K. (2006) "The neoliberal underpinnings of the bioeconomy: The ideological discourses and practices of economic competitiveness," *Genomics, Society and Policy* 2 (3): 1-15.

¹¹¹ European Commission "Communication on Conflict Prevention" Brussels: COM (2001), 211, 2001. Nowotny, H., Scott, P. and Gibbons, M. (2003) "Introduction; Mode 2 Revisited: The New Production of Knowledge" *Minerva* 41(3): 179-194.

¹¹² Wynne, B. (1975) "The rhetoric of consensus politics: a critical review of technology assessment," *Research Policy* 4(2): 108-58.

example of the former process may proceed from the 'security economy' policy document published in 2004 by the OECD. In this document, security is framed in terms of a series of threats whose origins and causes are socially complex and, thus, difficult to address while its implications and consequence are well-defined and relatively easy to address through the appropriate development of security technologies. *'Faced with an array of potential hazards, from terrorism and computer viruses to fraud and organised crime, the world is perceived by many to be an increasingly dangerous place. As a result, the focus on security issues has sharpened and the demand for security-related goods and services has steadily grown, giving rise to a wide and varied range of economic activities in both the government domain and the business sector. This is the emerging security economy'*¹¹³. Framing security as a technical issue paves the way to technological solutions, but this in turn obscures not only the whole array of social, economic and political factors that may cause violence and crime but also obscures the contribution to the problem of the very innovation regime of which the companies developing security technologies are indeed part.

The first step—framing societal problems in such a way that technologies emerge as a cost-effective solution—is usually accompanied by a second step, where promises and expectations are articulated. Once it has been shown, very often without making reference to the actual achievements and contradictions of the existing technologies, that the new economic scenario is not only feasible and on its way, but also positively embedded in the dominant imaginaries of how the world should look like and should be acted upon, financial support need to be mobilized. This mobilization is framed in different ways, and includes raising levels of public R&D funding, growing financial support to innovation in private sector, and also a constant plea for an alignment of research institutions and private companies.

Although essentially presented as a general investment in new technologies, from the development of which citizens, the economy and the very environment are equally likely to benefit, the economic strategy of the enactment, however, is often organized along a typical neoliberal scheme, which socializes the costs but privatizes the benefits of research and innovation. The general mechanism works around a steady but targeted increase in public research funds and the alignment of public research agenda to meet the goals and objectives of a rapid commercialization of the new security technologies, whose main customer remain public authorities.

This process of enactment, however, is generally always part and parcel of a more ambitious endeavour, whose aim is to transform society, to bend and align existing social and political arrangements with the techno-social imaginaries in which new security technologies are embedded. This is especially visible when the process of enactment engage in the fourth and fifth steps: the definition of the obstacles and hurdles that are expected to hinder the unfolding of the security economy, and the subsequent pressures on the regulatory frameworks, both at national and supranational level.

The identification and framing of hurdles and obstacles it is a crucial step, because it serves the function of both clearing the path and catalysing concern and critique away from the internal contradictions, limits and uncertainties of the technologies. In several policy documents on security strategy the first and most common hurdle identified is the public, in the sense of public acceptance, public support or public understanding of the benefits (and the risks) of the new security technologies. Whenever public acceptance is a problem, public education, information and understanding is identified as the way out. A well-informed, and therefore supposedly more supportive, public is identified not only as a necessary condition but also often as a competitive advantage.

In spite of the long and fruitful debates that have been set up on the issues of public understanding of science, lay public expertise, public engagement and upstream involvement of lay public¹¹⁴, the issue of public acceptance is still fundamentally framed in terms of better information and communication or better marketing campaigns. The ultimate goal is neither to improve the quality and transparency of

¹¹³ OECD (2004) *op. cit.* p. 8.

¹¹⁴ Felt, U. et al. (2007) *op. cit.* Wynne, B. (2008) "Elephants in the Rooms Where Publics Encounter 'Science'? A Response to Darrin Durant, 'Accounting for Expertise: Wynne and the Autonomy of the Lay Public,'" *Public Understanding of Science* 17(1): 21–33. Wilsdon, J. and Willis, R. (2004) *See-through science: Why public engagement needs to move upstream*. London: Demos.

technological development nor to increase the accountability when technology is deployed: it is rather to build trust among the public. The emphasis on public acceptance, moreover, shifts away the attention from the internal contradictions, limitations and unintended consequences of many these new technologies. Unknowns may be acknowledged, but are framed in terms of advance rate and competition and are not addressed in details and no mention is made of scientific and technical uncertainties.

Techno-social imaginaries associated with technological progress, economic growth and pre-emptive security are powerful imaginaries that are progressively shaping research and policy agenda, as well as economic and political choices in the fields of security, but have by no means monopolized the collective imaginary of what the Western society should be and how it should be acted upon. Alternative imaginaries, associated with political accountability, transparency of information, state of law, certainty and impartiality of justice, consumer protection, collective goods, public education and scientific research autonomy do exist and participate in the permanent, complex and articulated ideological negotiations that shape and enforce existing social orders. The field of regulation and governance is, perhaps, the domain where this negotiation is more easily observed.

Several EU documents address the issue of regulation and governance in a very explicit and bold way. Their strategy is deeply embedded in the neoliberal approach to technological and economic regulation, not only in the sense that governance and self-regulation should, whenever possible, replace direct, stringent governmental regulation, but also in the sense that they are informed by the belief in the ability of the market forces to regulate the commercial implementation of these technologies in an optimal way. The role of intellectual property rights (IPRs), together with patenting, play a constitutive role in this process of enactment, not only in the sense of allowing new inventions to produce economic profits, but actually in the more fundamental sense that without a broad patenting and IPR regime these inventions would not have been conceived in the first place.

An interesting example of the former process is the recently issued European Plan for the security market.¹¹⁵ In this document, the European Commission expresses its fears that Europe's share of the world security market could decrease by 2020 and proposes an action plan to reverse the decline. The document suggests that the main problem is the lack of a 'EU brand' in security, which allegedly is due to three primary causes: the fragmentation within the market, a gap between research and the market, which makes research investment risky, and the 'societal dimension', i.e. public concerns for privacy and data protection and the conflict between security and privacy.

To overcome these problems, following quite closely the enactment process, the EC proposes three primary policy actions. The first is to overcome market fragmentation by creating EU-wide security standards, harmonizing conformity standards and assessments, and better exploiting synergies between security and defence technologies. These synergies, as we shall see more in details in the next chapter, could be questioned from technological as well as democratic/constitutional perspectives.

The second is to reduce the gap between research and market, through the improvement of European funding programmes, a more effective deployment of IPRs, a harmonization of pre-commercial procurement (PCP) by the public sector, a wider opening of the EU partners internal markets and better integration of the 'societal dimension' of security. As to the latter, the EC plans to introduce societal 'impact checking' during the development phase in order to allow development and purchase to proceed with confidence that products will be 'accepted by society'. And to ensure this acceptance the EC is proposing that new products be developed with 'privacy by design' and 'privacy by default' principles via 'an appropriate EU standard.' While this could be seen as counter-productive to new developments, the Commission says it is 'convinced that there will be strong peer pressure for companies to follow such a standard which should gain a similar recognition value as for example the ISO 9000 management standard.'

¹¹⁵ European Commission "Action Plan for an innovative and competitive Security Industry" COM (2012) 417 final

3 Security, technology and democracy:

The rise and implications of the trade-off between security and liberty

3.1 Introduction

Despite the different approaches, the four streams of literature outlined and discussed in the previous sections seem to converge on one main issue: the steady and progressive entanglement of security and surveillance technologies. Moreover, though looking at different types of implications and consequences, they also agree on one more important issue, that is the controversial and complex relation between this progressive entanglement of security and technology and the ways in which democracy and liberty are being affected. In other words, the key issue at stake seems to be how come that security is increasingly associated with the implementation of new surveillance technologies and what the main implications of this phenomenon for our democracy and our liberty are.

In this section, we will first review some of the main issues and questions usually associated with the concept of security, especially when in association with technology and surveillance. In the second part of this chapter, we will analyse three key European policy documents on security strategy, from 2003 and 2008. In the third and last section, we will also try to complement the analysis performed on the European documents with the information and data proceeding from the national feedbacks, which review security, technology and democracy in the nine European countries participating in the SurPRISE Project. This section will be followed by some conclusive remarks, which will then pave the way to the last chapters of the deliverable.

3.2 Security, technology and democracy before 9/11

Security is a term that nowadays seems to be ubiquitous. A brief search on almost any policy document of the European Union contains at least one or two reference to security. Where security was traditionally associated, at least during the Cold War, with territorial integrity, it is not infrequent today to find, on the EU website, references to economic security, social security, infrastructure security, energy security, health security or even food security. Such an expansion of the use of, and reference to, the word 'security' has certainly not helped to clarify the meanings and limits of what has often been considered an essentially contested concept.¹¹⁶

The contemporary ubiquity of the term security should not, however, mislead. The term was widely used well before the end of the Cold War or the Twin Towers attack. For a long time, though, it was a term mostly associated with theories of international relations usually underpinned by realist perspectives emphasizing national integrity and sovereignty¹¹⁷. Security was, therefore, mostly related to the often military or foreign policy choices needed to ensure national sovereignty and preserve territorial integrity. While the object of security, i.e. the nation state and its sovereign territory, was often considered uncontroversial¹¹⁸ traditional debates in International Relations addressed the question related to whether nation states were actually the only or the most powerful international actors, as both the realist and neorealist approaches suggested¹¹⁹, or rather important actors among other equally important actors, such as NGOs, multinational corporations or intergovernmental organizations, as the

¹¹⁶ Baldwin, D.A. (1997) "The concept of security." *Review of International Studies* 23(1):5-26. Essentially contested concepts are said to be so value-laden that no amount of argument or evidence can ever lead to agreement on a single version as the 'corrector standard use'. See Gallie, W.B. (1955) "Essentially contested concepts." Pp. 167-98 in *Proceedings of the aristotelian society*: JSTOR.

¹¹⁷ Morgenthau, H.J. (1993) "Politics Among Nations. The Struggle for Power and Peace (Brief Edition)." *Revised by Thompson KW McGraw Hill. Boston.*

¹¹⁸ Walt, S.M. (1998) "International relations: one world, many theories." *Foreign Policy*:29-46.

¹¹⁹ Morgenthau, H.J. (1993) *op.cit.* Waltz, K.N. (1979) *Theory of international politics*. New York: McGraw-Hill.

liberal paradigm would reply¹²⁰. Other approaches, mainly those associated with neo-Marxist theories, emphasized the structural dependency of developing countries on developed countries, which allegedly gave rise to a new form of Western imperialist dominance.¹²¹ In fact, more debate was triggered, at least in theoretical terms, as to what sort of ethical and normative theory could be invoked to legitimize the use of power and military force to protect the national state integrity¹²². Though the debate among these traditional IR schools was at times quite harsh and polarized, the issue of national security as such was hardly debated, and even less theorized.

Traditionally speaking, the national security doctrine was overwhelmingly focused on nation states, and essentially addressed two main issues: national sovereignty and territorial integrity, with a strong emphasis on the military aspect of security¹²³. During the Cold War, owing to the relatively stable international context and blocks, this doctrine looked exhaustive and comprehensive enough to account for both relevant international political changes and foreign policy developments. Critiques of this doctrine, however, began to emerge already during the 1980s, which constituted in many respects the apogee of national security doctrines. Writing in 1984, Barry Buzan¹²⁴, for instance, affirmed that one important step to consider, when addressing a slippery concept like national security, is that the individual level cannot be separated from the national or state level. Not much later, in 1991, Buzan¹²⁵ considered that security was still an underdeveloped concept. Quite some time before Buzan, Wolfers¹²⁶ had identified the ambiguity of the concept of national security, as he acknowledged that 'national security', given the potential conflict with individual security, could be a dangerously ambiguous concept if not properly defined and specified. In his own terms, security was defined as 'the absence of threats to acquired values'¹²⁷.

Wolfers' definition of national security could represent a useful starting point for our analysis of the European evolution of the concept of security, both theoretically and empirically. In his own formulation, Baldwin¹²⁸ identified two key questions arising from Wolfers' definition: first, 'security for whom?', and, second, 'security for which values?'. We can add a third one, perhaps: 'absence of which type of threats?' These questions pave the way to a 'contextual understanding of security', an approach that takes distance from an essentialist perspective, expands its scope to address the multiplicity of uses, definitions and meanings of security and seems, thus, a much more fertile approach to security¹²⁹. Since Buzan and Baldwin were discussing the variety of aspects and features of a complex concept like security, several scholars have tried to define security¹³⁰. With the collapse of the Berlin Wall, however, the debate about the meaning and implications of security was gradually dominated by a new, emerging definition of security: the 'human security': The concept was initially formulated as an extension of the human development approach that had been, in the meanwhile, elaborated by the UNDP. The basic idea behind the concept was the need to bridge conceptually the two pillars of security, i.e. freedom from fear and freedom from want. In a nutshell, the pursuit of human security implied that no one could be really secure unless s/he is at the same time protected from both fear and indigence. However, the concept went further: it also insisted on the idea that to achieve proper security individuals need to be able to protect and enjoy their most important values. In the 1994 Human Development Report, human security, as a concept, added six types of security to a

¹²⁰ Strange, S. (1996) *The retreat of the state: The diffusion of power in the world economy*: Cambridge University Press.

¹²¹ Wallerstein, I. (1979) *The capitalist world-economy*: Cambridge University Press.

¹²² Frost, M. (1996) *Ethics in international relations: a constitutive theory*: Cambridge University Press.

¹²³ Sorensen, T.C. (1990) "Rethinking national security." *Foreign Affairs*:1-18.

¹²⁴ Buzan, B. (1984) "Peace, power, and security: contending concepts in the study of International Relations," *Journal of Peace Research* 21(2):109-25.

¹²⁵ Buzan, B. (1991) *People, states and fear: An agenda for international security studies in the post-cold war era*. Boulder, Colorado: Rienner.

¹²⁶ Wolfers, A. (1952) "'National Security' as an Ambiguous Symbol," *Political Science Quarterly*: 481-502.

¹²⁷ *Ibid.* p. 495.

¹²⁸ Baldwin, D.A. (1997) *op. cit.*

¹²⁹ Brooks, D.J. (2009). "What is security: Definition through knowledge categorization." *Security Journal* 23(3): 225-39.

¹³⁰ Manners, I. (2002) "European [security] Union: from existential threat to ontological security." Roskilde University Publications.

conventional concern with security from physical violence: income security, food security, health security, environmental security, community/identity security and security of political freedoms.¹³¹

Most importantly, 'human security' was openly concerned with the security of persons as opposed to the security of states. It also openly affirmed that state security could be legitimate only if it was based on and consistent with the security of individuals. Building on the concept of human security, the European Commission formulated its own concept of security, which was based on the idea that security means the protection of what Sabina Alkire¹³² defined as, quite ambiguously 'the vital core' of human development. Other contributions suggested that human security could be measured in terms of the years spent in a lifetime "outside generalized poverty"¹³³. In summary, human security complemented and broadened the human development concept with a concern with the stability of whatever goods are highlighted within human development and a higher emphasis on the physical security of persons¹³⁴. It also broadened the scope of the security studies concept of security beyond state and military security¹³⁵. Effectively, it also affirmed that human security would not be achieved without development, and vice versa.

The rise of human security, however, could not be understood unless placed in the wider context of the international world order following the end of the Cold War. On the one hand, the collapse of the rigid counter position of two blocks led some observers to claim the victory of capitalism and the end of history¹³⁶. On the other hand, more prosaically, new threats were likely to emerge and new balances and alliances were to be forged. In this eventually brief parenthesis, the UN and its organizations acquired a new legitimacy in the world order, and multilateralism became a new paradigm to address and solve international conflicts. If globalization was the new buzzword, peace building was, in many ways, the new approach to be fostered in order to deal with rogue states, ethnic conflicts and religious fundamentalisms¹³⁷. Needless to say, the UN peace-building approach was inevitably associated with the promotion of (Western) democracy and liberal values¹³⁸ as well as with the promotion of science, humanism and rational thinking¹³⁹.

Critiques of human security did not wait too long before they made their way into the debate. While some observers suggested that human security was far from being a new and relevant conceptual paradigm¹⁴⁰, others warned human security, as a concept, legitimized the word 'security' by giving it the connotation 'human'. In many ways, human security, and its immediate policy imperative of humanitarian intervention helped the state system with its monopoly on the violent means of security to use this newly acquired legitimacy, justifying intervention inside other states in the name of 'human security'¹⁴¹. Finally, starting from the consideration that perceived security and real security are quite different concepts, and the former could also be easily manipulated by media campaign, ideological beliefs and personal experiences, other observers have shifted their emphasis on psychological aspects

¹³¹ Kaul, I. (1994) "Human Development Report 1994," *American Journal of Economics and Sociology* 54(1):56-565. Ul Haq, M. (1995) *Reflections on human development*: USA: Oxford University Press.

¹³² Alkire, S. (2003) "A Conceptual Framework for Human Security," Working Paper CRISE 02 Jul 2009 <http://www.crise.ox.ac.uk/pubs/workingpaper2.pdf>

¹³³ King, G. and Murray, C.J.L. (2001) "Rethinking human security," *Political Science Quarterly*: 585-610.

¹³⁴ Gasper, D. (2005) "Securing humanity: Situating 'human security' as concept and discourse," *Journal of Human Development* 6(2): 221-45.

¹³⁵ Axworthy, L. (2001) "Human security and global governance: putting people first," *Global governance* 7:19.

¹³⁶ Fukuyama, F. (1989) "The end of history," *Globalization and the Challenges of a New Century*: 161-80.

¹³⁷ Cousens, E.M., Kumar, C. and Wermester, K. (2001) *Peacebuilding as politics: cultivating peace in fragile societies*: Lynne Rienner Pub.

¹³⁸ Santiso, C. (2002) "Promoting democratic governance and preventing the recurrence of conflict: the role of the United Nations development programme in post-conflict peace-building," *Journal of Latin American Studies*.

¹³⁹ Pavone, V. (2007) "From intergovernmental to global: UNESCO, as response to globalization," *The Review of International Organizations* 2(1):77-95.

¹⁴⁰ Paris, R. (2001) "Human security: paradigm shift or hot air?" *International Security* 26(2): 87-102.

¹⁴¹ Gasper, D. (2005) "Securing humanity: Situating 'human security' as concept and discourse," *Journal of Human Development* 6(2): 221-45

of human security¹⁴². Considering that several studies indicate that perceived insecurity is often unrelated to objective insecurity – indeed sometimes it is inversely correlated¹⁴³ – the danger arises that the security agenda could be hijacked by the fears and priorities of those individuals who are most influential in economic and political terms.¹⁴⁴

As we can see from this brief historical and conceptual reconstruction of security as a concept, the potential conflict between individual security and national security, as well the basic questions about security for whom and for which values, had emerged as very controversial issues well before what effectively constituted a turning point in the trajectory of security as a concept, that is the terrorist attack on the Twin Towers on September 2001. These issues, as we shall see in the next section, remained two crucial, unresolved problems of the relationship between security and democracy during the last decade. Yet, during the 1980s and the 1990s, some other crucial issues, such as for instance the relationship between security and technology, and its implications for democracy and liberty, not only had not been theorized, they had remained almost completely undetected. It was only very recently, for instance, that the impact and relevance of science and technology for international relations and security studies has been openly acknowledged¹⁴⁵. Yet, the gradual, massive development and introduction of new surveillance-orientated security technologies, which had effectively begun before 9/11 along with an increasing securitization of the EU policy agenda¹⁴⁶ was about to change our understanding of security to an extent never experienced before.

3.3 Security, technology and democracy after 9/11

*'We live in a world that holds brighter prospects but also greater threats than we have known. The future will depend partly on our actions. We need both to think globally and to act locally [...]. In an era of globalization, distant threats may be as much a concern as those that are near at hand [...]. The first line of defence will be often abroad. Conflict prevention and threat prevention cannot start too early'.*¹⁴⁷

The end of the Cold War meant the end of a bipolar system, in which two main coalitions engaged in a permanent confrontation swinging from deterrence to détente. Soon after the end of the Cold War, a new lively debate addressed again the definition of security. While during the 1990s security had increasingly focused on *human* security, emphasizing the role of integrated, global systems of international intervention to complement the effort of ineffective states in securing their citizens, the war on terrorism seems to have encouraged an explicit re-evaluation of *homeland* security into the new global context. In the multiple scenarios that emerged during the 1990s, new threats materialized as a result of the combination of objective factors, such as the transnational nature of new agents and phenomena, and subjective factors, which relate to the social construction of certain events as risky and the changing public understanding of security¹⁴⁸. In the face of global terrorism, nuclear proliferation, state failure and transnational organized crime, new approaches to terrorism and security emerged. The NATO Strategic Concept¹⁴⁹ suggested that security strategy should focus on the active management of risks, while the EU Security Strategy¹⁵⁰ called for a new security approach based on threat and conflict prevention.

More recently, the EU initiated a specific programme on 'Prevention, Preparedness and Consequence Management of Terrorism and Other Security-related Risks'¹⁵¹. Sharing a common understanding of the

¹⁴² Leaning, J. and Arie, S. (2000) Human security: a framework for assessment in conflict and transition. Washington:United States Agency for International Development/Complex Emergency Response and Transition Initiative.

¹⁴³ Mueller, J. (2006) *op.cit.*

¹⁴⁴ Pavone, V. and S. Degli Esposti, S. (2012) *op. cit.*

¹⁴⁵ Weiss, C. (2005) "Science, technology and international relations." *Technology in Society* 27(3): 295-313.

¹⁴⁶ Manners, I. (2002) *op.cit.*

¹⁴⁷ European Security Strategy (2003) *op. cit.* p. 4-5

¹⁴⁸ Coker, C. (2004) "NATO and the unbearable lightness of being," *RUSI Journal* 149(3):18-23

¹⁴⁹ NATO (1999) "The Transformation of the Alliance" in *Strategic Concept*, pp. 33-58.

¹⁵⁰ European Commission (2003) *op. cit.*

¹⁵¹ European Commission (2007) *Specific Program on 'Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks'*. Brussels 12 February 2007, Doc. 2007/124/EC.

emerging security threats, these approaches seem to be progressively abandoning traditional means-ends rationality applied to the deterrence of specific threats for a more promising *risk management* perspective¹⁵². While Cold War security approaches focused on security *dilemma*, which reduced uncertainty to calculable set of options whose outcomes were known, in a risk management perspective security policy is locked in a *paradox* where strategic choices have to be made in conditions of partially unknown probabilities and outcomes¹⁵³. Under these conditions, the pragmatic containment of security threats is being replaced by a commitment to an ideal of absolute security, which can only be accomplished through the utter eradication of the source of threat. Leading to the adoption of anticipatory approaches based on pre-emptive action to avert future probabilistic scenarios¹⁵⁴, no matter what the probability, these new security strategies seem to provoke intensification rather than reduction of terror and terrorism, as the Iraqi war demonstrates¹⁵⁵. As the 'Coalition of the Willing' shows, the combination of risk management perspectives with pre-emptive security strategies may encourage the emergence of risk communities, i.e. coalitions of national actors sharing a similar perception of global risks and common approach on how to manage them¹⁵⁶. These coalitions are *loose*, because they operate outside the formal framework of international organizations and *contingent*, as they cooperate on specific issues and grounds¹⁵⁷.

Both US and EU security strategies acknowledge the global and unpredictable nature of security threats but seek to control and dominate risks through preventive actions which rely heavily on the implementation of new technological devices, from biometrics to IT technologies¹⁵⁸. While the lobbying effort of the industry and the tight connection between economic and political interests made technology uptake a crucial factor of security policies across the globe, the implementation of these technologies may lead to a political exploitation of public fear¹⁵⁹. These transformations are encouraging the development of Western security strategies along two main directions: (a) the adoption of surveillance and pre-emptive technologies and (b) the introduction of legal provisions restrictive of civic rights and freedom¹⁶⁰.

Scholarly security studies, however, have surprisingly paid little attention to technological changes¹⁶¹. In fact, some fundamental questions have emerged since 9/11 and so far remain unaddressed. First, why has the introduction of new legal frameworks based on emergency measures, restrictive of civil rights, been increasingly associated with the introduction of new security technologies? What kind of relationship exists between the extension of security, the implementation of new security technologies and the restriction of civil liberties? What kinds of arguments have been used to justify these measures? Second, Manners¹⁶² argued that new security agendas are emphasizing 'freedom from fear' as opposed to 'freedom from want'. As fear becomes a key factor in the definition of freedom, is 'Homo metuens' replacing the 'Homo economicus' as the main reference mark of new security policies?

The emergence and development of a European Security Strategy can be better understood by keeping in mind these major changes in security agenda and security approaches. Pretty much like in any other part of the Western world, in the EU, too, security had remained confined to military strategy, diplomacy

¹⁵² Rasmussen, M. V. (2001) op. cit. Coker, C. (2002) *Globalization and Insecurity in the Twenty-First Century: NATO and the Management of Risks*. Oxford: Oxford University Press.

¹⁵³ Kessler, O. and Daase, C. (2008) "From Insecurity to Uncertainty: Risk and the Paradox of Security Politics" *Alternatives: Global, Local, Political* (April/June).

¹⁵⁴ Heng, Y. (2006) "The 'Transformation of War' Debate through the Looking Glass of Ulrich Beck's World Risk Society" *International Relations* 20(1): 69-91.

¹⁵⁵ Spence K. (2005) op. cit.

¹⁵⁶ Coker, C. (2004) op. cit. Williams, M. J. (2008) "(In)Security Studies, Reflexive Modernization and the Risk Society" *Cooperation and Conflict* 43: 57-79

¹⁵⁷ Williams, M. J. (2008) op. cit.

¹⁵⁸ Beck U. and Lau, C. (2005) op. cit.

¹⁵⁹ Zureik, E. and Salter, M.B. (2005) op. cit.

¹⁶⁰ Amoore L. and De Goede, M. (eds.) (2008) *Risk and the War on Terror*. New York: Routledge.

¹⁶¹ Eriksson, J. and G. Giacomello, G. (2006) "The information revolution, security, and international relations: (IR) relevant theory?" *International political science review* 27(3): 221-44. Levi, M. and Wall, D.S. (2004) op. cit. Rasmussen, M.V. (2006) op. cit. Weiss, C. (2005) op. cit.

¹⁶² Manners, I. (2006) op. cit.

and foreign policies during most of the 1990s. In combination with the end of the Cold War, the new emphasis on human security and the shift from territorial integrity to human development and peace building had the unwelcome effect of reducing the importance and, thus, the development and the market for military technologies¹⁶³. Given that, traditionally, the military industry was also a major player in the domain of technological research and development, which effectively implied a substantial reduction of investments in security-related technological research.

Already at the end of the 1990s, and, thus, well before the event of 9/11 a debate emerged on how to reconvert military industry and technologies into a new set of tools and instruments to foster a different type of security, that is a security no longer focused on defence strategies and requirements, less orientated towards the preservation of national integrity and more orientated towards preservation of peace, order and safety inside national borders¹⁶⁴. It was also acknowledged that the traditional separation between civil and military industry and research did not make sense any longer, as sometimes it was civil research that would first develop tools and instruments later effectively converted into military technologies¹⁶⁵. Moreover, the separation between internal and external security also did not stand unshaken any longer: religious fundamentalism, ethnic conflicts and guerrilla-type wars had well illustrated how often the sources of threats and fear would come from inside the state borders¹⁶⁶. These blurring boundaries also affected the process of securitization, which eventually influenced both internal and external security agenda, to the extent that the two, in a way, merged together¹⁶⁷.

Upon these premises, and with a view, on the one hand of taking action against the demise of the military-industrial complex, and, on the other hand, of effectively addressing what were the considered new types of threats and challenges that defied the traditional distinction between internal and external security, the EU began to develop a new and, to a certain extent unique, security strategy. It is interesting to notice that the approach adopted to address these problems was essentially an economic one, and focused on what was then framed as an excessive fragmentation of the defence markets¹⁶⁸. At the time, the main problem seemed to be that the EU defence-related industries were likely to become sub-suppliers to prime US contractors¹⁶⁹. Yet, at the beginning of the new decade, the frame of the problem was mainly still conceived in terms of how the European defence industry could actually face and overcome US competition, rather than in terms of how to reconvert the industry towards new goals, new forms of procurements and, thus, new markets. Slowly, however, the framing process shifted the emphasis from competition to research and development, suggesting that the renaissance of the EU defence industries would come from a renewed effort in R&D¹⁷⁰. This new focus found a better and more articulated expression in the first of the three EU security documents we will be revising here: the Group of Personalities final report, entitled '*Research for a Secure Europe*', published in 2004.¹⁷¹ At the same time, more or less, the EU published its first security strategy document: the 2003 '*A secure Europe in a better world*'.

¹⁶³ European Commission (1996) "The challenges facing the European Defense-Industry, A contribution for action at European Level", Brussels: COM (96), 10 1996.

¹⁶⁴ Harbor, B. (1990) "Arms conversion and military-civilian technological synergy," *Science and Public Policy* 17(3): 194-200.

¹⁶⁵ Cowan, R. and Foray, D. (1995) "Quandaries in the economics of dual technologies and spillovers from military to civilian research and development," *Research Policy* 24(6): 851-68. Eriksson, J. and Rhinard, M. (2009) "The Internal-External Security Nexus Notes on an Emerging Research Agenda," *Cooperation and Conflict* 44(3): 243-67.

¹⁶⁶ Lutterbeck, D. (2005) "Blurring the dividing line: The convergence of internal and external security in Western Europe," *European Security* 14(2): 231-53.

¹⁶⁷ Bigo, D. (2000) "Internal and external securitisations in Europe," *International Relations Theory and European Integration: Power, Security and Community*: 154.

¹⁶⁸ European Commission (1997) "Implementing a European Union Strategy on Defence-related Industry", Brussels: COM(97), 583, 1997.

¹⁶⁹ Adams, G., Cornu, C. James, A. and Schmitt, B. (2001) *Between cooperation and competition: the transatlantic defence market*. Western European Union: Institute for Security Studies.

¹⁷⁰ European Commission (2003) "Toward an EU Defence Equipment Policy", Brussels: COM (2003), 113, 2003.

¹⁷¹ European Commission (2004): "Research for a secure Europe: Report of the Group of Personalities in the Field of Security Research," Luxembourg Office for Official Publication of the European Communities.

The GOP acknowledged and refined important concepts and ideas often discussed in the academic literature and yet already circulating in the policy domain. It promoted, for instance, the blurring boundaries between internal and external security and the synergy between civil and military resources and suggested the changing nature of security threats and challenges: *'Political, social and technological developments have created a fluid security environment where risks and vulnerabilities are more diverse and less visible. New threats have emerged that ignore state borders and target European interests inside and outside the EU territory. [...] These threats call for a comprehensive security approach that addresses internal as well as external security and can combine civil and military means.'*¹⁷²

While these concepts had already been circulating in the academic debates and in some policy documents of the EU, the GOP introduced a new, and quite important, element, which will dramatically affect the meaning of the concept of security during the next decade: the role of technology: *'To achieve these goals, Europe must take advantage of its technological strengths. Technology itself cannot guarantee security, but security without the support of technology is impossible'*¹⁷³. This was going to be a crucial step: for the first time in the conceptual trajectory of the concept, security is considered impossible without technology, or, to put it differently, it becomes impossible to conceive security without technology. Obviously, military technology had always been an important component of national security, and even during the debates on human security, technological tools and instruments had never disappeared. Yet, never before had technology been conceived as a conceptually central component of security.

The GOP, in fact, went further and emphasized that security, as a concept, constituted a shared platform where civil and defence strategies converged to become one security strategy, not only because the type of security threats no longer respected national borders or predefined settings, but also because *'civil, security and defence applications increasingly draw on the same technological base'*.¹⁷⁴ Technology, thus, becomes a force enabler for a secure Europe.

In the following pages, the document stressed the importance of developing a security research agenda, with a dedicated European Security Research Programme (ESRP) that could help European security industries to develop and implement the necessary technological advances to promote security within and outside the Union borders. The PASR, the preparatory action on security research, approved in 2005 for three years, represented precisely this first step into a new direction, which eventually led the EU seventh framework programme to create a specific security section.

The GOP's novelty, though, was not limited to the central role assigned to technology with regards to European security, it also acknowledged and emphasized the emergence of new global risks and the changing nature of security. In the document, technology was also, in a way, responsible for new vulnerabilities: ICT technologies have strengthened cooperation and interdependence at global level but precisely this interdependence of *'interconnected infrastructure in transport, energy, information and other fields increases the vulnerability of modern societies'*¹⁷⁵. In the aftermath of 9/11, said the documents, our understanding of security had profoundly changed and it was deeply shaped by emerging threats, like terrorism, ethnic conflicts and organized crime, that have little to do with large-scale military aggression. New challenges, argued the documents, required new strategies and measures, among which the deployment of new security technologies featured as one of the most important. Given that new threats ignored borders and may strike in unexpected places and times and by unpredictable actors, the distinction between internal and external security ceased to be meaningful: security became an encompassing concept that had been stretched to be applied to almost every social domain.

Needless to say, the deployment of new security technologies, under this new holistic concept of security, came at a cost: a restriction of civil liberties may be necessary to ensure an effective and successful security strategy. Facing uncertain and unpredictable threats, which may strike any time anywhere as a result of the action of unexpected actors, the pursuit of security becomes a sort of never-ending endeavour whose effectiveness may require the sacrifice of very specific, concrete and long-

¹⁷² Bukard Schmitt, et al. (2004) *op. cit.* p. 7

¹⁷³ Ibid, p.7

¹⁷⁴ Ibid

¹⁷⁵ Ibid, p.9

standing civil rights and liberties. To put it differently, security and liberty, in what then constituted a novel conceptual twist, get framed as two interchangeable goods that can be traded against each other: any increase in security requires an equivalent contraction of civil liberties. In the GOP's words: 'Striking the right balance between security and freedom will be a permanent challenge while respecting the highest ethical principles'. Although the idea of exchanging liberty for security had been already discussed and criticized by Benjamin Franklin in 1755¹⁷⁶, the GOP was one of the first contemporary policy documents to explicitly propose the trade-off between security and liberty as a benchmark for security policy.

Beside the role of technology, the redefinition of security threats, the expansion of security into an holistic concept and the formulation of the trade-off between security and liberty, the GOP report accomplished one more important conceptual task: it proposed and endorsed a technological fix approach to the problem of security. In the document, the threats were collected and defined and then the only question asked remained: 'Which technologies do we need to successfully address these challenges?'. The focus, thus, shifted completely from the search for a (complex) variety of causes and factors that had produced the on-going transformation of security threats to the (simple) series of technological remedies that could be conceived, developed and implemented to keep these challenges under control. In the GOP's words: '*What are the threats? What are the missions required to tackle these threats? What are the capabilities needed to accomplish these missions? What are the technologies – or combination of technologies than can provide the necessary capabilities?*'¹⁷⁷ Needless to say, the more multifunctional were the technologies to be developed (where multifunctional means that they could be applied to both military and civil needs), the better they were because multi-functionality increased marketability of technological products.

It may seem inappropriate to have addressed this report, which chronologically followed the first EU Security Strategy, in a section on security, technology and democracy after 9/11. However, there are two main reasons why this EU document has been addressed here. First, it is not, technically speaking, a security policy document, but rather a research policy document. Second, it was among the first documents that really brought to the fore the constitutive role of technology in the redefinition of security. Third, it well illustrates the economic drivers behind the conceptual changes in the meaning of the term security, which normally do not come to the fore in security policy documents. Finally, it shows how some key features of the new concept of security – such as the blurring boundaries between internal and external security, or the trade-off between security and liberty – proceed also from economic and commercial concerns and interests. As it is now clear, it would have been impossible, really, to address the trajectory of security as a concept without taking into account the constitutive role of security technologies and industries.

3.4 Pre-emptive security and the trade-off between security and liberty: the EU security strategy (2003-2010)

Although the EU security research is still restricted mostly to internal security, the European Security Strategy is a relatively recent attempt made by the EU to integrate defence and foreign policies with internal security. As previously mentioned, it came to life as a response to a changing landscape of security threats, but also as a response to a changing understanding of what security was and a changing role of nation states, technologies and globalization. It incorporated the need for a more integrated strategy coordinating internal and external security actions, the economic drivers of new security markets for the EU military-industrial complex¹⁷⁸ and the increasing overlap between civil and military research and development policy.

¹⁷⁶ 'Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety'. Benjamin Franklin "Pennsylvania Assembly: Reply to the Governor", November 11, 1755; as cited in The Papers of Benjamin Franklin, v. 6, p. 242, Leonard W. Labaree, ed. (1963).

¹⁷⁷ Ibid. p.17.

¹⁷⁸ Haggerty, K.D. (2010) *Surveillance and democracy*. Cavendish Pub Limited. Hayes, B., Rowlands, M. and Buxton, N. (2009) *op. cit.*

The first European Security Strategy document was issued in 2003, as a result of previous work done in commissions and workshops to develop the concept of security. The EU strategy took its start from the Oxford dictionary definition of security, whereby security is defined as 'the condition of being protected from or not exposed to danger; [...] a feeling of safety or freedom from or absence of danger'.

Also described as 'freedom from fear', security thus clearly contains a subjective element, an element of perception, which has been elsewhere defined as 'confidence in the future'. Security policy, in the document, is a policy that aims to keep the EU values and interests safe, while the strategy is a policy-making tool that outlines the long-term overall policy objectives to be achieved and the basic categories of instruments to be applied to that end. It serves as a reference in a rapidly evolving and increasingly complex international environment and it guides the definition of the means that need to be developed¹⁷⁹.

The first debates on a common security strategy began to be organized at the end of the 1990s, along with the launch of the European Security and Defence Policy (ESDP). The debates emerged during the elaboration of the ESDP were essentially focused on how to arrange a common complex and yet effective military framework for the whole Union, when it was clear that no common strategic vision existed. In the years that witnessed the climax of multilateralism and in the face of the Kosovo and Balkan crisis, the EU external action lacked direction, determination and consistency. As Biscop suggests, without a clear strategy of its own, the EU could not escape the American framework of thought and had no way to promote its own policy priorities. The European Security Strategy formulated in 2003 also constituted an attempt to elaborate an approach to security alternative to the US reaction to 9/11. It drew consistently, especially at the beginning, from the ideas and principles associated with the human security framework to formulate a concept of comprehensive security¹⁸⁰. Comprehensive security contemplates a multidimensional concept of security where the political, the socioeconomic the cultural and the military dimensions are interdependent, and therefore focuses on dialogue, cooperation and partnership, or *cooperative security*.

Before 9/11, the EU strategy was still very much in line with the human security discourse. In its 2001 *Communication on Conflict Prevention*, the Commission was still orientated towards the 'root causes of conflict' and aimed at achieving 'structural stability', a concept that implied sustainable economic development, democracy and respect for human rights, viable political structures and healthy environmental and social conditions, with the capacity to manage change without resort to conflict. In this document, the echoes of peace-building and peace-keeping, as well as the principles of human security and human development were still fresh and valid, but the subsequent documents, written after 9/11 show a gradual yet firm shift towards a different concept of security, more orientated towards pre-emptive action, risk assessment and technological deployment.

At first, the EU called for 'an in-depth political dialogue with those countries and regions of the world in which terrorism comes into being' and 'the integration of all countries into a fair world system of security, prosperity and improved development'¹⁸¹. Although the dramatic impact of 9/11 gave an extraordinary impulse to the elaboration of a common strategy, the main challenge remained how to elaborate a strategy that could be alternative to the US and still preserve transatlantic cooperation in the face of the terrorist challenges. The task of elaborating and proposing a background document for the EU strategy was assigned to Javier Solana, who presented 'A Secure Europe in a Better World' at the European Council in Thessaloniki. This document constituted the benchmark for the first European Security Strategy, which was published in December 2003.

The ESS of 2003 emphasized the importance of globalization as the driving force behind the on-going transformation of security threats and challenges, stressing also the importance of the world's stability for Europe's security. The document acknowledged the vulnerability of European citizens and

¹⁷⁹ Biscop, S. (2004) *The European security strategy: implementing a distinctive approach to security*: Centre d'etudes de Defense.

¹⁸⁰ Biscop, S. (2005) *The European Security Strategy: A global agenda for positive power*. Ashgate Publishing Company. Rieker, P. (2006) "From Common Defence to Comprehensive Security: Towards the Europeanization of French Foreign and Security Policy?" *Security Dialogue* 37(4):509-28.

¹⁸¹ European Commission "Communication on Conflict Prevention" Brussels: COM (2001), 211, 2001.

infrastructures as a result of a changing nature of security threats, which could no longer be confined and contained by national borders. It was actually more than that, as security threats like terrorism did not fade with geographic distance: the security of the US was key to the one in Europe and vice versa.

According to Biscop, the 2003 ESS did represent a security strategy almost opposite to the US one. While the Bush administration emphasized, under a new perspective based on pre-emption, the importance of national sovereignty and national interests, which constituted a big shift away from multilateralism, the EU policy reaffirmed the importance of multilateralism and comprehensive security. However, if compared to the US counterpart, the EU Security Strategy and agenda tried to adapt and reconsider multilateralism and human security in the new context this does not really imply that the US and the EU emerged as two opposite strategies. Pretty much like the US strategy, the EU 2003 document was also overly threat-based and overestimated the impact and relevance of terrorism and transnational organized crime, and reinforced the importance of defence and military strategy. Moreover, as Biscop acknowledged, the links between the five key threats and globalization was also overemphasized, but no consistent effort was devoted to an in-depth analysis of the social and political dynamics that facilitated the emergence of the identified key threats. Finally, the EU document flipped upside down the basic principles underlying the human security paradigm, by affirming that security is a precondition for development without also acknowledging that there cannot be security without development either.

A closer look at the policy documents reveals a few important changes, compared to the situation in the EU before 9/11, which will, over the years, mature and develop along with the very concept of security, as we can see in the last EU security document, the 2011 EU Internal Security Strategy. In effect, the opening of the document emphasized the importance of peace, prosperity and cooperation, which has characterized the action of the EU in the previous 50 years. These past actions in favour of peace and prosperity are interpreted precisely as a call to assume the responsibility for global security as a global player. Two main concepts make their way in the first pages: the indissoluble link between internal and external security and the relationship between global integration, increased dependence and, thus, increasing vulnerability.

In this context, security becomes a precondition for development: if infrastructures, energy, information and transportation are increasingly interconnected, this interconnection increases their vulnerability as an attack in any section of the network will inevitably affect all the network as such. Increasing vulnerability, as the EU suggests, jeopardizes development.

Increasing vulnerability, though, does not proceed exclusively from increased dependence and interconnection, it is also due to a shifting nature of key security threats: *'In an era of globalization, distant threats maybe as much a concern as those that are near at hand.'*¹⁸² New threats like terrorism, organized crime and proliferation of weapon of mass destruction (WMDs) constitute different risks, compared to traditional large-scale military aggressions: they could strike anywhere, at anytime, without premonitory signs and with a full-scale power, and they are difficult to track, or to predict and require a different approach. In the document words: *'Taking these different elements together – terrorism committed to maximum violence, the availability of WMDs, organized crime, the weakening of the nation states and the privatization of force, we could be confronted with a very radical threat, indeed'*¹⁸³.

The shifting nature of these new threats and the increasing interconnection associated with globalization required a new approach, now focused on threat prevention: *'Our traditional concept of self-defence [...] was based on the threat of invasion. With the new threats the first line of defence will often be abroad. The new risks are dynamic [...] this implies that we should be ready to act before a crisis occur. Conflict and threat prevention cannot start too early.'*¹⁸⁴ Threat prevention however was no longer intended as it was traditionally understood during the 1990s, that is as a strategy to address the underlying causes of conflicts, like poverty, marginalization, religious fundamentalisms or political tensions. The emphasis began to shift and focus on the work of intelligence and investigation, with a

¹⁸² European Commission "A Secure Europe in a Better World – European Security Strategy", Brussels: COM (2003).

¹⁸³ Ibid. p. 6

¹⁸⁴ Ibid. p. 8

view of gathering enough information to be able to stop the attack before it would actually be delivered: *'Dealing with terrorism may require a mixture of intelligence, police, judicial, military and other means'*¹⁸⁵. Prevention here, and more so in the next two documents, meant prevention of the acts rather than prevention of the causes underlying the perpetration of the act. While the approach to failed nation states and ethnic conflicts still followed the traditional approach based on economic support, democracy and diplomacy: *'The best protection for our security is a world of well-governed democratic states'*⁰; the approach to terrorism and organized crime progressively converged towards the US pre-emptive approach.

This metamorphosis of security and security strategy can already be seen in the European Security Strategy update, which was published in 2008. In this document, which was a report on the implementation of the 2003 policy strategy, global warming, environmental degradation and the economic crisis made their way into the security threats scenario, expanding security concerns and action into previously not securitized domains. A closer look at the anti-terrorist strategy, for instance, reveals a growing reliance on security technologies and a wider adoption of pre-emption as the dominant paradigm. One reason for that, as the document itself suggests, is that by 2008 terrorism had struck in Europe, too. The EU counter-terrorism strategy was then arranged into a set of four actions: prevention of terrorist attacks, protection of civilians, prosecutions of terrorists and response in the aftermath of attack.¹⁸⁶ The implementation of these four actions required increasing reliance on new security technologies: *'Further work on terrorist financing is required, along with an effective and comprehensive EU policy on information sharing, taking into due account of protection of personal data.'*¹⁸⁷ This passage, together with the following one, where cyber-security appears as a new cornerstone of the EU Security Strategy, not only reveals the importance acquired by security technologies surveilling, storing and exchanging personal data of EU citizens, it also admittedly shows the increasing conflict between the deployment of dataveillance and personal and information privacy, a scenario announced by the GOP document five years earlier. Moreover, new domains get reframed in terms of security agenda and issues, such as energy policy. Securing energy becomes a new security objective, expanding security as a concept and securitizing energy at the same time. The nexus between poverty eradication, economic development, democracy and security is maintained as a cornerstone of the EU Security Strategy vis-à-vis the management of ethnic conflicts and failing states, but it seems to stand somehow in isolation from the strategy pursued against terrorism, organized crime and proliferation of WMDs.

The 2010 Internal Security Strategy represents a cornerstone not only in the evolution of a new European approach to security but also in the very transformation of the concept of security. It contains in a well-organized and systematic way all the major shifts and conceptual changes affecting the trajectory of security as a concept over the past decade. It shows how surveillance-orientated security technologies (SOSTs) became key elements of the EU Security Strategy and how the trade-off between security and civil liberties became the dominant framing device to address the relationship between security and liberty, often in a context characterized by a growing implementation of new SOSTs and a parallel restriction of citizens' liberties and rights and often through an incessant curbing of individual privacy. It also shows, however, how the tension between liberty and security, triggered by the adoption by the trade-off approach begins to be questioned by the need to reconcile liberty and security as they are both key values of the EU constitutional design. Nonetheless, it finally shows how pre-emptive monitoring and control and risk management-orientated policy actions remain the dominant approach of this newly re-conceptualized security culture.

The document begins by stressing the role of technological advances in opening our societies and the importance of reaching a *'larger consensus on the vision, values and objective that underpins the EU internal security.'*¹⁸⁸ The European internal security strategy, the document affirms, demonstrates a firm

¹⁸⁵ Ibid. p. 8

¹⁸⁶ Council of the European Union "Report on the implementation of the European Security Strategy – Providing Security in a Changing World", CAB66, 17/04/2008.

¹⁸⁷ Ibid. p. 7

¹⁸⁸ Council of the European Union "Draft Internal Security Strategy for the European Union: Towards a European Security Model" (Brussels, DG H, 7120/10) p. 2.

commitment to making progress in the areas of justice, freedom and security through a *European security model* that needs to protect rights and freedom, to address the causes of insecurity and not just the effects, prioritizing prevention and anticipation [...] and establishing a global security approach with third countries.

The new European security model implies an expansion of security threats and domains, which implies a further advance in the process of securitization of policy domains that traditionally fell under the competence of ordinary political, democratic debates. Apart from terrorism, the proliferation of WMDs, organized crime, rogue states and ethnic conflicts, the EU security model now considers child pornography, drug-trafficking, cross-border crimes and illegal migration, economic crime and corruption, cyber-crime, man-made and natural disasters, energy procurement, environmental and infrastructure protection as issues and topics of security policy. In the document terminology: *'the concept of internal security must be understood as a wide and comprehensive concept which straddles multiple sectors in order to address these major threats and others which have a direct impact on the lives, safety, and well-being of citizens, including natural and man-made disasters such as forest fires, earthquakes, floods and storms'*.

In the document, we can detect a new emphasis on *'protection'*, be it the protection of values, infrastructures, cyber-communication or people's physical integrity. Ordinary crime, money counterfeiting, undocumented migration or even road traffic accidents cease to be an issue of justice or social integration and become an issue of security concern. As such, they are re-framed with urgency and exceptionality and subjected to a new approach that emphasizes threat anticipation: *'Our strategy must therefore emphasize prevention and anticipation, which is based on a proactive and intelligence-led approach as well as procuring the evidence required for prosecution. It is only possible to bring successful legal action if all necessary information is available'*. Threat anticipation often implies the deployment of surveillance and action before the crime is actually committed: *"While effective prosecution of the perpetrators of a crime remains essential, a stronger focus on the prevention of criminal acts and terrorist attacks before they take place can help reduce the consequent human or psychological damage which is often irreparable'*.

In a regime of threat anticipation, risk assessment and risk management emerge as the dominant approaches to security analysis: *'For this reason, a comprehensive approach must be taken that is geared to constant detection and prevention of the threats and risks facing the EU in the various areas of internal security, and the main issues of concern to the public.'* The new approach, which aims at detecting, analysing and evaluating risks and threats, trying to anticipate their trajectory and impact, is conceived as a broad, pragmatic and realistic approach that should not focus merely on criminal aspects but on risks of any kind: security is expanded here well beyond the criminal domain into any sort of suspicious behaviour, information or action that could potentially constitute a threat even if it is not illegal or criminal as such: *'(we need) a broad, pragmatic, flexible and realistic approach, continually adapting to reality, taking into account risks and threats which could impact on citizens in a wider perspective, not focusing only on criminal aspects but taking into account risks of any kind which might create a security problem in the broader sense.'*

From the perspective of threat anticipation and risk-assessment, the monitoring and surveillance of people's movements, actions, communications and transactions become a crucial component of security responses, which, in turn, makes surveillance technologies a necessary tool of such security responses. For instance, the case of border control is emblematic: *'New technologies play a key role in border management. They may make it easier for citizens to cross quickly at external-border posts through automated systems, advance registration, frequent-traveller schemes etc. They improve security by allowing for the necessary controls to be put in place so that borders are not crossed by people or goods which pose a risk to the Union'*. While undocumented migration, as such, has not been proven to constitute any threat for national or human security, clearly, in order to securitize border control and migration processes it is necessary to reframe migrants into potential criminal subjects constituting a security threat. As such, they can be considered a matter of political urgency and exceptionality, and subjected to a restriction of civil rights and to the legitimate deployment of SOSTs. Yet, the securitization of people's movements and actions is not confined to migrants, as the EU security model aims at controlling and integrating all sorts of information databases about ordinary citizens: *'The (European Security) model will include all the*

different EU databases relevant for ensuring security in the EU [...] for the purpose of providing effective information exchange across the whole of the EU and maximizing the opportunities presented by biometric and other technologies for improving our citizens' security within a clear framework that also protects their privacy'.

These technologies, as previously discussed are often surveillance-orientated technologies, and the EU strategy explicitly plans to use them in all their width *'Data bases such as the Schengen Information System and networks have also been established for the exchange of information on criminal records, on combating hooliganism, on missing persons or stolen vehicles and on visas which have been issued or refused. The use of DNA and fingerprint data helps put a name to anonymous traces left at crime scenes'.* And also in all their depth: *'If law-enforcement authorities are to be able to prevent and act early they must have timely access to as much data as possible.'*

Expansion of security agenda, securitization of several societal domains, threat anticipation and pre-emptive action, massive use of SOSTs and risk-orientated analysis and responses emerge, therefore, as key elements of the new European security model formulated in the European internal security strategy. The combination of these characteristics makes the trade-off between liberty and security almost inescapable, or so it is presented anyway: *'This information exchange model must always fully respect the right to privacy and protection of personal data. If a higher level of security means an increase in data exchange, it is important that that increase be managed carefully, that it be proportionate and that it respect data protection laws.'*

The trade-off approach takes it for granted that any increase in security levels need to be accompanied by a reduction in civil liberties. This is essentially due to the fact that the increase of security levels is intrinsically associated with an ever-increasing implementation of surveillance technologies and with a strong emphasis on pre-emptive action. It does not consider possible, for instance, that it could be possible to increase security levels through either non-surveillance-orientated technologies or through non-technological actions and interventions. It also does not believe it reasonable to adopt a reactive approach instead of a proactive one, even if the latter clearly clashes with a basic principle of the European Charter of Rights: the presumption of innocence.

Aware of these implications, EU policymakers have usually accompanied the trade-off approach with an emphasis on shared consensus and values: *'The values and principles established in the Treaties of the Union and set out in the Charter of Fundamental Rights have inspired the EU's Internal Security Strategy: [...] transparency and accountability in security policies, so that they can be easily understood by citizens, and take account of their concerns and opinions. [...] dialogue as the means of resolving differences in accordance with the principles of tolerance, respect and freedom of expression'.* As a result, some the characteristics and implications of these technologies and to explore to what extent and under what conditions these technologies are acceptable and what criteria and factors make them so in the eyes of the European citizens. Most of these exercises, however, have used the same trade-off as a starting point, asking citizens to state how much of their privacy and liberties they would be willing to renounce in exchange for the increase of security provided by the new technologies. In this way, the trade-off not only underpinned the security policies formulated in the past ten years or so, it also came to underpin the very same technology assessment exercises that were supposed to assess and evaluate these policies. In doing this the trade-off approach effectively disappeared unperceived into the background and was not itself part of the evaluation processes. In turn, it became a cornerstone of security policies and, to date, it is still taken for granted¹⁸⁹. While the influence of the trade-off approach in technology assessment exercises will be dealt with more in depth in the next chapter, here we will address the political implications of the new nexus between pre-emptive security, surveillance technologies and the trade-off between liberty and security.

Before engaging with this issue more in detail, however, it is important to take a look at the national security strategies, which had been developed by a number of European countries in response to the on-going debate and policy developments at the Union level.

¹⁸⁹ Pavone, V. and Degli Esposti, S. (2012) op. cit.

3.5 Security, technology and democracy: national developments and public debates

In general, security is always focus in protection of individuals and the state, central to the idea of internal security is the concept of public order (the regular course and good order of civil living), security issues arise in a number of different areas, but in each case it arises in relation to material ties or persons that are considered potentially vulnerable. Security, as a concept, also varies according to the field, the actors and the national socio-political context in which it is used. Despite a plethora of attempts to define security, to date there is no shared definition: the meaning of security changes according to those who make use of it and depending on the social domain where it is used (national security, cyber-security, people's security, infrastructure security, etc.)

If we need to define security more specifically, we must take into account the specific historical and cultural differences between countries that directly relate to the way in which security is framed. Also the evolution of the social values and the role of the media lead us to a new characterization of the idea of security of the European States. Moreover, in the post 9/11 world, security is regarded as a prerequisite and a precondition for the proper functioning of the advanced democracies *'Security in all its dimensions is a precondition for the functioning of a constitutional democracy and the economic well-being of society and citizens [...] Austria has its strategic course in security policy in several aspects: security is defined as holistic concept'*¹⁹⁰. Considering all these issues, general and specific, a closer look at the national feedbacks confirms the trends about the recent changes in the security concept.

The National Security Strategies reflected the changes in this field have been living in recent years in Europe and tried to adapt legislation to shifting conceptual transformations, as we have seen in the previous section. The Italian strategy, as formulated in the document 'Relazione sulla Politica dell'Informazione per la Sicurezza 2011' shows the essential interest in the combination of economic crisis and system vulnerability, the reappearance or subversion, the internal impact of external challenges, such Arab spring, as for global challenges as the cyber threat and finally, environmental threats. In its Report on Security 2010, the Swiss government states that *"[security policy] refers to the right to self-determination of the nation and of the individual, to the integrity of the state and to the individual conditions of life and prosperity"*¹⁹¹. The fear of terror, instead, has had a remarkable impact on the Danish legislation on security and surveillance since the attacks on the New York World Trade Centre in 2001.

In general terms, pretty much like the EU counterpart, new national security strategies tend to be holistic, which is a transformation that has indeed caused controversies. In Austria, civil society organizations have protested on the grounds that the new security strategy is guilty of political opportunism and subjected citizens to excessive surveillance: *'The Austrian security strategy had strongly been criticized by several institutions such as Austrian Research Centre to Peace and Conflict Solutions (ÖSKF). The Centre, inter alia, criticized the strategy for being too imprecise: due to the use of different and sometimes even conflicting terms and concepts of security the strategy document remained open for political opportunism. The strategy focus towards a comprehensive/holistic security concept entails the threat of totalizing security policy resulting in a surveillance state'*¹⁹².

Furthermore, the fact that security is increasingly dependent on the development and implementation of new surveillance-orientated security technologies (SOSTs) has produced, in some cases, legislation and national security strategies that are hasty and poorly designed, so that instead of helping to solve an existing problem caused a new conflict, the rush for new technological security solutions has undermined sometimes precisely the values these technologies were supposed to protect. In some cases, these security strategies have been misused or poorly designed and political authorities responsible for designing policies and regulative legal frameworks have not produced appropriate legislation: *'The creation of legal frameworks is often mis(used) to create a legal basis for SOSTs without aiming at designing the legal regulations to reduce the controversial and problematic aspects of the*

¹⁹⁰ <http://www.bka.gv.at/site/3503/default.aspx>

¹⁹¹ <http://www.news.admin.ch/NSBSubscriber/message/attachments/22860.pdf>

¹⁹² <http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=47986>.

technology and towards privacy-respecting implementations'. The lack of appropriate and effective legislation runs the risk of paving the way to excessive surveillance as the UK Information Commissioner warned with their emphasis on the risk of sleepwalking into a surveillance society¹⁹³.

In many ways, the broader spectrum of changes in the concept of security and deployment of security policies and technologies is well expressed in the UK's approach to national security. The latter is overseen by the National Security Council and detailed in the National Security Strategy (NSS) (2010). The implementation of that strategy is considered in *The Strategic Defence and Security Review* (SDSR) (2010). *The Strategic Defence and Security Review* outlines a series of security tasks and planning guidelines designed to implement the National Security Strategy: (1) Identify and monitor national security risks and opportunities; (2) tackle at root the causes of instability; (3) Exert influence to exploit opportunities and manage risks; (4) Enforce domestic law and strengthen international norms to help tackle those who threaten the UK and our interests, including maintenance of underpinning technical expertise in key areas; (5) Protect the UK and our interests at home, at our border and internationally, to address physical and electronic threats from state and non-state sources; (6) help resolve conflicts and contribute to stability; (7) provide resilience for the UK by being prepared for all kinds of emergencies, and able to recover from shocks and to maintain essential services, (8) Work in alliances and partnerships wherever possible to generate stronger responses.¹⁹⁴

The introduction of the risk and crisis management principles has been the most important change in Norwegian internal security and safety policy since the Cold War. The Norwegian security strategy is now based on three *central principles: liability, decentralization and conformity*. The liability principle implies that every ministry and authority has responsibility for internal security and safety within its own sector. The decentralization (or subsidiarity) principle emphasizes that a crisis should be managed at the lowest operational level possible. The principle of conformity emphasizes that organizational forms in a crisis or a crisis-like situation should be as similar to 'normal organizational' forms as possible¹⁹⁵. Decentralization is also a priority issue in Germany where the historic experience of repressive regimes has some specifics in regard to the structuring of governmental bodies and institutions as the separation police and intelligence agencies and separation of police bodies on federal and regional levels.

Despite their nationally specific approaches, the different historical trajectories and the inevitable cultural elements present in each of the national security strategies, it is possible, especially if we compare them to the EU Security Strategy, to identify some common trends. A closer look at the trajectory of the European Security Strategy, as discussed in the previous section, suggested that **security is an expanding concept**. National security strategies in Europe confirm this trend, and endorse the idea that security in Europe has suffered a global shift, is no longer a concept with clearly defined boundaries and has become an even more complex concept, a multidimensional and multidisciplinary concept covering new fields such as the environmental and economy challenges, terrorism threats, etc. This expansion is, for instance, especially visible in the Italian security Strategy. *The 'Documento Programmatico Sulla Sicurezza 2012-2014'* defines internal security issues and priorities as follows: *'First the thriving of domestic and international crime, with its impact on economic activities, and the persistence of national terrorism, as well as international terrorism; second is the constant influx of migration from North Africa, in particular illegal migrants; third comes the diseases/pathologies affecting security/safety of the territory, such as the retrogression of urban centres, the persistence of certain crimes, road accidents, the deterioration of orderly civil co-habitation; fourth are the problems relating to the economy; then come environmental challenges and, finally, the public deficit'*.

¹⁹³ <http://www.surveillance-studies.net>.
<http://www.publications.parliament.uk/pa/cm200708/cmselect/cmhaff/58/58i.pdf>.
<http://www.publications.parliament.uk/pa/7ldselect/ldconst/18/1802.htm>.

¹⁹⁴ The UK's approach to national security is overseen by the National Security Council and detailed in the National Security Strategy available at:
http://www.direct.gov.uk/prod_consum_dg/groups/dg_diitalassets/@dg/@en/documents/digitalasset/dg_191639.pdf?CID=PDF&PLA=furl&CRE=nationalsecuritystrategy

¹⁹⁵ <http://www.regjeringen.no/nb/dep/jd/dok/regpubl/stmeld/2007-2008/stmeld-nr-22-2007-2008-.html?id=510655>

The expansion of the security agenda, and the securitization of new policy domains, requires a renewed effort to preserve security in the European States working in co-operation within and between the different territorial levels (regional, national and supranational). The Spanish national security strategy, for instance, suggests that preserving security requires co-ordination, both international and internal, as well as contribution by society overall. The limits between interior and exterior security have become faded and therefore only an integral focus, that conceives security broadly and in an interdisciplinary manner may tackle the complex challenges we are facing. The same trend can be observed in Switzerland, where since the end of cold war, non-military dangers have been integrated within the security policy and where strategies strive for more multilateral coordination as well as for a reinforcement of the links with the Cantons and municipalities in charge of the personal security of individuals through police forces: *"According to the 2010 security report of the Swiss government, security policy covers all measures taken by the government, the cantons and municipalities to prevent, remove and control threats and politico-military or criminal actions aiming at limiting the power of self-determination of Switzerland and of its people or harm them. It also includes the management of natural and anthropogenic and other emergencies."*¹⁹⁶ This decentralization, in some cases, is associated with secondary effects such as the difficulty of communications between the various agencies responsible for safeguarding the security at various levels and the lack of transparency in the communication between them. This runs the risk of effectively hindering security policies and actions, especially when coordination between national, European and local forces is crucial. In some cases, where different branches of police and security forces exist, like in Italy, the problem may constitute a serious obstacle not only in achieving effective security activities but also in preventing the performance of these activities with the necessary transparency and accountability.

The EU internal security strategy showed how the expansion of the security agenda and the securitization of energy, immigration and environmental policies are being accompanied by a parallel emphasis on a new type of security, which is about **pre-emption and threat anticipation**. This new emphasis can also be retrieved in various national security strategies. In Austria, for instance, prevention and pre-emption are positioned as the main objectives in the development of the new Austrian new security strategy: *'New ways in prevention/pre-emptiveness is an explicit objective of the new security strategy. (...). There is a global shift of security and law enforcement authorities towards more pre-emptive state mechanisms'*.¹⁹⁷ This orientation and effort towards prevention has justified, in some cases, the expansion of wiretapping in Italy, something that would be seriously sanctioned by the citizens if they believed that these surveillance technologies had not been deployed for the exclusive purpose of the preservation of security and crime prevention. A similar situation has emerged in Germany, where intelligence services have competences to initiate the surveillance of letters and communications but are solely bound to the preventive defence of existential state security and to the principle of individual investigations.

Pre-emption and expansion have been also increasingly associated to the re-framing of security in terms of **risk assessment and risk management**. This is especially clear in the Norwegian security strategy. Taking into account the nature of the new security threats, the Norwegian security strategy suggests the introduction of new management skills and a new frame from which to approach threats: *'The most important change in Norwegian internal security and safety policy since the Cold War has been the introduction of the risk and crisis management principles'*.¹⁹⁸

If science, technology and social order are co-produced, as Jasanoff suggests, we would not be surprised to find out that expansion, securitization, pre-emption and risk assessment come in a mutually constitutive relation with security technologies, and more specifically surveillance-orientated security technologies. This mutually constitutive relation has produced an interesting paradox. On the one hand, the technologies, related to security and privacy, have so far received in general a significant level of support, because they are expected to improve the level of personal protection as well as the protection of goods and properties. On the other hand, the increasing complexity of security

¹⁹⁶ <http://www.news.admin.ch/NSBSubscriber/message/attachments/22860.pdf>

¹⁹⁷ <http://www.bka.gv.at/site/3503/default.aspx>

¹⁹⁸ <http://www.regjeringen.no/nb/dep/jd/dok/regpubl/stmeld/2007-2008/stmeld-nr-22-2007-2008-.html?id=510655>

technologies raises a sense of anxiety; generally connected with the risk of abuse that such a complexity may carry: *'technologies, with a proper control, might indeed improve the level of security in given areas of people's life'*¹⁹⁹. Whether security increase is effectively related to the development and implementation of new technologies, however, remains strongly controversial because there is no empirical evidence that SOSTs have a positive impact. See for example the case of the controversy in the UK with CCTV: *'In the UK the assertion that more data collection and analysis, more cameras, more surveillance is equivalent to more security is challenged. New forms of surveillance create new vulnerabilities, and therefore new insecurities'*.²⁰⁰ A similar situation occurred in Germany with the test of body scanners at the airports: *"The benefit of such technologies to airport security could not be proven unambiguously, thus leading to the termination of the test deployment in Hamburg in July 2011."*²⁰¹ Alternative strategies for a non-technological orientated surveillance are being developed in some countries precisely as a response to these controversies. The highest profile campaign which promoted a non-technological surveillance for security purposes is the London Metropolitan Police's *'Individuals were encourage to look out for suspicious houses, suspicious behaviour on public transport, and to be suspicious of those taking photographs'*.²⁰²

The trade-off approach is no less influential at national level than it is at the European one. In Denmark, surveillance is explicitly considered acceptable only when it is used in preventing and solving crimes, but not when it comes too close to the private sphere; near the home or at the workplace²⁰³. At the same time, surveillance could be accepted if it is used in the proper way as the instrument to guarantee and achieve the conditions for liberty, even if it comes at the expense of 'some liberty'.²⁰⁴

3.6 Implications and conclusive remarks

The concept of security has been changing over the past 50 years. Nonetheless, and despite several attempts to define the concept, security remains an essentially contested concept that may acquire different meanings, implications and features depending on where it is used, by whom and in relation to which threats. National elements, cultural peculiarities and historical events add a further layer of variability and complexity. The complexity is further increased by the existing difference between perceived and actual security, as the perception of being safe is not always or inevitably associated with an actual decrease of risks and threats. Besides, the concept keeps maintaining blurring boundaries with other terms, like safety or integrity. For these reasons, perhaps the best way to approach security as a concept is not through an abstract philosophical enquiry on its potential meanings and on the theoretical background of each of them. It seems impossible to achieve or formulate a universally valid and exhaustive definition of security as a concept. Our suggestion, therefore, was to try to follow the trajectory of the concept through time and space, focusing not so much on the variety of definitions proposed but on the complex bundle of ideas, principles, practices and relations that have emerged around the practical use of the concept at each point in time and space. We have therefore tried to cast light on security as a concept considering security as a practice. Like all sorts of practices, the best way to approach them remains the study of what is done with them, how, where and with what implications.

In this chapter, reviewing the literature of security studies and in international relations, we have identified three main paradigms of security, which, in spite of diverging definitions and emphasis, may have temporally converged on a common understanding of the basic characteristics and boundaries of

¹⁹⁹ Pavone, V. and Degli Esposti, S. (2012) *op. cit.*

²⁰⁰ McCahill, M. (2012) Surveillance, Crime and the Media in Ball, K, Haggerty, K. and Lyon, D. (eds.) *The Routledge Handbook of surveillance Studies*. London: Routledge.

²⁰¹ Spiegel online news article published August 31 2011, Flugsicherheit: Nacktscanner versagen im Praxistest, available at:
<http://www.spiegel.de/reise/aktuell/flugsicherheit-nacktscanner-versagen-im-praxistest-a-783550.html>.

²⁰² [http://www.epuk.org/Blogs\(825/thousands-of-people-produce-parodies-every-day](http://www.epuk.org/Blogs(825/thousands-of-people-produce-parodies-every-day) Accessed 5th October 2012

²⁰³ Lauritsen, P. (2011) *Big Brother 2.0*. Information Forlag)

²⁰⁴ Campesi, G. (2009) *Genealogia della pubblica sicurezza. Teoria e storia del moderno dispositivo poliziesco*. Verona: Ombre Corte.

the concept. During the Cold War, security was a term mainly associated with the preservation of national sovereignty and territorial integrity of nation states, and was essentially linked to military strategy, technology and defence policies. The collapse of the Berlin Wall made this paradigm obsolete: as time passed, the likelihood of a territorial attack or the emergence of a threat to national sovereignty eventually became insignificant while the relevance of nation states as the dominant actors in international relations was also challenged. Globalization, the emergence of NGOs and multinational corporations, together with the renewed role played by the UN and its satellite agencies, like UNESCO, paved the way to a new understanding of security. In this new perspective, also known as *human security*, the importance of multilateral actions, aid to development, the spread of humanitarian intervention and the UN operations of peacekeeping and peace building became crucial aspects of security strategies and policies. From a human security perspective, security, which was no longer based only on the freedom from fear but incorporated freedom from want as a major component, could be best achieved through multilateral cooperation, a mixture of diplomacy and military intervention and always with a specific support action directed at relieving populations from poverty, marginalization, authoritarian rule and extreme environmental conditions. The human security approach remained the dominant paradigm until the terrorist attack on the Twin Towers gave a fresh and dramatic impulse to a quiescent debate. The vivid images of the aeroplanes crashing into the World Trade Center made human security obsolete with the same speed that the crumbling down of the Berlin Wall made national security obsolete 20 years before.

New approaches to security emerged, first in the US, so tragically hit by the attack, but later also in the EU, which experienced the drama of terrorist attacks four years later in London and Madrid. This new approach, as we have seen in the section on the European Security Strategy, is characterized by a number of novel principles and characteristics, which no doubt have crucial implications on the relation between security, technology and democracy. The security agenda is expanding, incorporating new social policy domains previously free from the security concerns and rules: migration, organized crime, social integration, environmental management, energy policy and even Internet navigation have become integral parts of security policy. This expansion is not merely to be understood in terms of extension: the incorporation of these policy domains into security policy is also a way of securitizing them, which means removing them from the ordinary political debate and subjecting them to the urgency, the pressure and the rules of security issues. When a social problem becomes an issue of security policy, it is removed from ordinary political debate and ceases to be addressed along traditional democratic means. Expansion and securitization are also subjecting these policy issues to a new approach, which is fundamentally based on threat anticipation and pre-emptive action. Pre-emption implies action before a crime has actually been committed, and yet, according to the European Union Charter of Rights, everyone is innocent not only before he/she commits a crime but actually until the contrary is proved in court. Maybe the risk of terrorist attack being perpetrated may justify a suspension of this basic civil right, but a suspension this remains nonetheless.

This is, in a way, a security paradox that lies at the heart of the new concept of security and is further aggravated by the new emphasis on risk assessment and risk management. The attempt to prevent a security threat from materializing needs the deployment of a powerful and ever-expanding intelligence service being able to gather massive amounts of information in order to assess the risk and manage its possible manifestation. In this perspective, all citizens can be subjected to surveillance and be assigned a security label on the basis of the level of risk they pose to the system. Needless to say, these tasks cannot be performed, at least in the terms in which they have been conceived, without the massive deployment of surveillance-orientated security technologies. A higher emphasis on surveillance technology often implies a lower emphasis on the social and economic determinants of crime and restricts focus only on those aspects of security that can actually be addressed by a technology. Thanks to surveillance studies, we are today aware of social sorting, ethnic discrimination and self-censorship usually associated with SOSTs.

Although this was not an inevitable outcome, these technologies have often introduced surveillance as a routine practice, with the unwelcome result of a significant restriction of individual privacy. With privacy curbed down, all the democratic and civil rights that rely on the preservation of the anonymity, confidentiality and intimacy of human behaviour and actions have been negatively affected. Freedom of expression, press, association, movement and political action cannot be fully enjoyed in the absence

of sufficient level of privacy. Precisely as a result of this gradual shift towards a surveillance society, the implementation of new surveillance-orientated security technologies has been framed, and proposed to the public, in terms of a trade-off between security and liberty. When adopted, the trade-off always implies a reduction of civil liberties in exchange for (allegedly) more security.

Citizens are often asked to renounce part of their liberty and civil rights in exchange for an increased level of security. Security, the national and European Security Strategy documents suggest, is a precondition for development, or for democracy. Without security, as they say, democracy would simply not be possible. However, as the EU Charter of Rights acknowledges, security and liberty are both essential elements of our liberal democracy. Citizens cannot be free unless they are safe. However, they cannot be safe unless they are free or they would no longer be citizens. This is why it does not seem acceptable or, for that matter, productive to keep thinking of liberty and security as in opposition to each other. Security and liberty are not mutually exclusive but rather mutually constitutive. As a consequence, security policies need to be radically reconsidered: either they aim at a mutual reinforcement between liberty and security, or they, simply, won't be at all.

This process of reconsideration, as odd as it may seem, needs to start from the very subjects that have been bearing so far the costs and the implications of security policies based on SOSTs, pre-emption and risk assessment: the citizens. There is need to allow them to express their views, which are more complex and sophisticated than what we are used to thinking. There is need, moreover, to change the questions to involve them in novel ways, as they are, ultimately, the subjects and the sovereign of political actions. The next section aims, precisely, at this new endeavour: the elaboration of a new theoretical model where the criteria and factors influencing public acceptability of new security measures – be they surveillance orientated or not, technology based or not – do necessarily proceed from a frame where security and liberty stand at odds with each other. It aims at something more: the elaboration of a new engagement process where citizens are not asked how much liberty they are willing to trade in exchange for more security, an engagement process where they have a chance to set the rules and the boundaries without having to choose from a path of predefined options already settled. If security is, first and foremost, a practice, this is a first step towards a new practice and, thus, a new security for all.

4 Drivers of technology acceptability

4.1 Introduction

In the previous sections, we have dealt in details with the shifting nature of security and the role played by security technologies. It has been pointed out that security is expanding as concept and as a domain. Several social and political issues are being transformed into security issues, while new approaches to security are emphasising pre-emption and threat anticipation as well as risk management strategies. These changes are have important and, to a certain extent, worrisome implications, not only in terms of civil liberties, being restricted or curbed, but also in terms of political responsibility and democratic accountability. This shifting conception of security is endorsing a massive implementation of surveillance-orientated security technologies (SOSTs), which, in turn, may increase public opposition and resistance as these measures impose surveillance and other restrictive procedures to ordinary citizens.

To address the issues rose by the introduction of SOSTs, in this chapter we focus our attention on the fundamental research question informing the SurPRISE project, i.e. what factors and criteria do influence public acceptability of SOSTs. In order to find potential answers to this question we have undertaken a revision of the academic literature that has dealt with the topic of public acceptance and acceptability of technology. Although the majority of the studies reviewed here focus on acceptance, in our approach we prefer to focus on “acceptability” rather than “acceptance” because we are looking for insights regarding what elements make a given SOST more or less acceptable, as further explained in the next chapter. Out of a vast literature, we have selected and organised information coming from Science, Technology and Society (STS) studies and the psychological, sociological, and technical analysis of technology risks. In this section we also focus on the study of privacy from a social science perspective, while the discussion on privacy as human right, here only briefly mentioned, was developed at length by the deliverable “D3.2 – Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy”²⁰⁵.

The chapter is divided into four main parts. The first two sections present main theoretical perspectives and corresponding explanatory models influencing public acceptance and acceptability of technology. The following section revises privacy and security studies and moves the attention from public acceptance of technology in general to acceptability of SOSTs. The subsequent section presents concrete examples of public acceptance of SOSTs in Europe. The chapter ends with a table reporting all those variables identified both in the literature and through the consortium review of national issues and debates around SOSTs.

4.2 Public assessment of science and technology

On the basis of their own societal and experiential knowledge, citizens have often come to question the need, the appropriateness and the actual impact of prospected or recently implemented technologies. Innovations like nuclear energy, biotechnology or nanotechnology can raise controversial issues and have ethical, social, economic and public health implications that can trigger public outcry and rejection. Collective actions and protests against nuclear power plants in the 1980s and against GMO food in the 1990s have brought the issue of public acceptance of technology to the attention of both policymakers and social scientists. Although SurPRISE is not about exploring the relation between science and public, and it is not specifically concerned with public acceptance of technology and technology development in general terms, insights from this literature may shed light on a number of factors that may be relevant when we study public acceptability of surveillance technologies implemented for security purposes.

²⁰⁵ Porcedda, M.G., M. Vermeulen et al. (2013). Report on regulatory frameworks concerning privacy and the evolution of the nrm of the right to privacy. Deliverable 3.2, SurPRISE Project. Florence, European University Institute.

The end of that unconditional support for science and technology, which characterised the years of reconstruction after the World War II, leads an increasing number of scholars to criticize the linear model of innovation, which considers that citizens accept technological breakthrough under the premise that this would bring prosperity and wealth. Catastrophic accidents like nuclear meltdown at Three Mile Island or Chernobyl, or cases of contamination like the BSE syndrome, have drastically changed the perception of the public of the risks associated with new technology. In the same way, premises and models to understand public acceptance of technology have changed dramatically.

Theorists have adopted different perspectives, from the deficit model, which attributes opposition towards technology to a lack of scientific knowledge, through the contextual approaches, in which different socio-cultural variables must be taken into account to understand acceptance or rejection of technology, to the public-engagement-in-science proposal, which emphasizes the need to involve citizens in the decision-making process as a way of democratising science and increasing acceptance of technological developments. All these streams of inquiry share the same objective of offering guidelines for preventing the rejection of innovation. In fact, what benefits would science and technology bring to society if citizens reject their use and application?

In the following sections we will revise some relevant studies focusing on the public assessment of science and technology in search of insights about those factors that may hamper or reinforce public acceptability of technology.

4.2.1 The deficit model

Classic studies on social perception of science used to address the relationship between public and science from a perspective known as the 'deficit model'. The latter used the level of scientific knowledge (or the lack of knowledge) as the independent variable and considered the level of support for science and technology as the dependent variable²⁰⁶. The initial response of scientists to growing levels of public detachment and mistrust was to embark on a mission to inform. The Chernobyl nuclear disaster in the 1980s and the BSE crisis in the mid-1990s triggered a growing scepticism about science as a guide to progress and development. Inspired by the findings of traditional studies of social perception of science, some authors attributed this scepticism to a deficit in public understanding of scientific issues, which encouraged numerous governments, advised by the experts, to develop campaigns to improve the level of scientific knowledge of citizens and thereby reduce the scepticism and hostility to certain innovations²⁰⁷. In the UK, Sir Walter Bodmer's influential 1985 report for the Royal Society argued that '*It is clearly a part of each scientist's professional responsibility to promote the public understanding of science*'.

During the 1990s, it was found that while the deficit model is adequate to explain the attitudes towards science and technology in general, it is problematic in determining the acceptance of those technologies that seem to produce higher ethical controversies²⁰⁸. More recently, some studies also demonstrated how people tend to evaluate the validity and timeliness of scientific research and technological applications in relation to the objectives that the latter are prefixed, and that a greater consensus on their final objectives corresponds often with an increased tolerance and support for scientific and technological research, especially when they are ethically or socially controversial²⁰⁹.

²⁰⁶ Miller, S. (2001) "Public understanding of science at the crossroads", *Public Understanding of Science* 10:115-120.
Allum, N. et al. (2008) "Science knowledge and attitudes across cultures: a meta-analysis" *Public Understanding of Science* 17: 35-54.

²⁰⁷ Durant, R. F. and Legge J. S. (2005) "Public Opinion, Risk Perceptions, and Genetically Modified Food Regulatory Policy" *European Union Politics* 6(2):181-200

²⁰⁸ Evans, G. and Durant, J. (1995) "The relationship between knowledge and attitudes in the public understanding of science in Britain," *Public Understanding of Science* 4(1): 57-74.

²⁰⁹ Brown, J.L. and Ping, Y. (2003) "Consumer perception of risk associated with eating genetically engineered soybeans is less in the presence of a perceived consumer benefit," *Journal of the American Dietetic Association* 103(2): 208-214. Qin, W. and Brown, J.L. (2008) "Factors explaining male/female differences in attitudes and purchase intention toward genetically engineered salmon," *Journal of Consumer Behaviour* 7(2): 127-45.

Eventually, and, despite a variety of different outcomes, critical studies of the cognitive deficit model came often to converge on a common conclusion: positive and negative attitudes toward science and technology were not related exclusively to scientific knowledge of the citizens or the scientific development of the country, several other social, cultural and political influences were also very relevant.²¹⁰

4.2.2 Contextual approaches

Later in the 1990s, some authors began to consider the impact of social, cultural and policy factors associated with the institutional environment as independent variables in relation to the growing or diminishing level of public support towards new technologies²¹¹. Without rejecting the relevance of scientific information, gradually, new approaches began to emphasize the influence and relevance of the social and political context. These studies proposed a different relationship between the scientific world and the public, where the latter featured as an active participant, precisely on the grounds of their knowledge of the contextual factors that are likely to affect development and implementation of science and technology. This societal and experiential knowledge was considered necessary to complement the scientific and technical knowledge provided by experts²¹². A contextual approach can also explain the different support for science and technology between different social groups and different countries or between different technologies. For instance, the relevance of the cultural and national differences in the acceptance of technology was brilliantly shown by a comparative study on the perception of nanotechnology in the United States and the European Union, in which Americans were very positive, and Europeans showed sceptical or pessimistic values when it came to support nanotechnology innovation.²¹³

Levidow and Marris elaborated one of the first consistent shifts away from the deficit model²¹⁴. In their argument, they suggested that public opposition was less due to the 'lack of scientific knowledge' and more to the 'lack of trust' towards scientists, politicians and governments. In contextual approaches, social trust was usually defined as the willingness to believe the opinions of those who have the responsibility to make decisions and take actions concerning the management of science, technology, environment, health and public safety²¹⁵. An important group of studies in this field has analysed the influence of social trust as a relevant factor in the attitudes towards science and technology. Siegrist, for instance, argued that when people have a limited scientific knowledge, their need to rely on the judgment of experts, which they consider reliable, to form an opinion increases. In turn, this implied that both the perception of the risks and benefits associated with science and technology and the confidence of citizens in the institutions responsible for regulating them are important factors in explaining public attitudes²¹⁶. However, there are many variables that influence social trust. The same study suggested that the similarity of salient ethical values (SVS) allowed people to have more confidence in those who shared the same values. As a result, the more similar the values of the public and the experts, the easier it was for the public to trust the scientific community. Other studies

²¹⁰ Gross, A. G. (1994): "The roles of rhetoric in the public understanding of science", *Public Understanding of Science* 3 (1): 3-23. Miller, S. (2001) *op. cit.* Burns, T. W., O'Connor, D.J. and Stocklmayer, S.M. (2003) "Science Communication: A Contemporary Definition," *Public Understanding of Science* 12: 183-202.

²¹¹ Pavone, V., Osuna, C. and Degli Esposti, S. (2010) "Invertir en ciencia y tecnología en tiempos de austeridad económica: ¿Qué opinan los ciudadanos?", *Percepción Social de la Ciencia y la Tecnología 2010*, FECYT, available at: <http://www.fecyt.es/fecyt/detalle.do?elegidaSiguiete=&elegidaNivel3=&SalaPrensa;publicaciones;estudiosin formas&elegidaNivel2=&SalaPrensa;publicaciones&elegidaNivel1=&SalaPrensa&tc=publicaciones&id=PSC2010>.

²¹² Miller, S. (2001) *op. cit.*

²¹³ Gaskell, G., Eyck, T. et al. (2005) "Imagining nanotechnology: cultural support for technological innovation in Europe and the United States," *Public Understanding of Science* 14: 81-90.

²¹⁴ Levidow, L. and Marris, C. (2001) "Science and Governance in Europe: lessons from the case of agbiotech," *Science and Public Policy* 28(5): 345-60.

²¹⁵ Siegrist, M and Cvetkovich, G. (2000) "Perception of Hazards: The Role of Social Trust and Knowledge", *Risk Analysis* 20: 713-720.

²¹⁶ Connor, M. and Siegrist, M. (2010) "Factors Influencing People's Acceptance of Gene Technology: The Role of Knowledge, Health Expectations, Naturalness, and Social Trust", *Science Communication* 32: 514-538.

suggested that confidence in the stakeholders²¹⁷, regulatory institutions and government²¹⁸ and the intrinsic motivation of the scientists were also factors having relevance influence over public trust.²¹⁹ Finally, more recent studies focused on how social trust influences the perception of the risks and benefits of new technologies, usually increasing the perceived benefits and reducing the perceived risks²²⁰. Other studies also suggested that the evaluation and interest in science and technology also depend on the social implications, risks and benefits that individuals used to associate with science in general and with each of these technologies in particular. For example, the level of confidence in solar energy remains very high, although this sector has not experienced any spectacular progress in the last years²²¹; by contrast support levels for nuclear energy remain very low, even if, allegedly, the safety of nuclear reactors has increased over the last two decades.²²²

Several studies following the contextual approach ended up suggesting that social trust could be restored through dialogue and debate, ultimately through public participation in decision-making. In 2000, an influential UK House of Lords report detected 'a new mood for dialogue'. Similar reports or analysis have to be found in other European countries. For example, in Switzerland, the Foundation 'Science et société' was created on the initiative of the State Secretariat for Education, Research and Innovation, with the mission to encourage the dialogue and trust between science and citizens. Actual trigger for the creation of the Foundation was the so-called genetic protection initiative, which came to a vote in 1998. The referendum campaign made clear that between science and the public a wide gap existed²²³. In France, a first 'citizen conference' on GMOs has been organized in 1998 by the "Office parlementaire d'évaluation des choix scientifiques et technologiques", and other participatory events have been organized later on²²⁴. All these initiatives were based on the pioneer work in the Netherlands and in Denmark (consensus conferences, constructive Technology Assessment)²²⁵. In 2002, at EU level, the first Science and Society programme was incorporated in the sixth Research Framework Programme with new initiatives around public participation. The language of 'science and society' became prominent, and there was a fresh impetus towards accountability and engagement. In the following years, there actually was a perceptible change: the science community adopted a more conversational tone in its dealings with the public. This was not always embraced with enthusiasm, but at least it became clear to both scientists and policy makers that new forms of engagement were now a non-negotiable clause of their licence to operate²²⁶.

Some debate on the actual purpose of dialogue, however, emerged quite soon. De Marchi²²⁷, for instance, considered that the purpose of public dialogue was not to eliminate conflicts, but to enable clarification of what is actually in conflict with public opinion. Public participation became, therefore, the answer to the problem of public opposition, which could also accommodate a new type of knowledge in the field of decision making. The dialogue with, and the inclusion of, the public appeared for a while as an effective remedy to the loss of credibility and trust in science and regulation. Engagement with the public, thus, emerged as a necessary tool to reduce the lack of public trust and

²¹⁷ Gottweiss, H. (2002) "Gene therapy and the public: a matter of trust," *Gene Therapy* 9(11): 667-669.

²¹⁸ Barnett, J. et al. (2007): "Belief in public efficacy, trust and attitudes toward modern genetic science," *Risk Analysis* 27 (4): 921-933.

²¹⁹ Critchley, C. R. (2008): "Public opinion and trust in scientists: the role of the research context, and the perceived motivation of stem cell researchers," *Public Understanding of Science* 17: 309-327.

²²⁰ Siegrist, M. (2008) "Factors influencing public acceptance of innovative food technologies and products." *Trends in Food Science & Technology* 19: 603-608.

²²¹ Spence A. et al., (2010) "Public Perceptions of Energy Choices: The Influence of Beliefs About Climate Change and the Environment", *Energy and the Environment* 21 (5): 385-407.

²²² Pidgeon, N. F., Lorenzoni I., and Poortinga W. (2008): "Climate change or nuclear power-No thanks! A quantitative study of public perceptions and risk framing in Britain", *Global Environmental Change* 18: 69-85.

²²³ Bovet, A. (2012) *Gènes dans la démocratie. Le génie génétique dans l'espace public suisse (1992-2005)*. Lausanne; Éditions Antipodes.

²²⁴ Callon, M. et al. (2009) *Acting in an Uncertain World. An Essay on Technical Democracy*, Cambridge,

²²⁵ Joss, S. and Bellucci, S. (eds.) (2002) *Participatory Technology Assessment. European perspectives*. London: Centre for the Study of Democracy,

²²⁶ Wisdom, J. (2007) "Public engagement of science across the European Research Area," *Public engagement of science*.

²²⁷ De Marchi, B. (2003) "Public Participation and risk governance," *Science and Public Policy* 30: 171-176.

legitimize controversial decisions. During the 1990s, in fact, the relationship between science and the public, especially in Europe had been characterised by the mistrust and constant public opposition to some of the applications of biotechnology for commercial purposes, an intense pressure from governments to be internationally competitive and, third, a growing influence, direct and indirect, of some social elements in scientific research.²²⁸ And yet, why was dialogue expected to restore public trust? Addressing this question, Joanna Goven came to the conclusion that the dialogue was eventually considered a therapy in itself, regardless of its actual outcomes or impact on decision-making.

4.2.3 Public engagement approaches

As public engagement inspired studies began to generate significant results, the same institutions and regulatory practices of science and technology became more reflective. At some point, it was even proposed to include not only the scientific and technological contents but also the actual practices, processes and regulatory institutions as part of the public assessment process²²⁹. The scientific community eventually embraced dialogue and engagement, if not always with enthusiasm, then at least out of a recognition that BSE, GM and other controversies have made it a non-negotiable clause of their 'licence to operate'. Experts and scientists do their work in alerting the public about problems and disputes arising in the world, but the public is normally expected to assess and evaluate science and technology only after the scientific community, policymakers and private companies have already determined the technologies to be developed and implemented and the objectives to be pursued. Compared to the deficit model inspired policy strategies, the public certainly had more room in the political process, and democracy in scientific and technological decision-making was made stronger.

Yet, Carolan²³⁰ has recently addressed the problem of decision-making in science and technology policy, introducing the sociotechnical issue of a grey area between science and politics that is characterized by the presence of questions that are asked to science, but that science cannot resolve. In order to resolve this conflict, Carolan suggested including new types of experience allowing for a new type of decision-making, which could also take fully into account social knowledge, that is, knowledge based on social experience. It involves full inclusion of lay public and civil society organizations in the rooms of decision-making. The democratization of science and the inclusion of public participation in decision making were presented as a way to achieve a robust social knowledge, a path that exceeds the premises of reliable knowledge to be valid outside the walls of science, in the real world, where social, economic and cultural factors do play a role. Robustness of social knowledge refers, thus, to the process through which knowledge is generated. This democratization of experience, says Nowotny²³¹, can cause tension especially at the institutional level, since the experts are asked to make decisions in stressful situations, even forcing them to transgress the limits of their powers when they are asked to take critical decisions in a context of little knowledge at all.

In spite of these recent socio-technical changes in the way the relationship between science, technology and the public is framed and organized, the link between public engagement and the choices, priorities and everyday practices of science remains fuzzy and unclear. Dialogue tends to be restricted to particular questions, posed at particular stages in the cycle of research, development and exploitation. Possible risks are endlessly debated, while deeper questions about the values, visions, and vested interests that motivate scientific endeavour often remain unasked or unanswered. More recently, there has been a wave of interest in moving public engagement 'upstream' – to an earlier stage in the processes of research and development. There is a sense that earlier controversies have created a window of opportunity, through which we can see more clearly how to reform and improve the governance of science and technology.

²²⁸ Goven, J. (2006) "Processes of Inclusion, Cultures of Calculation, Structures of Power". *Science, Technology and Human Values* 3(5): 565-599.

²²⁹ Todt, O. et al. (2010) "Practical Values and Uncertainty in Regulatory Decision-making," *Social Epistemology* 24(4): 349-362.

²³⁰ Carolan, M. (2006) "Science, expertise and democratization of decision-making process," *Society and Nature Resources*, 19: 661-668.

²³¹ Nowotny, H. (2003) "Dilemma of expertise" *Science and Public Policy* 30(3): 151-156.

This work on public engagement has sought to develop mechanisms on how publics can be involved in the research process, especially where strong negative views on certain scientific and technological developments are expressed²³² and restore the acceptability. This has been an important theoretical and empirical development with regards to how scientific and technological research should be conducted and governed²³³. It has, for example, been a cornerstone of theoretical and empirical work in European social sciences in relation to new scientific development and technological innovations²³⁴. If we examine research funded through European schemes, the argument has been so successful that the call for the public to be engaged or involved with the research and innovation process is almost ubiquitous and remains a critical development. These new ways of conducting science and technology practices, which include mechanisms of public engagement in science and technology policy almost by default, constitute the peculiarity of European science and technological innovation, compared, for instance, to the US²³⁵. Whether this deliberative approach has effectively produced a democratization of science and technology policy, however, remains a controversial issue.²³⁶

More radical approaches, in fact, have tried to shift the attention from democratization of science to a more comprehensive critique of PES²³⁷. These authors have questioned dominant public engagement approaches on a number of theoretical and empirical issues that are usually unaddressed. These issues relate, for instance, to who is the public and how it has been constituted, who decides what is going to be talked about and on what grounds, why is dialogue to be preferred to conflict, and at what stage of policy making is participation set and why. As Sheila Jasanoff puts it, *"The purpose is to hold science and industry answerable, with the utmost seriousness, to the fundamental questions of democratic politics: Who is making the choices that govern lives? On whose behalf? According to whose definitions of the good? With what rights of representation? And in which forums?"*²³⁸

These questions remain largely unaddressed, when not bluntly ignored. Governments continue to rely on scientific expertise to sustain and legitimize their public authority, shifting the burden of responsibility of emerging conflict and mistrust to an imagined and constructed public²³⁹. Even recent PES exercises have mainly been set up with a view of getting support for science in exchange for dialogue, showing little self-reflexivity²⁴⁰. For instance, it is increasingly clear that there is no univocal position within the public, and that we are always in the presence of a variety of publics. It has also been acknowledged that civil society organizations and publics in general are seldom anti-science, for they support scientific research but call for a more open and reflexive decision-making process, where knowledge production mechanisms, research agenda priorities, regulatory frameworks and ownership and distribution guidelines may be openly questioned and addressed²⁴¹.

Despite these criticisms, PES exercises continue addressing scientific and technological issues in terms of risk assessment, presenting risk considerations made by expert involved as 'scientific' and referring to public views as 'perceptions'. In addition, when risks are valued against benefits, the latter are usually uncritically inflated and presented as 'just around the corner'²⁴². Whilst science and technology innovation remains strongly supported in the name of an unjustified pressure of commercialization in

²³² Sapient Deliverable 1.1

²³³ Kurath, M. and Gisler, P. (2009) "Informing, involving or engaging: Science communication in the ages of atom, bio- and nanotechnology", *Public Understanding of Science* 18 (5): 559- 573.

²³⁴ Nesserini, F. and Bucchi, M. (2011) "Which indicators for the new public engagement activities? An exploratory study of European research institutions," *Public Understanding of Science* 20(1): 64-79.

²³⁵ Wilsdon, J. and Willis, R (2004) *op.cit.*

²³⁶ Ferretti, M.P. and Pavone, V. (2009): "What do civil society organisations expect from participation in science? Lessons from Germany and Spain on the issue of GMOs" *Science and Public Policy* 36(4).

²³⁷ Jasanoff, S. (2005) *op. cit.* Wynne, B. (2006) "Public Engagement as a Means of Restoring Public Trust in Science: Hitting the Notes, but Missing the Music?" *Community Genetics* 9(3): 211–20. Felt U., Wynne, B. et al. (2007) *op. cit.*

²³⁸ Jasanoff, S. (2005) *op.cit*

²³⁹ Wynne, B. (2006) *op. cit.*

²⁴⁰ European Commission (2007) *Public engagement in science*. European Research Area.

²⁴¹ Ferretti, M.P. and Pavone, V. (2009) *op. cit.*

²⁴² Evans, R., Kotchetkova, I. and Susanne, L. (2009) "Just around the Corner: Rhetoric of Progress and Promise in Genetic Research", *Public Understanding of Science* 18(1):43-59.

the face of globalization, no potential alternatives are taken into considerations and no room is made for negotiation. As Wynne puts it *"we can notice a systematic exclusion from public engagement with science of any accountable debate and negotiation of the driving purposes and expectations shaping innovation and knowledge."*²⁴³ . Other authors suggested shifting attention from the public and its alleged value-driven attitude (as opposed to a rational, informed assessment) to the very institutional practices promoting and regulating science and innovation. Up until now, public engagement has mainly questioned the public and its 'understanding', yet the 'problematization' of the public prevents a deeper questioning of the regulatory systems and of the systems of knowledge production. The latter domain, in this way, has remained so far out of sight and, thus, unquestioned.

In the light of these criticisms, it seems urgent to address public participation in, and public engagement with, science under a radically different light. First, it seems important, at a very general level, to ask new questions about the relationship between science, politics and society. The reasons and the ways in which certain issues, and not others, have become objects of public policy; how and as a result of whose action has this happened; and what kind of society are we trying to achieve through current innovation directions and priorities become therefore key questions that deserve attention well before single technologies can be assessed. In current participatory practices: *"dialogue tends to be restricted to particular questions, posed at particular stages in the cycle of research, development and exploitation. Risks are endlessly debated, while deeper questions about the values, visions and vested interests that motivate scientific endeavour often remain unasked or unanswered"*²⁴⁴.

As long as PUS and PES keep focusing on the reaction, and/or opinion, of the wider public in risk assessment exercises associated with the development and introduction of new technologies, these questions will never be addressed. The focus on public concerns and values keep values, concerns and interests shared and pursued by the scientific communities and the industrial corporations outside the scope of public debate and scrutiny, implicitly assuming that this is not problematic. A recent report published by the European Commission on Public Engagement in Science²⁴⁵ show signs of self-reflexivity and urges scientific and policymaking institutions alike to acknowledge the need for a broader debate on the social contract for science: *"We need to renew the social contract for science. There is an increasing body of evidence showing that interactions between science, civil society and the wider public can generate new forms of social intelligence and create mutual benefits by stimulating new directions for innovation"*²⁴⁶. And yet, as recognised by the same report, *"policy makers and the scientific community are desperate to avoid the developments in fields like Nanotechnology, neuroscience, and synthetic biology becoming the next GM"*. In other words, not only questioning the public remains a dominant concern of public engagement schemes, it remains also associated with a general purpose that aims at reducing conflict and securing support for scientific innovation and expert-based policy-making.

Recent perspectives in public engagement have, in principle, accepted that the public may contribute not only with 'values and concerns' but also with lay knowledge: *"Lay knowledge, or lay expertise, emerges from dialogue between experts and non-experts and, it is listened to, it contributes to socially robust science"*. Yet, the dominant dichotomy between facts and values, science and society, prevents that the values and interests knowledge production, technological innovation and regulation processes, may come explicitly to the fore and face public scrutiny. On the other hand, the confinement of public contribution to 'values' allow further marginalisation of alternative perspectives for values, in a neo-liberal context are considered 'private' and cannot be imposed on the society as whole. As a consequence, individualistic solutions, based on market or consumer choice approaches, are encouraged and endorsed, with an increasing emphasis on individual risk management and responsibility. Individualistic approaches, in turn, facilitate the gradual disappearance of the social and

²⁴³ Wynne, B. (2006) "Public Engagement as a Means of Restoring Public Trust in Science: Hitting the Notes, but Missing the Music?" *Community Genetics* 9(3): 211–20.

²⁴⁴ European Commission (2007) *op. cit.* p.16.

²⁴⁵ Ibid.

²⁴⁶ Ibid, p.11

political aspects associated with the technologies under development and of the social or medical problems in relation to which these technologies were developed in the first place

In conclusion, the complexity and uncertainty surrounding the development and implementation of new technologies affects public attitudes towards them and, clearly, the deficit model is not sufficient to explain public acceptability or rejection of these technologies. New approaches have been, thus, developed, which have emphasized the importance of socio-cultural factors, like trust, and the need to take into account lay knowledge as a relevant type of knowledge and the experience of citizens in the decisions process about the directions of science and technology to guarantee socially robust and publically shared development of new technologies.

4.3 Acceptability of security technologies from a risk analysis perspective

Public assessment towards the development and implementation of new technologies and practices does not merely depend, though, on their appropriateness or their ability to successfully address specific social problems. It also depends on the amount and nature of risks that their implementation and use entail. If we look specifically at SOSTs, for instance, a number of different risks come to the fore. For instance, the introduction of SOSTs often constitute a risk in terms of privacy infringement, of being identified as a false positive, or a risk of social sorting and restriction of democratic rights of free speech, expression and association due to self-censorship or induced conformism, not to mention health related risks. SOSTs, moreover, constitute a peculiar case study, for these technologies are supposed to carry some risks for the individuals but are meant, at the same, time to prevent them from becoming victims of more dramatic threats. As a result, the academic literature studying precisely how individuals and groups assess new technologies, and their related practices, in terms of risk is effectively very relevant to cast light on some other factors likely to affect public acceptance and acceptability of SOSTs.

The concept of 'risk' has gained significance in public and academic debates in particular after WWII²⁴⁷ It was mainly linked to the development of new technologies, such as nuclear energy applications. Nowadays the concept of risk is relevant to many scientific disciplines, but despite its current development and growing interest, the social sciences have not been able to establish a coherent theory that can structure this field of work and interconnect the multiple research results of risk problems. In this section, we are going to review three conceptions of the acceptability of technology from a risk perspective, taking into account the three frames existing in the literature.

First, the technical approach insisted on the possibility of obtaining a scientific and objective measure of the risks related to each technology. A second, psychological approach focused on the individuals and includes subjective and contextual factors in the acceptability of risk, using a psychometric test. According to this approach, it would possible to talk about objective risk only when sufficient data exist for a solid statistical calculus of probability. As this is rarely the case, in the absence of such data, only the subjective estimation of risks made by experts or by the lay people could really be considered. As a result, the psychological approach reduces the distinction between objective and subjective risk to the difference between two sources of subjective risk, ones from the experts and ones from lay people. A third approach, therefore, took distance from the technological and psychological approaches, focused on the importance of social structures and cultural behaviours is developed, in which trust in institutions is a central point.

Technical Approach	Psychological Approach	Sociological Approach
--------------------	------------------------	-----------------------

²⁴⁷ Zinn, J. O. (2010) "Risk as a Discourse: Interdisciplinary Perspectives." *Critical Approaches to Discourse Analysis across Disciplines* 4(2): 106-124.

Acceptability of risk as a function of probability and magnitude of potential damage	Acceptability of risk as a function of psychometric variables	Acceptability of risk as a function of socio-cultural factors
--	---	---

Table 2. Risk analysis approaches

4.3.1 The technical approach

The technical approach was the dominant paradigm at the origins of risk research, especially in relation to first social controversies associated with the development and the implementation of nuclear energy. Nowadays, as an approach to risk research, it is often adopted by several private enterprises and public administration in the study of the implementation and security issues of modern technologies²⁴⁸. The operational objective of this approach is to develop a universally valid measure of risk, with which it could then be possible to establish a comparison between different types of risks. Risk assessment is the scientific process of defining the components of risk in precise quantitative terms, calculating the probabilities for unwanted consequences, and aggregating both components by multiplying the probabilities by the magnitude of the effects²⁴⁹. Acting in this way, it pretends to get a rational explanation of the acceptability of the various risks according to the degree of their probabilities and their consequences by applying the formula $R = P \times M$.

Technical analyses of risk have encountered much criticism in the social sciences²⁵⁰. The first group of critiques focuses on the variability of what people perceive as an undesirable effect, which normally depends on their values and preferences.²⁵¹ A second group of critiques emphasizes that the interactions between human activities and their consequences are more complex and unique than the average probabilities used in technical risk analyses are able to capture.²⁵² A third group argues that the institutional structure of managing and controlling risks is prone to organizational failures and deficits that may eventually increase the actual risk²⁵³. A fourth stream of criticisms suggests that risk analysis cannot be regarded as a value-free scientific activity, for ethical and political values are reflected in how

²⁴⁸ Lowrance, W. W. (1976) *Of Acceptable Risk: Science and the Determination of Safety*. Los Altos: William Kaufman. Fischhoff, B., Lichtenstein, S., Slovic, P., Derby, S. L. and Keeney, R. L. (1981) *Acceptable Risk*. Cambridge: Cambridge University Press. Fritzsche, A. (1986) *Wie sicher leben wir?* Köln. Renn, O. (1991) "Risikowahrnehmung und Risikobewertung: Soziale Perzeption und gesellschaftliche Konflikte," in Chakrabarty, S., Yadigarolu, G. (eds.) *Ganzheitliche Risikobetrachtung*, Köln: 1–62. Rowe, G. (1977) *An Anatomy of Risk*. New York. Bechmann, G. (1995) "Riesgo y desarrollo científico técnico. Sobre la importancia social de la investigación y valoración del riesgo" *Cuadernos de Sección Ciencias Sociales y Económicas* 2:59–98. Zinn, O. (2006) "Recent Developments in Sociology of Risk and Uncertainty" *Forum Qualitative Research* 7(1).

²⁴⁸ Kolluru, R. V. and Broks., D.G. (1995) "Integrated Risk Assessment and Strategic Management" in *Risk Assessment and Management Handbook. For Environmental, Health, and Safety Professionals*. New York: McGraw-Hill.

²⁴⁹ Ibid.

²⁵⁰ Hoos, I. (1980) "Risk Assessment in Social Perspective" in *Perceptions of Risk*. Measurements. Washington, DC: NCRP. Douglas, M. (1985) *Risk Acceptability According to the Social Sciences*. New York: Russel Sage Fondation. Beck, U. (1992) *op. cit.* Freudenburg, W. R. (1989) "Perceived risk, real risk: social science and the art of probabilistic riskassessment," *Science* 242: 9–44. Shreder-Frechette, K. S. (1991). *Risk and Rationality*. Berkley: University of California Press. Reiss, A. (1992) "The Institutionalization of Risk" in: Short, J.F. and Clarke, L. (eds) *Organizations, Uncertainties, and Risk*, Boulder: Westview. p. 299–308,

²⁵¹ Dietz, T. et al. (1996) "Risk, Technology and Society" in Dunlap and Michelson (eds.) *Handbook of environmental sociology*. Westport: Greenwood Press.

²⁵² Fischhoff, B., Goitein, G. and Shapiro, Z. (1982) "The Experienced Utility of Expected Utility Approaches", in Feather, N.T. ed. *Expectations and Actions: Expectancy-Value Models in Psychology*, Hillsdale: Lawrence Erlbaum. p. 315–40.

²⁵³ Perrow, C. (1984). *Normal Accidents: Living with High Risk Technologies*. New York: Basic Books. Short, J.F and Clarke, L. (1992) "Social Organization and Risk", in Short, J.F. and Clarke, L. (eds) *Organizations, Uncertainties, and Risk*, Boulder: Westview. pp. 309–21.

risks are characterized, measured and interpreted²⁵⁴. In this respect, purely technical risk assessment provides too much power to an elite that is neither qualified and nor politically legitimated to impose risks policies on a population. Finally, it has also been pointed out that the numerical combination of magnitude and probabilities, which assumes equal weight for both components, assigns the same risk value to events with high consequences and low probability and to events with low consequences and high probability. As Renn²⁵⁵ argued, the technical approach in risk analysis represents a narrow framework, which cannot, alone, be the single criterion for risk identification, evaluation and management. Technical risk analyses do help decision makers to estimate the expected physical harm and provide the best knowledge about actual damage that is logically or empirically linked with each possibility of action. Yet, the technical approach needs to be complemented by social science orientated risk analyses, which may effectively address the areas of experiential knowledge normally either ignored or dismissed²⁵⁶. The exclusion of the social context in technical studies provides an abstraction that enhances the inter-subjective validity of the results but at the price of neglecting the social processing of risk²⁵⁷.

The concept closest to the technical approach in the social sciences is the economic concept of risk²⁵⁸. In contrast to the technical approaches, in economics probabilities are not only conceptualized as relative frequencies but also as strength of beliefs²⁵⁹. The economic theory perceives risk analyses as part of larger cost-benefit considerations in which risks are the expected utility losses resulting from an event or activity. The major difference between technical and economical approaches is the transformation of physical harm or other undesired effects into subjective utilities²⁶⁰. If risk can be expressed in terms of utilities, then they can be integrated into a decision process in which costs and benefits are assessed and compared²⁶¹. The economic approach serves several functions in risk policies²⁶². It provides instruments to measure and compare utility losses or gains from different decision options, thus enabling decision makers to make more informed choices; it enhances technical risk analyses by providing a broader definition of undesirable events, which include nonphysical aspects of risk; it provides techniques to measure distinctly different types of benefits and risks with the same unit; and it provides a model for rational decision making, if decision makers can reach agreement about the utilities associated with each option. The economic risk concept constitutes a useful framework for situations in which individuals are making decisions in a specific context in which the consequences of the action are confined to the decision maker, but both conditions are rarely met and this is its major weakness.

4.3.2 The psychological approach

Struggling with the major limitations of the technical approach, the psychological approach was first developed in the 1960s. It took as a starting point the discrepancy between what is technically counted

²⁵⁴ Fischhoff, B. (1995) "Risk perception and communication unplugged: twenty years of process,," *Risk Analysis* 15(2): 137-145.

²⁵⁵ Renn, O. (1998) "Three decades of risk research: accomplishments and new challenges," *Journal of Risk Research* 1(1): 49-71.

²⁵⁶ Pavone, V., Goven, J. and Guarino, R. (2011) "From risk assessment to in-context trajectory evaluation-GMOs and their social implications," *Environmental Sciences Europe* 23(1):3-13.

²⁵⁷ Brehmer, B. (1987) "The Psychology of Risk", in Singleton, W.T. and Howden, J. (eds) *Risk and Decisions*, New York: Wiley. pp.25-39. Renn, O. (1992) "Concepts of Risk: A Clasification" in Krimskie and Golding (eds.) *Social Theories of Risk*. Westport: Preager."

²⁵⁸ Renn, O. (1998) *op.cit.*

²⁵⁹ Fischhoff, B. et al. (1981) *op. cit.*

²⁶⁰ Just, R.E., Health, D.L. and Schmitz, A. (1982) *Applied Welfare Economics and Public Policy*, Englewood Cliffs: Prentice Hall. Smith, V.K. (1986) "A Conceptual Overview of the Foundations of Benefit-Cost Analysis", in Bentkover, J.D. Covello, V.T. and Mumpower, J. (eds) *Benefits Assessment: The State of the Art*, Dordrecht: Reidel. pp. 13-34.

²⁶¹ Renn, O (1992) *op.cit.*

²⁶² Ibid.

as an acceptable risk and what people are actually willing to accept. In general it is assumed a dualism between the objective risk (defended by the technical approach) and the subjective risk, understood in terms of cognitive representation as a mental state of individual agents with subjective probabilities and degrees of acceptability, which depend on contextual variables relating to states of belief or agent behavioural rules. The psychological approach assumes that risk is a multidimensional concept and cannot be reduced to the product of probabilities and consequences.

The psychological perspective on risk includes all undesirable effects that people associate with a specific event. Whether these cause-effect relationships reflect reality or not is irrelevant, because individuals respond according to their perception of risk and not according to an objective risk level or the scientific assessment of risk. The psychological perspective on risk expands subjective judgements about the nature and magnitude of risks, it focuses on personal preferences for probabilities and attempts to explain why individuals do not anchor their risk judgements on expected values²⁶³. In fact, the perception of probabilities in decision making identified several biases in people's ability to draw inferences from probabilistic information²⁶⁴: for example, events that come to people's mind immediately are rated as more probable than events that are less mentally available²⁶⁵. Finally, the psychological perspective on risk gives more importance to contextual variables in risk estimations and evaluations²⁶⁶. Psychometric methods have been employed to explore these qualitative characteristics of risks using contextual variables, which affect the perceived risk by using psychophysical scaling and factor analysis to produce quantitative representations or 'cognitive maps' of risk perception.

This psychometric paradigm is based on the assumption that some characteristics of risks are perceived similarly, e.g. voluntariness is correlated with controllability, catastrophic potential with inequity, absorbability with knowledge about the risk, and immediacy with novelty. In 1978 in a paper that still constitutes a milestone in the psychological studies of risk, Fischhoff et al. compiled nine dimensions from the literature²⁶⁷. The first one was whether people face risk voluntarily: the respondents were asked to indicate on a seven-point scale whether some of the risks were voluntarily undertaken and some were not (voluntary = 1, involuntary = 7). The second scale asked about the immediacy of effect and the respondents were asked to indicate whether death affected immediately or if the effect was delayed. The third asked the extent that the risks were known precisely by the person who was exposed to those risks, the scale went from risk level known precisely to risk level not known. The fourth scale asked about the chronic or catastrophic potential of the risk, that is a risk that kills a small number of people over a long period of time (chronic risk) or a risk that kills a large number of people at once (catastrophic risk). The fifth dimension measured the level of dreadfulness: the subjects were asked to indicate whether this was a risk that people have learned to live with and can think about reasonably calmly, or was it one that people have great dread for – on the level of a gut reaction. The sixth scale asked about the severity of consequences and subjects were asked to indicate how likely it was that the consequence would be fatal if the risk from this activity was realized in the form of a mishap or illness. The seventh question concerned to what extent the risks are known to science: the subjects were asked to rate if the risk level was known precisely or not known. The eighth dimension focused on the level of control, in terms of personal skill or diligence, which the subjects perceived they had if they were exposed to the risk. The last dimension concerned the newness of the risk. From these scales we can observe the psychological aspects attenuating or amplifying the perception of risk as we summarize in the table below.

²⁶³ Lopes, L. L. (1983) *op. cit.* Luce, R. D. and Weber. (1986) *op. cit.*

²⁶⁴ Festinger, L. (1957) *op. cit.* Kahneman, D. and Tversky, A. (1974) *op. cit.* Kahneman, D. and Tversky, A. (1979) "Prospect theory: an analysis of decision under risk," *Econometrica* 47(2): 263-91. Ross, L.D. (1977) The Intuitive Psychologist and His Shortcomings: Distortions in the Attribution Process, in: Berkowitz, L. (ed.) *Advances in Experimental Social Psychology* Vol.10, pp. 173-220, New York: Random House.

²⁶⁵ Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S. and Combs, B. (1978). "How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits," *Policy Sciences* 9: 127-152.

²⁶⁶ Slovic, P. (1987) "Perception of Risk," *Science* 236: 280-285. Renn (1992) *op.cit.*

²⁶⁷ Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S. and Combs, B. (1978) *op. cit.*

Attenuate risk perception		Amplify risk perception	
Familiarity	↔	Exoticism	
Individual control	↔	Control by others	
Natural	↔	Man-made	
Statistical	↔	Catastrophic	
Clear benefit	↔	Little or no benefit	
Fair distribution	↔	Unfair distribution	
Voluntary	↔	Imposed	
Information from trusted sources	↔	Information from untrusted sources	
In the media	↔	Not in the media	

Table 3. Psychological aspects attenuating or amplifying risk perception

Studies using the psychometric paradigm have shown that it is possible to quantify and predict perceived risk. The technique seems appropriate to identify similarities and differences in the perception of different risks²⁶⁸. Following this argumentation, the location of a new risk topic in the risk factor space can yield helpful information to forecast public acceptance²⁶⁹. From a policy perspective, knowledge of individual perception of risks cannot be transferred directly to public policy because people's perception may often be the outcome of lack of information and/or existing clichés, plus risk perceptions usually vary among individuals and groups. Yet, risk perceptions, in a way, reflect the concerns of the public about the side effects of given technologies at stake that are commonly forgotten by technical approaches. In response to this dilemma, the study of the social perception of risk can contribute to the creation of public policies revealing social values; serving as an indicator of public preferences; documenting desired lifestyles; helping in the design of communication strategies and representing personal experiences in ways that may not be possible in the scientific assessment of risk²⁷⁰. The major weakness of the psychological approach, however, remains the focus on the individual and his/her subjective estimations of risk²⁷¹. The multiple dimensions that people use to make judgements and the reliance on intuitive heuristics and anecdotal knowledge make it hard, if not impossible, to aggregate individual preferences and to find a common denominator for comparing individual risk perceptions²⁷². Finally, some of these physical studies fail to explain why individuals select some characteristics of risks and ignore others²⁷³.

²⁶⁸ Covello, V. T. (1983) "The perception of technological risks: a literature review," *Technological Forecasting and Social Change* 23: 285-297. Fischhoff, B. (1995) *op. cit.* Fischhoff et al. (1981) *op.cit.*. Sjöberg L. (2000) "Factors in Risk Perception", *Risk Analysis* 20(1): 1-11. Slovic, P., Fischhoff, B. and Lichtenstein, S. (1985) "Rating the risks: The structure of expert and lay perceptions" in: Covello, V. T., Mumpower, J. L., Stallen, P. J. M. und Uppuluri, V. R. R. (eds.) *Environmental impact assessment, technology assessment, and risk analysis*. Berlin, Heidelberg, New York: Springer, pp. 131-156. Slovic, P. et al. (1986) *op. cit.* Slovic, P. (1987) *op. cit.* Slovic, P. (2000) *The Perception of Risk*. Earthscan.

²⁶⁹ Schmidt, M. (2004) *Investigating risk perception: a short introduction*. Available at: www.markusschmidt.eu/pdf/intro_risk_perception_Schmidt.pdf

²⁷⁰ Renn, O. (1992) "The social amplification of risk: theoretical foundations and empirical applications," *J.Soc.Iss.* 48(4): 137-160..

²⁷¹ Mazur, A. (1987). "Does public perception of risk explain the social response to potential hazard?" *Quarterly Journal of Ideology* 11: 5-41. Plough, A. and Krimsky, S. (1987) "The Emergence of Risk Communication Studies: Social and Political Context," *Science, Technology, and Human Values* 12(3 and 4): 4-10.

²⁷² Renn, O (1992) *op. cit.*

²⁷³ Dietz, T., Scott Frey, R. and Rosa, E. (1996) *op. cit.*

4.3.3 The socio-cultural approach

Public attitudes regarding risk issues do not usually present a uniform distribution of all the possible points of views, as they normally show a distribution with few vertices²⁷⁴, in correspondence to the most common standpoints among the sampled population. Given the limitations of the psychological approach, a sociological approach has been developed, in which the risks are not seen as objective properties that depend on how the world is physically configured, or subjective properties that depend on how individuals cognitively operate. The sociological approach considers risks as social constructs that depend on sociocultural factors associated with given social structures. Sociocultural perspectives include undesirable events that are socially constructed²⁷⁵ and 'real' consequences that are always mediated through different types of social interpretations, usually linked with distinct group values and interests. While psychological research includes the acceptance of risk as a result of subjective individual decision, the sociological approach focuses on the factors that make risks resulting dominant in certain social groups or how polarizations and conflicts regarding the distribution of risk may occur. From this perspective, the acceptance of technologies largely depends on issues such as social values, trust in institutions or the ways in which social media process information.

The socio-cultural perspective supports the need to anchor risk policies on the experience of inequities, unfairness and perceived organizational incompetence²⁷⁶. Given that many of the psychological perception variables, such as personal control and voluntariness, are also relevant to the socio-cultural approach²⁷⁷, the latter can help addressing the issues of fairness and competence and provide normative conclusions for legitimizing risk policies²⁷⁸. Sociocultural perspectives on risk can help to enrich risk management, they can identify and explain public concerns associated with different risk sources; explain the context of risk-taking situations; identify cultural meanings and associations linked with special risk arenas. They can also help to articulate objectives of risk policies in addition to risk minimization, such as enhancing fairness and institutional trust and reducing inequities and vulnerability; to design procedures or policies to incorporate these cultural values into the decision-making process and to design programmes for participation and joint decision making, Dialogue with the public can be organized in the form of advisory committees, citizen panels, formal hearings, and others. Finally, they help to design programmes for evaluating risk management performance and organizational structures for identifying, monitoring and controlling risks.

A cultural theory of risk has evolved over the past years to become an important framework for understanding how groups in society interpret danger and build trust or distrust in institutions creating and regulating risk²⁷⁹. Douglas and Wildavsky²⁸⁰, for instance, suggested that risk emerges as a culturally given way to respond to threats *within* the boundaries of a group, organisation or society and their definitions of reality and ways to maintain social order. From this view, risk is mainly understood as a function of the difference between the self and the others.²⁸¹ Cultural theory accepts the uniqueness of subjective individual positions but predicts a limited number of cultural biases in the collective representations of dangers. It looks at the relationships among human beings and argues: *Risks are defined, perceived, and managed according to principles that inhere in particular forms of social organisation. The cultural theory of risk also tries to explain why risks become politicized, defining risk in political terms means that it is a function of fairness considerations such as trust, liability distribution, and*

²⁷⁴ Ibid.

²⁷⁵ Renn, O (1998) *op. cit.*

²⁷⁶ Perrow, C. (1984) *op. cit.*; Short, J. F. (1984) *op. cit.*; Stallings, R. A. (1987) Organizational Change and the Sociology of Disaster. Dynes, R et al (eds) *Sociology of Disasters*. Dietz, T., Scott Frey, R. and Rosa, E. (1996) *op. cit.*

²⁷⁷ Renn, O. (1998) *op. cit.*

²⁷⁸ Wynne, B. (1984) "Public Perceptions of Risk" in Aurrey, J. (ed.) *The Urban Transportation of Irradiated Fuel*. London: Macmillan.

²⁷⁹ Tansey, J. and O'Riordan, T. (1999). "Cultural theory and risk: a review." *Health, Risk and Society* 1(1): 71-90.

²⁸⁰ Douglas, M. (1992) *Risk and Blame: Essays in Cultural Theory*. London: Routledge. Douglas, M. and Wildavsky, A. B. (1982). *Risk and Culture: An essay on the selection of technical and environmental dangers*. Berkeley: University of California Press.

²⁸¹ Zinn, O. (2006) "Recent Developments in Sociology of Risk and Uncertainty" *Forum Qualitative Research* 7(1).

consent²⁸². Cultural theory does not question the validity of technical procedures for hazard identification, but tries to explain why some issues become politicised and hence embroiled in disputes over the allocation of blame and the distribution of power, while others appear to be tolerated within norms of social values and trust.²⁸³

Over time, this perspective seems to have split up into two separate streams. A quantitative standardized approach contributes to the already developed research on risk perception, often in combination with the psychological approach. Combined, they attempt to integrate the ontological realism and the social construction of risk experience in a new framework, called the social amplification and attenuation of risk²⁸⁴. The concept of social amplification and attenuation of risk is based on the thesis that events pertaining to hazards interact with psychological, social, institutional and cultural processes in ways that can heighten or attenuate individual and social perceptions of risk and shape risk behaviour. Despite this quantitative development, a qualitative perspective in cultural studies of risk has also been developed and applied as to analyse different responses to risk.

In recent years, anthropologists and cultural sociologists have suggested that social responses to risks are determined by prototypes of cultural belief. Based on a number of studies on the organizational principles in tribal communities, one school of anthropologists has identified several generic patterns of value clusters that distinguish different cultural groups from each other²⁸⁵. In turn, it seems that, on the basis of these value clusters, different groups form specific positions on risk topics and develop corresponding attitudes and strategies. This approach, thus, suggests that cultural patterns structure the mind-set of individuals and social organizations and influence the adoption of certain values and the rejection of others. These selected values, in turn, determine the perception of risks and benefits. Risk approaches based on cultural prototypes are often employed to predict individual responses, and more specifically how individuals respond in their social roles as representatives of agencies, industries or private organizations.

From a methodological point of view, these types of studies are quite similar to psychological surveys, for they employ Likert scales on an agree-disagree response to preselected statements. The formalization of Douglas's ideas on pollution and danger in her earlier work²⁸⁶ came with the development of a formal typology based on two axes: grid and group. This typology has become the best-known element of the cultural theory of risk. Indeed, the typology is often confused with the theory within which it is embedded²⁸⁷. In *Essays in the Sociology of Perception*, Mary Douglas sets out the basic assumptions behind two axes of the typology. First she considers the minimum forms of commitment to life in a society postulated by political theory. These are represented in terms of the strength of allegiance to a group. Second she considers the extent of regulation within or without the group; this is the grid axis. From these two variables, there exist four possible social groups or prototypes. The first of these is the *entrepreneurial prototype*, which perceives risk as an opportunity to succeed in a competitive market and to attain personal goals²⁸⁸: members are less concerned about equity issues and would like the government to refrain from extensive regulation or risk management efforts. Second, she presents the *egalitarian prototype*, which emphasizes cooperation and equality

²⁸² Rayner, S. (1992) "Cultural theory and risk analysis" in Krinsky, S. and Golding, D. (eds.) *Social Theories of Risk*. Westport: Praeger.

²⁸³ Douglas, M. (1992) *op. cit.*

²⁸⁴ Kasperson, R. E., Renn, O., Slovic, P., Brown, H.S., Emel, J., Goble, R., Kasperson, J.X. and Ratick, S. (1988) "The social amplification of risk: a conceptual framework," *Risk Analysis* 8 (2): 177-187. Renn O., Kasperson R.E. and Slovic P. (1992) "The social amplification of risk: theoretical foundations and empirical applications," *J.Soc.Iss.* 48(4): 137-160.

²⁸⁵ Douglas, M. (1966) *Purity and Danger, An Analysis of Conceptions of Pollution and Taboo*. London: Routledge. Thompson, M. (1982) "A three dimensional model" in Douglas, M. (ed) *Essays in the Sociology of Perception*. London: Routledge. Douglas, M. and Wildawsky, A.B. (1982) *op. cit.* Rayner, S. (1987) "Risk and Relativism in Science for Policy" B.B: Johnson and, B.B. and Covelio, V.T. (eds) *The Social and Cultural Construction of Risk*. Dordrecht: Reidel.p23.

²⁸⁶ Douglas, M. (1970) *Natural Symbols, Explorations in Cosmology*. London: Penguin.

²⁸⁷ Boholm, A. (1996) "Risk perception and social anthropology: a critique of cultural theory," *Ethnos* 61(1): 64-84.

²⁸⁸ Rayner, S. (1987) "Risk and Relativism in Science for Policy" B.B: Johnson and, B.B. and Covelio, V.T. (eds) *The Social and Cultural Construction of Risk*. Dordrecht: Reidel.p23.

rather than competition and freedom, focusing on long-term effects of human activities and more likely to abandon an activity than to take chances. Third, she identified a *bureaucrat prototype*, which relies on rules and procedures to cope with uncertainty, as long as risks are managed by capable institutions and coping strategies have been provided for all eventualities, bureaucrats believe in the effectiveness of organizational skills and practices and regard a problem as solved when a procedure to deal with its institutional management is in place. Finally, the fourth prototype is the *group of atomized or stratified individuals*, who mainly rely on hierarchies with which they do not identify themselves. These people trust only themselves, are often confused about risk issues, and are likely to take high risks for themselves, but oppose any risk that they feel is imposed on them.²⁸⁹

4.4 Acceptability of surveillance-orientated security technologies

Until now we have been focusing our attention on a variety of different factors influencing public acceptance of a large variety of technologies: from nanotechnology, to nuclear energy, to genetically modified food. Although the factors identified by these different streams of literature are relevant, not to the same extent, to the study of public acceptability of surveillance-orientated security technologies (SOSTs), it is time to pay attention to those elements that play a key role for understanding public reactions to the introduction and application of SOSTs.

In the following section, therefore, we collect insights from streams of literatures directly related to the implementation of SOSTs. As previously discussed, the introduction and regulation of SOSTs has been usually framed in terms of a trade-off between security and civil liberties, especially the individual right to privacy. In the following section, thus, we outline and discuss the way privacy has been defined and conceived from different academic perspectives and we also present a concise typology of privacy dimensions that will help us to assess potential privacy risks of SOSTs. In the subsequent section, we revise and discuss those factors affecting public acceptability of SOSTs that have been identified through empirical and anecdotal evidences proceeding from national experiences collected across the nine countries represented in the SurPRISE project.

4.4.1 Privacy expectations and concerns

Privacy, which refers to the safeguard of a person's intimate spatial or social space, represents a complex idea that has been investigated and discussed from many different perspectives and over many years without finding any conclusive answer. Privacy can be conceived (1) as a moral value, if seen from an ethical perspective; (2) as a commodity, if seen from an economic perspective; and, (3) as a psychological state when interpreted from a psychological or socio-psychological stand.

From a legal perspective, privacy is a fundamental human right. It is recognized in the UN Declaration of Human Rights and its origins can be traced back to the arrest of eavesdroppers in England in the XIV century.²⁹⁰ In terms of privacy protection regulations, it is worth mentioning the Swedish *Access to Public Records Act*, which required in 1776 that all government-held information to be used for legitimate purposes. In 1792, the *Declaration of the Rights of Man and the Citizen* declared that private property is inviolable and sacred. In 1858 the publication of private facts was prohibited in France.²⁹¹ In 1890, American lawyers Samuel Warren and Louis Brandeis described privacy as "the right to be left alone" in

²⁸⁹ Renn, O. (1992) *op. cit.*

²⁹⁰ Michael, J. (1994) *Privacy and Human Rights*, UNESCO. In 1765, Lord Camden, striking down a warrant to enter a house and seize papers wrote, "We can safely say there is no law in this country to justify the defendants in what they have done; if there was, it would destroy all the comforts of society, for papers are often the dearest property any man can have." *Entick v. Carrington*, 1758-1774 All E.R. Rep. 45.

²⁹¹ The Rachel affaire. Judgment of June 16, 1858, Trib. pr. inst. de la Seine, 1858 D.P. III 62. See Jeanne M. Hauch (1994), "Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris", 68 *Tulane Law Review* 1219 (May).

a seminal piece on the right to privacy as a tort action.²⁹² Despite being a fundamental right, privacy is not an absolute right and it usually balanced against others rights, such as the right to security.

Yet security is not a stand-alone-right either, but it is often expressed in relation to liberty. For instance, article 3 of the Universal Declaration of Human Rights states that “Everyone has the right to life, liberty and security of person.”²⁹³ By the same token, in the European Convention on Human Rights, article 8 proclaims the following: “(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”²⁹⁴

Thus, security and privacy should be equally safeguarded, according to European principles, rather than being exchanged one at the expense one of the other. These and other considerations related to the right to privacy and security within the current European regulatory framework are deeply discussed and developed in the deliverable “D3.2 – Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy” and will not be further discussed here²⁹⁵. The rest of the section is devoted to understanding people’s privacy concerns and expectations. In doing so, we will rely on social science literature, particularly on the study of privacy from a socio-psychological and from an economic perspective.

Psychologists and socio-psychologists have investigated privacy functions and sub-dimensions for over 40 years now.²⁹⁶ For Margulis, “Privacy, as a whole or in part, represents control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability”.²⁹⁷ According to Altman, privacy refers to “the selective control of access to the self”.²⁹⁸ And for Westin “privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”²⁹⁹ All these definitions underline the necessity in social life for moments of withdraw from social interaction or concealment of intimate matters from public gaze. With regards to the relation of the individual to social participation, “privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small group intimacy or, when among large groups, in a condition of anonymity or reserve.”³⁰⁰ The possibility of setting some boundaries between the self and the society guarantees the safeguard on one’s emotional and mental integrity. ‘Withdrawal into privacy is often a means of making life with an unbearable (or sporadically unbearable) person possible. ... Guarantees of privacy, that is, rules as to who may and who may not observe or reveal information about whom, must be established in any stable social system’³⁰¹.

Westin’s theory posits four states of privacy: anonymity, solitude, reserve, and intimacy (see definitions in Table 3). Pedersen extends Westin’s typology by adding *isolation* and by distinguishing between

²⁹² Warren, S. Brandeis, L. (1890), “The Right to Privacy”, *Harvard Law Review* 4: 193.

²⁹³ United Nation (1948) “The Universal Declaration of Human Rights”, available at: <http://www.un.org/en/documents/udhr/>

²⁹⁴ Council of Europe (1950) “Convention for the Protection of Human Rights and Fundamental Freedoms - as amended by Protocols No. 11 and No. 14”, available at: <http://conventions.coe.int/treaty/en/Treaties/Html/005.htm>

²⁹⁵ Porcedda, M.G., M. Vermeulen et al. (2013). Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy. Deliverable 3.2, SurPRISE Project. Florence, European University Institute.

²⁹⁶ Margulis, S.T. (2003). “On the Status and Contribution of Westin’s and Altman’s Theories of Privacy” *Journal of Social Issues* 59(2): 411-429.

²⁹⁷ Margulis, S.T. (1977) “Conceptions of privacy: Current status and next steps”, *Journal of Social Issues*, 33 (3): 5-21, p. 10.

²⁹⁸ Altman, I. (1975) *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*, Monterey, CA: Brooks/Cole Publishing, p.24.

²⁹⁹ Westin, A.F. (1967) *Privacy and Freedom*, New York: Atheneum, p.7.

³⁰⁰ Ibid.

³⁰¹ Schwartz, B. (1968) “The Social Psychology of Privacy”, *American Journal of Sociology* 73(6): 741-752.

intimacy with family from *intimacy with friends*, and tests the implicit assumption about the relationship between types (states) and functions of privacy (see Table 4).³⁰² While privacy types reflect kinds of privacy behaviours, privacy functions reflect different privacy needs met by privacy behaviours. The model implies a dynamic utilization of various types of privacy by various kinds of people in various circumstances to achieve desired levels of privacy.

Thus, privacy is a mechanism that allows people to set boundaries between themselves and other people. As Simmel rightly points out, 'directly as well as symbolically, bodily as well as spiritually, we are continually separating our bonds and binding our separations'³⁰³. The process of boundary setting, continuously performed through social interactions, should not be considered trivial and be taken for granted. This process is a means of protection against power abuses, especially from governmental side. The creation of boundaries, moreover, enables, individuals to exercise self-determination, which, in turn, is a key element of one's own individual and relational identity. In spite of being a fundamental social dynamic, this process is now constantly challenged by the introduction of new ICT technologies that, by challenging the distinction between the physical and the digital space, question the validity of traditional categories such as the distinction between the private and the public sphere. New developments of SOSTs bring some examples of the increasing interconnection between digital and tangible aspects in the deployment and implementation of SOST systems. As reported in the deliverable "D 3.1 - Report on surveillance technology and privacy enhancing design", technologies such as smart CCTV not only capture images of a person's physical body but also analyse and make inference about one's behaviour and all this through the mining of digital data, either footages, spatial and temporal coordinates, or information about one's identity and activity.

Westin's States of Privacy (1967)	<i>Solitude</i> is being free from observation by others.	Pedersen's Privacy Types (1999)	<i>Solitude</i> refers to placing yourself in a situation where other people cannot see or hear what you are doing, e.g. going to one's bedroom and closing the door. This permits a person to be undisturbed.
	<i>Intimacy</i> refers to small group seclusion for members to achieve a close, relaxed, frank relationship.		<i>Intimacy with family</i> refers to being alone with members of one's family to the exclusion of other people.
	<i>Anonymity</i> refers to freedom from identification and from surveillance in public places and for public acts.		<i>Intimacy with friends</i> is like intimacy with family except that the reference group is friends. For both types of privacy the intent is to reduce contact with outsiders while increasing interaction with the group.
	<i>Reserve</i> is based on a desire to limit disclosures to others; it requires others to recognize and respect that desire.		<i>Anonymity</i> is seeking privacy by going unnoticed in a crowd of strangers. Going to a concert alone or going shopping in a large shopping mall would be examples.
			<i>Reserve</i> is controlling verbal disclosure of personal information to others (especially to strangers). For example, it involves keeping one's ideas and feelings to one's self, rather than expressing them openly to other people.
			<i>Isolation</i> involves using physical distance to separate oneself from others to obtain privacy.

Table 4. Comparison of Westin's and Pedersen's privacy states

³⁰² Pedersen, D.M. (1999) "Model for types of privacy by privacy functions", *Journal of Environmental Psychology* 19(4): 397-405. Westin's typology was originally tested empirically by Marshall, N.J. (1974) "Dimensions of privacy preferences", *Multivariate Behavior Research*, 9(3), 255-272.

³⁰³ Simmel, G. (1957), *Brücke Und Tür*, Stuttgart: K. F. Koehler, p. 1.

Westin's Functions of Privacy (1967)	<i>Personal autonomy</i> refers to the desire to avoid being manipulated, dominated, or exposed by others.	Pedersen's Privacy Functions (1997, 1999)	Autonomy: break some social norms; do things that don't fit my usual role; experience failure; try out some new behaviours.
	<i>Emotional release</i> refers to release from the tensions of social life such as role demands, emotional states, minor deviances, and the management of losses and of bodily functions.		<i>Rejuvenation</i> : recover my self-esteem; protect myself from what others say; take refuge from the outside world; recover from bad social experiences. <i>Confiding</i> : share personal ideas with loved ones; let others in on who I really am; confide in others I trust; express my emotions freely. <i>Contemplation</i> : discover who I am; determine what I want to be; meditate and reflect; plan future social interactions). <i>Creativity</i> : engage in creative activities; develop a new thought or idea; work on solutions to problems; nourish my creativity.
	<i>Self-evaluation</i> refers to integrating experience into meaningful patterns and exerting individuality on events. It includes processing information, supporting the planning process (e.g., the timing of disclosures), integrating experiences, and allowing moral and religious contemplation.		
	<i>Limited communication</i> sets interpersonal boundaries. <i>Protected communication</i> provides for sharing personal information with trusted others.		

Table 5. Comparison of Westin's and Pedersen's privacy functions

The digital and the physical world are so increasingly intertwined to challenge the appropriateness and validity of old and well established ideas, such as the distinction between what we deemed private or public. To respond to those challenges posit to privacy by digital media and information technologies, Helen Nissenbaum claims that there is a urgent need for *context-relative informational norms* to ensure the appropriate flows of personal information within distinctive social contexts.³⁰⁴ In her book "Privacy in Context",³⁰⁵ Nissenbaum explains why the private-public distinction, as useful as it may be in other areas of political and legal philosophy, is a terrible dead-end for conceptualizing a right to privacy and for formulating policy: one cannot restrict privacy rights and claims to the domain of the 'private' because contemporary socio-technical systems have blown away these clear distinctions.³⁰⁶ She also challenges the definition of privacy as control over information about oneself because privacy is better conceived 'neither a right to secrecy nor a right to control but a right to appropriate flow of personal information'³⁰⁷. Therefore, the right to privacy is "a right to live in a world in which our expectations about the flow of personal information are, for the most part, met; expectations that are shaped not only by force of habit and convention, but a general confidence in the mutual support these flows accord to key organizing principles of social life, including moral and political ones"³⁰⁸.

The adoption of 'context-relative informational norms' enabling the appropriate and respectful management of personal information becomes particularly important nowadays. In the current digital era, in fact, huge amount of data are generated daily by different actors, from internet users to public and private organisations. These data, which may or may not contain, or be attached to, personal information, represent nowadays the majority of data worldly produced. Social media, for example,

³⁰⁴ Nissenbaum, H. (2004) "Privacy as Contextual Integrity," *Washington Law Review* 79,(February): 119-158.

³⁰⁵ Nissenbaum, H. (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Palo Alto, CA: Stanford University Press.

³⁰⁶ Bennett, Colin J. (2011) "Review of Nissenbaum's Privacy in Context: Policy and the Integrity of Social Life", *Surveillance & Society* 8(4): 541-543.

³⁰⁷ Nissenbaum, H. (2010) *op. cit.*, p. 127.

³⁰⁸ *Ibid.* p. 231.

create massive data flows. With more than 465 million accounts Twitter produced roughly 175 million tweets every day.³⁰⁹ 30 billion pieces of content are shared on Facebook every month.³¹⁰ And recent forecasts say that data production will be 44 times greater in 2020 than it was in 2009.³¹¹

As private companies manage and own the infrastructures through which the information is created and stored, individuals feel to have very limited control over this information, even though it refers to them and has been created by them. Thus, the huge stream of personal data daily produced seems to be absolutely out of control from the user's perspective. This lack of control produces anxieties among people, especially Internet users, and has captured the attention of the scientific community, and triggered the issuing of stricter regulations worldwide.

The debate focuses on *information privacy*, which is defined as "one's ability to control information about oneself"³¹², as well as on *information privacy concern*³¹³. From an economic perspective privacy is all about whether or not and under what circumstances individuals are willing to disclose information about them. According to this model, people perform a privacy calculus in which risks and benefits of disclosure are balanced against each other. In this context privacy is interpreted as a commodity whose relative value changes according to personal preferences.³¹⁴ Privacy as a commodity can easily enter in a cost-benefit calculation.³¹⁵

As summarised by Alessandro Acquisti: "the economic consequences of information sharing for all parties involved (the data subject and the actual or potential data holders) can be welfare enhancing or diminishing. In choosing the balance between sharing or hiding one's personal information (and in choosing the balance between exploiting or protecting individuals' data), individuals and organizations face complex, sometimes intangibles, and often ambiguous trade-offs. Individuals want to protect the security of their data and avoid the misuse of information they pass to other entities. However, they also benefit from sharing with peers and third parties information that makes mutually satisfactory interactions possible. Organizations want to know more about the parties they interact with, tracking them across transactions. Yet, they do not want to alienate those parties with policies that may be deemed too invasive."³¹⁶

³⁰⁹ Dawson, K. and Ziv, D. (2012) "A Conversation On The Role Of Big Data In Marketing And Customer Service", in MediaPost Blogs: CRM, on the 25th of April 2012, available at:

<http://www.mediapost.com/publications/article/173109/a-conversation-on-the-role-of-bigdata-in-marketing.html#axzz2Hseo32Br><http://www.mediapost.com/publications/article/173109/a-conversation-on-the-role-of-big-data-in-marketin.html#axzz2Hseo32Br>

³¹⁰ McKinsey Global Institute (2011) "Big data: The next frontier for innovation, competition, and productivity", by James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, Angela Hung Byers, published in May 2011, available at:

http://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovationhttp://www.mckinsey.com/Insights/MGI/Research/Technology_and_Innovation/Big_data_The_next_frontier_for_innovation

³¹¹ CSC Leading Edge Forum (2011) "Data rEvolution Report", available at:

http://assets1.csc.com/lef/downloads/LEF_2011Data_rEvolution.pdfhttp://assets1.csc.com/lef/downloads/LEF_2011Data_rEvolution.pdf

³¹² Stone, EF, Gardner, DG, Gueutal, HG, and McClure, S (1983) "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations," *Journal of Applied Psychology* 68(3): 459-468. Bélanger, F, Hiller, J, and Smith, WJ (2002) "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes", *Journal of Strategic Information Systems*, 11(3/4): 245-270.

³¹³ Smith, H Jeff, Milberg, Sandra J, and Sandra J Burke (1996) "Information Privacy: Measuring Individuals' Concerns about Organizational Practices", *MIS Quarterly* 20(2): 167-196.

³¹⁴ Davies, S. (1997) "Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity", in Agre and Rotenberg (ed) *Technology and Privacy: the new landscape*, MIT Press,

³¹⁵ Bennett, C.J. (1995) *The Political Economy of Privacy: A Review of the Literature*, Hackensack, NJ: Center for Social and Legal Research.

³¹⁶ Acquisti, A. (2010) "Background Paper #3: The Economics of Personal Data and the Economics of Privacy", *The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines*, OECD Conference Centre, available at:

This perspective, besides considering privacy as a very narrow concept only related to information withholding, do not take into account situations where the individual is covertly monitored and do not chose to share information at all. In the case of wiretapping or Deep Packet Inspection, for example, people have no idea their communications can be scrutinised or manipulated by third parties. When neo-classical economics assumptions are applied in the privacy-calculus, economists can even arrive to conclude that the protection of privacy can create inefficiencies in the market, as it diminish the total information pool available and create incentives for prospective employees to lie.³¹⁷ Similarly, consumers may suffer privacy costs when too *little* personal information about them is being shared with third parties, rather than too much.³¹⁸ In contrast, the modern microeconomic theory of privacy, based on different assumptions—such as incomplete information and bounded rationality—suggests that, when consumers are not fully rational, or in fact myopic, the market equilibrium will tend *not* to afford privacy protection to individuals, and therefore privacy regulation may be needed to improve consumer and aggregate welfare.³¹⁹

Despite the fact that in the case of SOSTs citizens have virtually no power to decide whether they want to be under surveillance, the most common way of understanding the relationship between privacy and security is exactly, as suggested by economists, through a calculus and an assessment of emerging trade-offs. In addition, in the case of SOSTs an individual has no choice to balance or negotiate on privacy once a surveillance measure has been implemented. For this reason people do not feel in control and are concerned about their overall privacy, both the physical and the information privacy, and lawmakers have drafted rules to protect individuals from the interference and observation of institutional entities, either private or public.

To conclude, while information privacy refers to access to individually identifiable personal information³²⁰, *physical privacy* “concerns *physical* access to an individual and/or the individual’s surroundings and private space. The two types of privacy can be reconciled under the category of *general privacy*.”³²¹ In the following section we try to build on previous typologies of general privacy in order to take into consideration all potential problems and risks generated by the implementation of intrusive surveillance measures within modern socio-technical and digitalised realities.

4.4.2 Concise typology of privacy dimensions and functions

Roger Clarke, an experienced privacy consultant and advocate, identifies four constitutive dimensions of privacy.³²² They are: privacy of the person; privacy of personal behaviour; privacy of personal communication; and privacy of personal data. Finn, Wright, and Friedewald (2013)³²³ add other three dimensions and construct a *taxonomy of privacy types* comprehending: privacy of the person, privacy of behaviour and action, privacy of personal communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space and privacy of association (including group privacy). See *Table 5* for a comparison and complete explanation of each category.

<http://www.oecd.org/sti/interneteconomy/46968784.pdf>
<http://www.oecd.org/sti/interneteconomy/46968784.pdf>

³¹⁷ Posner, R. A. (1978) “The right of privacy”, *Georgia Law Review* 12(3): 393–422. Posner, R. A. (1981, May) “The economics of privacy”, *The American Economic Review* 71(2): 405–409.

³¹⁸ Varian, H. R. (1996) “Economic Aspects of Personal Privacy”, Technical report, University of California, Berkeley.

³¹⁹ Acquisti, A. and J. Grossklags (2007), “What can behavioral economics teach us about privacy?”, in Alessandro Acquisti, Sabrina De Capitani di Vimercati (Ed.), *Digital Privacy: Theory, Technologies and Practices*, pp. 363–377. Auerbach Publications (Taylor and Francis Group). Acquisti, A., L. John, and G. Loewenstein (2009), “What is privacy worth?”, in *Workshop on Information Systems Economics (WISE 2009)*.

³²⁰ Smith, H. Jeff, Dinev, Tamara and Xu, Heng (2011) “Information Privacy Research: an interdisciplinary review”, *MIS Quarterly* 35(4): 980–A927, p. 991.

³²¹ Smith, H. J., Dinev, T. et al. (2011) op. cit.

³²² Roger, C. (1997) “Introduction to Dataveillance and Information Privacy, and Definitions of Terms”, Original of 15 August 1997, latest revs. 16 September 1999, 8 December 2005, 7 August 2006, available at:

³²³ Rachel, L. Finn, Wright, D. and Friedewald, M. (2013) “Seven Types of Privacy” in Gutwirth, S.; Leenes, R.; de Hert, P.; Pouillet, Y. (eds.) *European Data Protection: Coming of Age*, Chapter 1, Dordrecht: Springer. DOI 10.1007/978-94-007-5170-5_1

The taxonomy proposed by Finn *et al.* can be seen as an interesting attempt to capture privacy in complex social settings, as are the ones characterising our societies, and it is certainly worth taking it as starting point for reflection. We must acknowledge, for instance, that the taxonomy encompasses several dimensions of general privacy, from information privacy, which is reflected in the category “privacy of data and image”, to physical privacy, which is certainly reflected in the category “privacy of location and space”. Another positive aspect of the taxonomy is its interest for emotions, thoughts and actions, which are constitutive dimensions of humanity. Another valuable aspect is the reference to civil liberties and freedoms in explaining why privacy is worth.

The main reason why we decide not to adopt Finn *et al.*’s taxonomy is because we consider that information privacy must be considered a distinct category, transversal to all dimensions of privacy. Moreover, the final aim of our analysis is to focus on privacy concerns related to privacy states, and not on privacy types by themselves. Finally, the seven categories present some overlaps and it is difficult to consider them perfectly mutually exclusive. This consideration can create some problems at the time of translating the seven types into a testable empirical instrument.

In the previous chapters we have argued that digital information constitutes such an important and invasive element of modern times that information privacy is the most investigated form of privacy.³²⁴ For this reason we need a model of privacy able to reconcile the digital and the physical world, to follow people in semi-public spaces, and to face the challenges posited by advanced tracking technologies. As we need to understand how privacy functions in the digital era, we need a theoretical model of privacy able to take into account some intrinsic aspects of modern times, such as:

- The limited usefulness of traditional interpretative categories like the distinction between the public and the private, due to the multiplication of semi-public spaces, like social media platforms;
- The increasing overlap between the digital and the real world, as proved by recent innovations like augmented reality;
- The growing surveillance power of organisations over individuals generated by the multiplication of situational tracking devices, like mobile phones, RFID or GPS systems.

We propose to work with a concept of privacy characterised by only four dimensions, as Westin suggests. We consider adopting Westin’s terminology while extending the scope of each category to comprehend not just psychological states but real life situations, informed by current technological innovations. We start from defining *general privacy* as the state of being free from unauthorised intrusion and observation and we keep the partitioning of general privacy into physical and information privacy. While by *information privacy* we mean individual control over personal information, according to mainstream literature; we define *physical privacy* as the safeguard of an individual’s space, which can refer equally to an individual’s body, geographical location, social environment, or communications. These four dimensions are also identified in the deliverable D3.2³²⁵. We use the same terminology used by Westin, but extend and change the definition of each category to take into account not just psychological states, but sociological aspects like the relationship between the individual and the space, either physical, or relational, or communicative. As a consequence, physical privacy is partitioned into four dimensions: *intimacy* of the body and close personal relationships; geographical and spatial *solitude*; *anonymity* of behaviour and association; and *reserve* of communications. In the next paragraphs we explain each category in detail, their functions and relationship with information privacy, which is considered a dimension transversal to the four physical privacy types, as showed in Figure 1.

³²⁴ Smith, H. J., Dinev, T. *et al.* (2011) *op. cit.*

³²⁵ Porcedda, M.G., M. Vermeulen *et al.* (2013). Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy. Deliverable 3.2, SurPRISE Project. Florence, European University Institute.

Dimensions of Privacy	Taxonomy of Privacy Types
<p>Clarke (1997)</p>	<p>Finn, Wright & Friedewald (2013)</p>
<p>(1) Privacy of the person, sometimes referred to as 'bodily privacy' This is concerned with the integrity of the individual's body. Issues include compulsory immunisation, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and compulsory sterilisation.</p>	<p>(1) Privacy of the person encompasses the right to keep body functions and body characteristics (such as genetic codes and biometrics) private. ... Privacy of the person is thought to be conducive to individual feelings of freedom and helps to support a healthy, well-adjusted democratic society. This aspect of privacy is shared with Clarke's categorisation.</p>
<p>(2) Privacy of personal behaviour. This relates to all aspects of behaviour, but especially to sensitive matters, such as sexual preferences and habits, political activities and religious practices, both in private and in public places. It includes what is sometimes referred to as 'media privacy'.</p>	<p>(2) We extend Clarke's notion of privacy of personal behaviour to privacy of behaviour and action. This concept includes sensitive issues such as sexual preferences and habits, political activities and religious practices. ... The ability to behave in public, semi-public or one's private space without having actions monitored or controlled by others contributes to "the development and exercise of autonomy and freedom in thought and action".</p>
<p>(3) Privacy of personal communications. Individuals claim an interest in being able to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organisations. This includes what is sometimes referred to as 'interception privacy'.</p>	<p>(3) Privacy of communication aims to avoid the interception of communications, including mail interception, the use of bugs, directional microphones, telephone or wireless communication interception or recording and access to e-mail messages. This right is recognised by many governments through requirements that wiretapping or other communication interception must be overseen by a judicial or other authority. This aspect of privacy benefits individuals and society because it enables and encourages a free discussion of a wide range of views and options, and enables growth in the communications sector.</p>
<p>(4) Privacy of personal data. Individuals claim that data about themselves should not be automatically available to other individuals and organisations, and that, even where data is possessed by another party, the individual must be able to exercise a substantial degree of control over that data and its use. This is sometimes referred to as 'data privacy' and 'information privacy'.</p>	<p>(4) We expand Clarke's category of privacy of personal data to include the capture of images as these are considered a type of personal data by the European Union as part of the 1995 Data Protection Directive as well as other sources. This privacy of data and image includes concerns about making sure that individuals' data is not automatically available to other individuals and organisations and that people can "exercise a substantial degree of control over that data and its use". Such control over personal data builds self-confidence and enables individuals to feel empowered. Like privacy of thought and feelings, this aspect of privacy has social value in that it addresses the balance of power between the state and the person.</p>

Finn, Wright & Friedewald (2013)	<p>(5) Our case studies reveal that new and emerging technologies carry the potential to impact on individuals' privacy of thoughts and feelings. ... Individuals should have the right to think whatever they like. Such creative freedom benefits society because it relates to the balance of power between the state and the individual. ... Privacy of thought and feelings can be distinguished from privacy of the person, in the same way that the mind can be distinguished from the body. Similarly, we can (and do) distinguish between thought, feelings and behaviour. Thought does not automatically translate into behaviour. Similarly, one can behave thoughtlessly (as many people often do).</p>
	<p>(6) According to our conception of privacy of location and space, individuals have the right to move about in public or semi-public space without being identified, tracked or monitored. This conception of privacy also includes a right to solitude and a right to privacy in spaces such as the home, the car or the office. ... When citizens are free to move about public space without fear of identification, monitoring or tracking, they experience a sense of living in a democracy and experiencing freedom. Both these subjective feelings contribute to a healthy, well-adjusted democracy. Furthermore, they encourage dissent and freedom of assembly, both of which are essential to a healthy democracy.</p>
	<p>(7) The final type of privacy that we identify, privacy of association (including group privacy), is concerned with people's right to associate with whomever they wish, without being monitored. This has long been recognised as desirable (necessary) for a democratic society as it fosters freedom of speech, including political speech, freedom of worship and other forms of association. Society benefits from this type of privacy in that a wide variety of interest groups will be fostered, which may help to ensure that marginalised voices, some of whom will press for more political or economic change, are heard.</p>

Table 6. Taxonomy of privacy types

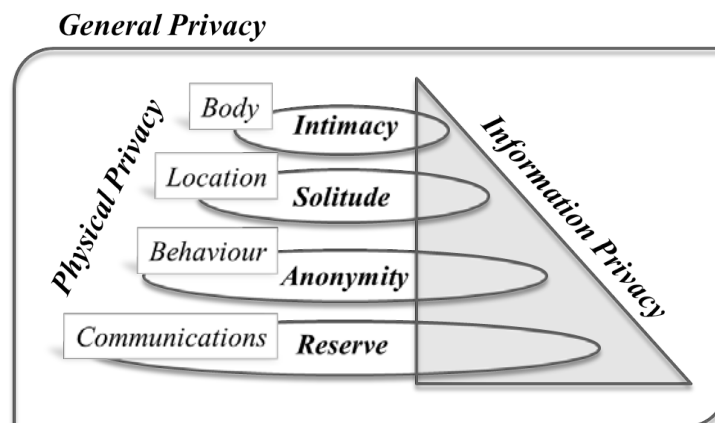


Figure 1. Relationship between physical and information privacy

Intimacy refers to the integrity of the human body, conceived as encounter of biological tissues and emotional states. It not only reflects the sacredness of the physical self, but also the need of respecting the most intimate relationships, like the ones between lovers, family members or close friends. We decide to comprehend in the same category the biological and the emotional part of the self because they strongly influence each other through both chemical reactions and interactions with the outside world. To bring some examples we may think of sexual preferences, which are partially biologically determined and partially socially constructed; but also the child-mother relationship, which is driven by both instinct and culture. Thus, intimacy concerns a due respect for intrinsic human conditions like birth, illness, love, and death. By extension, it entails the protection from publicity of medical

information, personal secrets, or signs of affection. Intimacy pursues two fundamental functions: on one side people can confide to love ones their feelings, anxieties and intimate thoughts; on the other side, people can take time to recover from distress produced in the outside world, relax and feel secure. Respecting intimacy means protecting human dignity, and physical and mental integrity.

Solitude concerns the right to move freely in the physical space, either to stay isolated and escape, or to go to places we like, without having to worry about being tracked or monitored. It reflects the need of making experience of different spatial contexts, from the top of a mountain, to a church, a public garden, a nightclub, a desert. This category emphasises the importance of the spatial context over the potential interactions, or lack of interactions, that in that place may be performed. In terms of functions, solitude helps people meditate and reflect about themselves, their expectations, desires with respect to the context. By helping people to reflect and connect with one's intimate soul, solitude helps people to freely expressing their consciences, in religious or secular terms.

Anonymity represents a way of protecting individual behaviour from collective pressure and expectations. In contrast to Solitude, anonymity refers to a situation where individuals do want to act and interact in public ad yet wish to be protected from social pressure by preserving their identity as unknown to the public. It is an important category for the functioning of democracies because it is a mechanism that leads to collective outcomes, such as the election of government through anonymous voting during elections, or the compilation of the census by citizens and the publication of national statistics. The possibility of detaching one's identity from behaviour, or to lose one's identity to be part of a crowd, helps people develop themselves through positive and negative experiences. Finally, a fundamental function of anonymity is helping people to experience new behaviours, make mistakes and being autonomous. Anonymity contributes also to people participation into collective action and political life by fostering the right of association and assembly.

Reserve is about being in control of one's expressive power through any form of communicative media. Conversations on the phone, correspondence sent through traditional or digital means, discussions during meeting or reunions are all communicative acts that deserve to be protected from third party intrusion through wiretapping or illicit hearing or recording. This principle implies that only invited people should participate to a conversation. Through reserve people can share their ideas with other people and being creative and innovative. Reserve, as a way of managing the communication flow, fosters self-expression and the right of being and staying informed.

Once we have presented our typology of privacy dimensions, we want to emphasise the danger and potential harms and adverse consequences of undermining privacy and its relevancy for human realisation and development. Since we consider privacy a fundamental precondition to human self-determination, self-expression and realisation, we want to identify the connections between privacy, liberties and fundamental rights especially within the European Union, and show in this way why it is important to care about privacy. As it has been noticed, 'in one sense, all human rights are aspects of the right to privacy'.³²⁶

We would start from the linkage between privacy and freedom and use Petersen's privacy functions³²⁷ and Westin's privacy types to better explain how our typology of privacy dimensions helps to tackle emerging threats to civil liberties and fundamental rights. We will use interviews, realised by Privacy International to various privacy experts and advocates, to show the relationship between privacy functions and fundamental rights within each privacy dimension.

Table 6 presents key definitions and relationships among privacy dimensions, privacy functions and related fundamental rights. The last column of the table presents quotes from interviews realised by Privacy International in the video 'Why privacy matters'. These quotes are used to clarifying each category by using a diverse, more direct language, and examples taken from real life. The second column from the left of the table associates some fundamental right, as stated in the Charter of Fundamental Rights of the European Union, to each privacy dimensions to show the correspondence, and proximity, between the safeguard of privacy and the fulfilment of these principles.

³²⁶ Volio, F. (1981) "Legal personality, privacy and the family" in Henkin (ed) *The International Bill of Rights*, New York: Columbia University Press.

³²⁷ Pedersen, D.M. (1997) "Psychological Functions of Privacy" *Journal of Environmental Psychology* 17(2): 147-156.

General Privacy		Article 7 - Respect for private and family life: Everyone has the right to respect for his or her private and family life, home and communications.		
Privacy Category		Fundamental Rights of the European Union ³²⁸	Privacy Function	Quotes from PI’s “Why Privacy Matters” ³²⁹
Physical Privacy	Intimacy refers to the integrity of the body, and the safeguard of its biological and emotional states. It can strictly refer to medical information as well as sexual orientation, and family relationships.	Article 1 - Human dignity: Human dignity is inviolable. It must be respected and protected. Article 3 - Right to the integrity of the person: 1. Everyone has the right to respect for his or her physical and mental integrity.	Confiding: (2) share personal ideas with loved ones; (11) let others in on who I really am; (13) confide in others I trust; (16) express my emotions freely. Rejuvenation: (3) recover my self-esteem; (6) protect myself from what others say; (9) take refuge from the outside world; (18) recover from bad social experiences.	“There are things that are private but not secret because we are vulnerable into them, or we look ridiculous.. the things you whisper to your lover late at night are not the things that you want to see on the front page of a newspaper the next day.. not because they are embarrassing, not because there are silly, not because no one else has said those words before, but because they are personal. And they lose some quality of that personal-ness when you have to disclose them.”
	Solitude, which means being alone, isolated from social interactions and free from observation by others, refers to the safeguard of the physical space wherein the individual is located.	Article 10 - Freedom of thought, conscience and religion: 1. Everyone has the right to freedom of thought, conscience and religion. This right includes freedom to change religion or belief and freedom, either alone or in community with others and in public or in private, to manifest religion or belief, in worship, teaching, practice and observance.	Contemplation: (5) discover who I am; (10) determine what I want to be; (14) meditate and reflect; (19) plan future social interactions.	“There is a remarkable gap between what is illegal and what other people will ostracise you for. And freedom, from my perspective, is the right to live your life like you want to not like you think everyone else think to.”

³²⁸ Charter of Fundamental Rights of the European Union (2000/C 364/01), Official Journal of the European Communities C 364/1, 18.12.2000, available at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf

³²⁹ Privacy International (2012) video "Why privacy matters" created by Michelle Leddon, posted online by Emma Draper on the 20th of November 2012, Featuring Cory Doctorow, Kade Crockford, Jameel Jaffer, Dan Kaminsky, Chris Soghoian, Marcia Hoffman, Moxie Marlinspike, Phil Zimmerman, Hanni Fakhoury and Eli O. available at: <https://www.privacyinternational.org/blog/why-privacy-matters>

	<p>Anonymity refers to freedom from identification and from surveillance in public places and for public acts. It reflects the necessity of letting people meet and behave as they wish, without imposing excessive control and social pressure on them.</p> <p>Reserve is based on a desire to limit disclosures to others; it requires others to recognize and respect that desire. It implies control over one's personal communications, in terms of recipients and contents of those communications.</p>	<p><i>Article 12 - Freedom of assembly and of association: 1. Everyone has the right to freedom of peaceful assembly and to freedom of association at all levels, in particular in political, trade union and civic matters, which implies the right of everyone to form and to join trade unions for the protection of his or her interests. 2. Political parties at Union level contribute to expressing the political will of the citizens of the Union.</i></p> <p><i>Article 11 - Freedom of expression and information: 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.</i></p>	<p>Autonomy: (4) break some social norms; (7) do things that don't fit my usual role; (12) experience failure; (20) try out some new behaviour.</p> <p>Creativity: (1) engage in creative activities; (8) develop a new thought or idea; (15) work on solutions to problems; (17) nourish my creativity.</p>	<p>"Privacy is the right to make mistakes... to think ideas that are probably fool ... To think things aloud without having everybody knowing what I've said"</p> <p>"I worry about a future where every website you go to, every link you click, everything you buy at the supermarket, every phone call you make, every place you go, you actually check yourself. Wait. If this shows up in the New York Times tomorrow, would I still have a job? Because that sort of living is not freedom. That's not a healthy place to be."</p> <p>"Privacy is necessary for creative expression, for taking risks..."</p> <p>"It is connected to freedom of inquiry: I wanna to be able to research what I want to research, to look into what I want to look into without being worrying that someone is looking behind my shoulders"</p>
Information privacy	<p><i>Article 8 - Protection of personal data: 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.</i></p>			<p>"If you can't be sure of the privacy of communication between you and your lawyer, you don't really have a lawyer!"</p>

Table 7. Relationships among privacy dimensions, functions and fundamental rights

4.5 Acceptance of security technologies in Europe: insights from the national reports

Despite a variety of approaches and theoretical perspectives may diverge on what are the most relevant factors when it comes to explain public acceptance of technologies in general and security technologies in particular, there is agreement that public attitudes, values and criteria may vary not only from technology to technology but also from country to country. In this section, we shall outline and discuss insights, evidences and anecdotes proceeding from the background review of national debates, technologies and issues performed by each of the members of the Consortium in their own respective country. These background review work has focused on the development and implications of the introduction of new security technologies in their own national contexts. The emphasis was given to the debates, controversies and emerging specific factors that are likely to have an impact on people's acceptability of new SOSTs. As a result, some technologies emerged as especially controversial in many of the European countries involved, although the reasons and the attitudes in these controversies may vary from country to country and indeed within the same country. For this reason, we have singled out these especially controversial technologies and we have reviewed how different postures, arguments,

issues and decisions have been emerged and evolved in each of the country involved. The aim was to show how the same technology may not only spark different reactions in different national contexts but also how even a similar reaction, say scepticism or rejection, may originate from different sets of arguments or problems. This section, therefore, is divided in different subsections, which look at the different technologies in each of the countries involved in the project.

4.5.1 Video-surveillance

Video-surveillance is widely used across Europe, though its distribution is quite uneven. Denmark has the world's highest concentration of CCTV cameras (1 camera to 15 inhabitants), while there are approximately twelve cameras, set up by the Police, in the entire Norwegian Country³³⁰. During the 1990s the United Kingdom home office spent nearly 80% of its budget on installing CCTV systems. It has been estimated that currently in UK there is 1 camera to 32 people.³³¹ Video-surveillance is used because it is considered to prevent crime, make citizens feel more secure, help police's investigative work and provide reliable evidence in court. Yet the effectiveness of video-surveillance as a preventive measure has been criticised saying that CCTV does not actually diminish crime occurrence but simply serves to move criminal activities from one area to another one. It seems that focused CCTVs surveillance is more acceptable than indiscriminate surveillance, in the sense that CCTVs are more acceptable when they target specific groups of suspicious individuals rather than when they are used to monitor indiscriminately³³². Quite consistently among the countries reviewed, lay people emphasize also the limited usefulness and necessity of implementing highly sophisticated CCTV systems and suggest investing in less expensive alternatives like streetlights.

In Hungary, surveillance cameras 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, but public authorities disclosed no official information about their location and function. Only in March 2007, after almost three years of litigation and a favourable sentence of the Supreme Court,³³³ HCLU - a privacy advocacy NGO - managed to receive information from the authorities on the location of cameras. This information was then made public through the publication of a map on Internet.³³⁴ Authorities have claimed that video cameras are efficient tools against crime. However, some NGOs have raised doubts about it and have demanded that rigorous studies on the impact of CCTVs were conducted. Another important reason behind the wide adoption of CCTVs, according to some investigative journalists, is the presence of companies involved in the "CCTV business", which try to have direct influence on policy makers³³⁵.

Although reasonably widespread and overall accepted, a number of controversial issues come along the adoption and implementation of video-surveillance. Management and duration of footage retention is a quite contested aspect. *"Videosurveillance systems should be activated only when other measures are inadequate or impracticable, any storage of images should be limited in time"*.³³⁶ There is also a preference toward passive CCTVs, which is usually checked only when a crime happens, with respect to active CCTVs, which is supposed to constantly monitor a space and help people in the control room to report immediately suspicious behaviour or criminal activity. There are also been public outcries related to the places where cameras have been located. For example, British people have complained

³³¹ URL: <http://www.guardian.co.uk/uk/2011/mar/02/cctv-cameras-watching-surveillance>

³³² Woodhouse, J (2010) CCTV and its effectiveness in tackling crime. Department of Home Affairs Standard Note SN/HA/5624

³³³ URL: <http://index.hu/belfold/kamter1017/>

³³⁴ Information available at: <http://geospace.hu/map2>

³³⁵ URL: http://index.hu/belfold/2009/05/18/kozteruletfelugyelok_is_kamerazhatnak/

³³⁶ <http://www.garanteprivacy.it/garante/doc.jsp?ID=1712680>

about the appropriateness of applying video-surveillance in schools,³³⁷ and German people are against street CCTVs positioned in front of private households.

*In 2006, the police installed CCTV cameras in the red light district Reeperbahn in Hamburg. These cameras were installed as a measure of crime prevention in public spaces. However, one resident of the houses in this area took upon judicial proceedings to achieve the stop of the optical surveillance of her home from the outside. The resident referred to a violation of her right to informational self-determination through the capture of window, door and balcony images of the house she is living.*³³⁸

In recent years there has been a sharp rise in relation to the installation of surveillance cameras in Spain. Its purpose is public security and citizens' safety, but they are being used for other purposes such as access control to neighbourhoods so that only residents can park or for traffic control. In general, Spanish people consider that CCTVs increase the capability of preventing crimes, contribute to the identification and capture of criminals and have a dissuasive power. In a recent debate on the use of CCTVs in the neighbourhood of Lavapiés, a multi-ethnic neighbourhood in Madrid, CCTVs have been presented as an example of racial discrimination rather than crime prevention. Although the camera have been introduced to improve the security and the safety of the local residents, in fact, they have been mainly criticized as an instrument of racial discrimination, given the specific ethnic composition of the neighbourhood. Surveillance cameras have also been considered from a different perspective, which focuses more on self-segregation than on active discrimination.

In 2011, the Hungarian State Railway Company started installing CCTV systems at its stations and on its trains.³³⁹ And since 2012, fines can be imposed in Budapest to people who violate traffic rules anytime these violations are recorded by surveillance cameras.³⁴⁰ In Austria, the use of CCTV was incrementally expanded. The security police law play a key role in this regard – it was amended several times and since 2005 it paved the way for significant extension of CCTV in public transport as well as neuralgic areas. Since then the police can define on their own in which areas and which cases to apply CCTV³⁴¹. In Norway, for instance, the police are allowed to set up CCTV anywhere without applying to the Data Protection Agency and yet there are only approximately twelve cameras installed by the police in the entire country, as opposed to about 20.000 private ones.³⁴² During major events, like the World Ski Championship in Oslo in 2011, additional cameras were introduced, but these were taken down after the event.

Not all Nordic countries, though, share the Norwegian approach: Denmark has the world's highest concentration of CCTV cameras per inhabitant. Danish perception and attitude towards surveillance has changed over time and today it is generally much more accepted than it was a few years ago, as it is generally considered that CCTVs help to prevent crime and increase the perceived level of security, apart from contributing to support the police's investigative work. There are limits though; only a minority of the participants can accept surveillance in all public places and in fitting rooms to prevent theft. Recent surveys, however, show that more cameras can also create a feeling of insecurity. One decisive factor when it comes to the acceptance of camera surveillance is whether it is passive or active cameras. The group discussions showed that the main part of the participants could accept passive cameras where the recordings are only looked through in case of an incident. Active cameras seem much more privacy infringing, probably because someone you are being actively watched and evaluated.

Pretty much like other European countries, in Switzerland, CCTVs are in place in a variety of places, including airports and train stations, and even in buses and trams. Face recognition cameras are operating at the boarding gates of Zurich airport, but other airports have not taken the plunge so far.

³³⁷ For more information see the right leaning campaign group "Big Brother Watch", at: <http://www.bigbrotherwatch.org.uk/>

³³⁸ Decision of the German Federal administrative Court of January 25th 2012, (Az.BVerwG 6 C 9.11).

³³⁹ <http://www.origo.hu/auto/20110208-bekamerazzak-a-vonatok-es-a-megallok-egy-reszet.html>

³⁴⁰ http://index.hu/belfold/budapest/2012/05/16/terfigyelo_kamerabol_is_buntet_a_rendor/

³⁴¹ <http://www.heise.de/newsticker/meldung/Ausweitung-der-Videoueberwachung-in-oesterreich-geplant-162226.html>,

³⁴² Teknologirådet og Datatilsynet 2013: Personvern. Tilstand og trender 2013.

Even though video-surveillance is subject of criticism in the country, several votes that took place on the installation of CCTV in municipalities showed that a majority of people actually consider it as an effective measure for crime prevention³⁴³.

4.5.2 Biometrics

The use of biometrics has a widespread use, for example, in the case of electronic passports. The European Council Regulation of 2004³⁴⁴ enforces EU member states to introduce biometric passports. The implementation process was accompanied by high public debate and serious concerns of privacy and legal experts about protection of fundamental rights³⁴⁵. Austria introduced biometric passports in 2009 and citizens are obliged to give two fingerprints when requesting a new passport. The fingerprints are stored on the electronic chip of the passport device³⁴⁶. In this case, controversies have emerged about the biometric information contained by passports, which in principle could be accessed by RFID reader. This is the case, for instance, in the UK: *"all passports and residency permits issues for the United Kingdom now contain biometric information, opposition to the passport highlights how the increase the risk of identity theft because the chips containing biometric information can be read with any RFID scanner"* (United Kingdom National Report). In Switzerland, biometric passports have been introduced since 2010, but their implementation has not been uncontroversial either: *"In summer 2008, the Parliament has adopted the legal bases necessary for the definitive introduction of biometrics passport, but opponents to this decision launched a referendum (any decision taken by the Parliament can be put to a referendum if it obtains 50'000 signatures of citizens). Swiss citizens thus voted on the introduction of the biometric passport in spring 2009 and accepted it to a slight majority (50.14%)."*³⁴⁷. In Italy the introduction of the electronic passport endowed with a RFID chip storing biometrics was proposed in 2005 but the plan was never to be implemented, *"the introduction of electronic passport endowed with an RFID chip storing biometrics was proposed in 2005 by the ministry of Foreign Affairs, the plan was never implemented because of the negative privacy consequences of RFID"* (Italian National Report).

Apart from biometric passports, biometric databases also exist. Austria, for instance, plays an important international role in DNA analysis since the 1990s. They introduced DNA-databases as part of the security police law and, since 2005, Austrian police took the lead of Interpol's DNA-database system. Austria today has the fourth biggest DNA database worldwide. Eventually, in 2008, the Ministry of Interior even announced plans to widen DNA analysis for smaller crimes (Austria National report). The police in Denmark use biometric DNA records, too. Although the Law 121 of 1981 prohibited the collection of sensitive data on citizens race, religion, political, opinion, disconnection law and practice, the Law n.85, approved in 2009, now allows the creation of DNA databases in Italy, too. In Hungary, law enforcement authorities also collect DNA samples from persons convicted of specific crimes and from suspects of crimes punishable by five years - or more - of imprisonment. The use of biometric data in criminal records is widely accepted by citizens³⁴⁸. Some important implications of DNA databases, however, are emerging in Norway, where the EURODAC database registering fingerprints can determine whether an asylum applicant or illegal immigrant has previously claimed asylum.³⁴⁹ It is known that several immigrants have tried to remove their fingerprints before arriving in Norway.

Finally, biometric identification systems are sometimes used to regulate access to workplaces. In general they are fingerprint scanners but, occasionally, palm scanners, iris scanners and systems using

³⁴³ Vidéosurveillance et risques dans l'espace à usage public: Représentation des risques, régulation sociale et liberté de mouvement. Travaux du CETEL (2006), p.17.

³⁴⁴ http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l14154_en.htm

³⁴⁵ <http://www.ad.or.at/index.php?/archives/21-Fingerabdrucke-im-Pass.html>
http://www2.argedaten.at/php/cms_monitor.php?q=PUB-TEXT-ARGEDATEN&s=79894vwi
<http://derstandard.at/2182198>

³⁴⁶ https://de.wikipedia.org/wiki/%C3%96sterreichischer_Reisepass

³⁴⁷ http://www.schweizerpass.admin.ch/content/pass/fr/home/ausweise/pass_10.html

³⁴⁸ http://www.prise.oew.ac.at/docs/PRISE_D5.6_Hungarian_Interview_meeting_report.pdf

³⁴⁹ https://www.politi.no/politiets_utlendingsenhet/aktuelt/nyhetsarkiv/2005_05/Nyhet_4365.xml

voice sample and ear sample are used. Similar systems are used in Spain and Hungary, but forbidden in Italy. According to the Danish Board of Technology the use of biometrics for access control in Denmark is more acceptable when the use of this technology is connected to specific situations and places. The group discussions indicated that the thought of a DNA-register is quite unfamiliar to the participants, even though such a register is in existence today.

4.5.3 Cyber-surveillance and data retention

A recent Eurobarometer has investigated citizens' attitudes towards the use, storage and exchange of personal data in several European countries. In Italy, 53% of respondents were not concerned whether personal data were retrieved and stored, and more than eighty per cent trusted that the police used their personal data in the proper way. An Italian survey conducted by the EurlSPES in 2009: confirmed that Italians generally trusted Carabinieri (69%) and Police (63%) as well as their data being held by public security forces (87%). The situation seems to be quite different in Germany, where citizens expressed an above-average level of trust (85%) in the police to appropriately handle their personal data but also expressed concerns about data privacy issues.

Since April 2012, Austrian internet- and telecom providers are obliged to implement the DR based in the European Directive from 2006 and keep record on phone calls and internet connections. The so-called "AK Vorrat" is a NGO, a civil society actor in organizing actions against the pre-storage of ICT data. A further controversial issue regarding profiling and data exchange is the agreement on profiling of flight passenger data with the US. Austrian critics denoted the draft as security hysteria towards Orwellian conditions. In April 2012, the majority of MEPs voted for the agreement. Shortly afterwards, plans went public about extending storage duration to five years and collecting additional data of flight passengers. Austria was the only country that raised serious privacy concerns.

In Norway, the 2006 *ISSP* The International Social Survey Program (ISSP) from 2006 showed that Norwegian citizens are positive towards giving the government extraordinary powers in case a terrorist attack is suspected. In practical terms, this implied, for example, that 86 % of the respondents approved wiretapping. The same study, in fact, shows how Norwegians have a strong trust in authorities. A later study, conducted by TNS Gallup in 2008 examined traveler's view on security in airports. 73 % of the respondents are satisfied with the security control on the biggest airport in Norway, and there is acceptance of the need for strong security (86%) and the rules that apply during the control (75%).

A similar level of trust towards public authorities has been found among Danes, who are less concerned about disclosing personal information online than the rest of the Europeans, and Danes have a strong trust that their online personal information is kept secure by websites and by public authorities (TNS Opinion and Social, 2012). Denmark is, in fact, a highly registered society. Until 1968 this kind of registration was decentralized. In the 1960's, due to the increasing development in IT, it was decided to create a central register with information about every citizen. In 1968 the civil registration system (Det Centrale Personregister, CPR) was created. Since 2004, the majority of civil registrations were made electronically. The civil registration number is a key to facts about the citizen - and the number is used when, for example, going to the doctor or submitting a tax return. Retention, scanning and combining of data, however, is acceptable for the majority of the Danish peoples only as long as the purpose is the investigation of specific terrorist attacks or crimes. When it comes to the use of these data for prevention purposes only a quarter of the participants to the above-mentioned survey is actually supportive.

The Spanish situation is altogether different, as we can observe a duality between public attitudes towards cyberthreats showing a general lack of attention given to individual protection of personal data and a low trust in the ability of the institutions to protect citizens in the cybercrime context. Spanish citizens in principle accept an expansion of data retention technologies and practices in case the police use the data belonging to criminals or in case databases are created to prevent terrorist attacks. On the other hand, Spanish citizens strongly oppose the use of these data for commercial purposes, which reveal a high sensitiveness towards this specific type of privacy infringement.

The Swiss situation stands at another extreme of the spectrum, as citizens show high level of concerns and trust public authorities but feel the latter should be given more powers and support to fight against crime and terrorism. Recent studies in Switzerland have explored trends in the opinion making of foreign, security and defence policy in Switzerland³⁵⁰. These studies, based on representative surveys of the Swiss electorate, demonstrate how the Swiss population is basically supportive towards measures to maintain homeland security: such as for instance, the control and penalization of hooliganism, the increase of police presence, the collection of data related to suspicious people and the engagement of the army to ensure peace and order, even if only 56% approves of violent breakups of demonstrations by the police forces. In the 2012 report of the Center for Security Studies³⁵¹, three out of four people approved video surveillance of relevant public spaces. A majority, however, rejects police surveillance of phone calls and private computers. The same study shows how four out of five respondents think it is important to fight against right-wing extremism (81%) as well as against left-wing extremism (67%). Nearly seventy per cent of the Swiss population is willing to accept restrictions of personal liberty in order to fight terrorism. Again, nearly eighty per cent support the idea of controlling the proportion of foreigners. However, regarding the question about entry inspections at public buildings, an ambivalent attitude of the Swiss becomes apparent as only about half of the respondents supported this measure.

Compared to the rest of the European countries, Hungary presents a different situation. Hungary is a relatively new democracy, and a great part of its citizens were socialized in the communist era, where privacy as a right 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 the workplaces - most of them owned and ran by the state -, the churches, as well as the residential communities. Even the letters arriving from abroad were opened and read before delivered to the recipients. At that time, the main technical solution was eavesdropping carried out via phone and listening devices, placed even in the homes of politically suspected citizens. Besides direct surveillance, all kinds of personal data were kept track of by the state authorities in a way that would be considered as unlawful today.

While in Germany, the earlier spying systems under the national socialist and the GDR regimes resulted in a significantly increased sensitivity regarding surveillance matters, in Hungary, this sensitivity can be observed only by particular groups of mostly elderly people. One of the reasons behind this difference might be that after the late 1950's, Hungarian socialism was much "softer" than that in the GDR and in other countries of the Eastern Bloc. Thus, it was often referred to as "soft dictatorship". From the 1960's onwards, Hungarian citizens were socialised partly to be ignorant and partly to run internalised self-control. After the change of the regime, the sense of threat disappeared, but not as the result of increase of trust in the society: *"Negligence was developed. Maybe there are things that disturb the people, but they do nothing about it"* – said an academic expert during the one in-depth interview of a qualitative research completed by Medián in 2012 on surveillance, privacy and security.³⁵² This opinion is confirmed by other sources. According to *"Special Eurobarometer 359 - Attitudes on data protection and electronic identity"*³⁵³, Hungary is among the countries where citizens are less concerned about privacy issues and tend to protect their privacy the least. A representative of a Hungarian NGO specialized in privacy issues argued that this attitude is based rather on carelessness and not on a conscious deliberation, – for an appropriate level of awareness and consciousness is missing. Very likely, the lack of awareness is also a serious problem behind the general indifference towards surveillance and towards the infringement of privacy. Some small groups of activists try to draw attention to this problem.

There is another group worth mentioning, which operates on the Budapest University of Technology and Economics. The group consists of young IT professionals and IT students that have created and continuously maintain the website "PET-portal" (<http://pet-portal.eu/>). Its content is accessible also in English and Dutch besides Hungarian. This group performs educational activity in the field of SOST and privacy, and tries to develop freely downloadable PET-solutions for protecting privacy on the Internet.

³⁵⁰ http://www.css.ethz.ch/index_EN

³⁵¹ http://www.css.ethz.ch/publications/DetailansichtPubDB_EN?rec_id=2081

³⁵² The research consisted of four in-depth expert interviews.

³⁵³ http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

There are only a few NGOs dealing with data protection and privacy issues, however, even these groups lack the support of the masses. Two very important NGOs, operating on the respective field are the Hungarian Civil Liberties Union³⁵⁴ (HCLU) and the Eötvös Károly Institute (EKINT)³⁵⁵."

4.5.4 Other Technologies and final remarks

Drones: The Swiss Army currently operates exploration drones that are used by the army, but also make services to civil authorities to security, for example, police borders or security during the Euro 2008. These drones are operating since several years and will reach within a few years the end of their term of use. To replace, Swiss government provides spend between 300 and 400 million francs, the main mission of new drones will be the exploration recognition airline, monitoring the territory and the assistance to border police (Switzerland National Report).³⁵⁶ The Hungarian army does not possess drones currently, but plans their acquisition. Under a drone-developing program, Hungarian companies have developed UAVs, which were presented to a wider public in October 2012.³⁵⁷

Body Scanners: In Norway in 2007 the Aviation Authority proposed to try body scanners in the security checkpoints, the strong reaction from public, labour unions and workers led to cancellation of the implementation. In Germany, the benefits such technologies to airport security could not be proven unambiguously, thus leading to the termination of the test deployment. In contrast, since July 2011, new facial scanners have been tested at the Spanish airports of El Prat and Barajas. While they have been in trial for some time at Manchester Airport, the lack of an unambiguous legal framework in Europe about the use of body scanners seems to have recently caused termination of their use in the UK. While the use of traditional scanners like those of metal objects in Spanish airports is considered as part of a routine, the scanner of the new generation, known as the *naked machine*, is perceived as substantially new, which often gives rise to a mixed feeling of uncertainty and distrust as well as curiosity and interest.

This brief overview of the different practices, sensitivities, debates and arguments existing and operating in the European countries, effectively confirms the complexity of the factors and criteria that are likely to have an impact in the way European citizens frame the acceptability of surveillance-orientated security technologies. On the one hand, it seems difficult, therefore, to identify single universally valid factors capable of explaining the different levels of acceptability that each and every SOST may enjoy in each European country. On the other hand, however, institutional, social and cultural factors emerge as crucial elements in the complex process leading European citizens to decide when, where, for what purposes and to what extent a surveillance-orientated security technology is acceptable. Although only at the level of anecdotal evidences, these outcomes, in many ways, seem to endorse the critiques made by the contextual approaches towards the deficit model in the studies on the public assessment of new technologies and, at the same time, seem to support also the claims of the socio-cultural approaches in risk analysis.

Despite this variety, and to a certain extent incommensurability of different factors and criteria, it is possible to identify a list of factors and criteria that seem to be relevant in most of the countries under study and relevant to the study of the acceptability of the majority of the technologies at stake. While the full list of these factors and criteria is summarized in the Table 7, here it is possible to make a brief summary of those factors and criteria that have emerged as a result of the overviews on security, technology and privacy performed by these national overviews. They have shown that different degrees of perceived surveillance exist as well as different degrees of perceived threats and insecurity in different countries. The same threat may be perceived as imminent and relevant in one country and as distant and less relevant in other countries. As you may expect, the experience of terrorist attacks, the level of public awareness on a given security issue or an authoritarian past may play a significant role in

³⁵⁴ In Hungarian: Társaság a Szabadságjogokért (TASZ)

³⁵⁵ Representatives of both institutes were asked in the in-depth interviews.

³⁵⁶ <http://www.bazl.admin.ch/dienstleistungen/02658/index.html?lang=fr>

³⁵⁷ <http://www.kormany.hu/hu/honvedelmi-miniszterium/hirek/a-katasztrofavedelemben-is-segithetnek-a-pilota-nelkuli-repulogepek>

this sense. The same seems to happen with surveillance practices, which may be perceived as very intrusive and/or very effective in one country and barely taken into consideration in another country.

This is partially due to the actual level of concern for privacy matters, which seems to vary significantly across countries. Spain and Hungary show very low levels of privacy concern while Germany seems to be exactly in the opposite situation. The level of trust in public authorities also emerged as a relevant factor, which seems to be strongly associated with the presence of a reliable implementation of the European data protection framework, for instance. The presence of reliable accountability/responsibility mechanisms if technology fails also seem to increase public level of trust towards public authorities

Another relevant factors emerging in the national reports is the familiarity with given technologies, which in some countries seems to enhance public acceptability, and in some other countries may actually foster resistance and rejection. Finally, two more factors seems to be playing a positive role in terms of public acceptability: the perception of a given technology as empowering and the restriction of the use of a given technology to specific groups of suspicious individuals and specific type of crimes and security threats.

4.6 Summary of potential factors

LIST OF FACTORS	THEORETICAL PERSPECTIVE / SOURCE	RELEVANT DIMENSIONS IN THE STUDY OF SOSTs
Scientific knowledge	Deficit Model	
Trust in technologies and scientists	STS / Contextual Approach	Trustworthiness of SOSTs operators
More deliberative decision-making process	STS / Public Engagement in Science and Technology	Engaging lay people in the design and assessment of SOSTs
Probability of undesirable consequences	Risk Analysis / Technical Approach	
Magnitude of damage of undesirable consequences		
Familiarity	Risk Analysis / Psychological Approach	Familiarity with SOST
Time proximity		Time proximity
Space proximity		Space proximity
Catastrophic potential		Risk-Benefit balance
Risk-Benefit balance		(perceived intrusiveness and perceived effectiveness of SOSTs)
Voluntariness		
Control		General positive or negative attitudes towards SOSTs
Compensability		
Past experiences		
Trust in institutions		Trust in the institutions managing SOSTs
Social Values	Risk Analysis / Sociological Approach	
Processing information in the media		
Privacy calculus	Privacy studies	Information and substantial privacy concerns
Privacy types and functions		
Information privacy concern		
Familiarity with SOST	Risk society perspective	Familiarity with SOST
Degree of perceived surveillance		Perceived level of security threat
Level of perceived threat and insecurity		
Recent terrorist attacks in the country		
Technologies perceived as empowering		Social proximity of SOSTs (i.e. perceiving of being the target of SOSTs)
Presence of reliable accountability/ Responsibility mechanisms		
Presence of strong data protection framework	National reviews	Trust in the institutions and operators managing SOSTs
Targeted vs. Universal surveillance		
Context of use of SOSTs		
Trust towards public authorities and technology operators		

Table 8. Factors identified in previous studies

5 Towards a theoretical model to explain acceptability of SOSTs

5.1 Introduction

This final chapter builds upon the revision of the literature offered in Chapter 5, and presents those empirical variables which are more likely to influence public acceptance of SOSTs. The chapter is organized as follows. We start with defining the dependent variable, i.e. *acceptability of SOSTs*, then, we present four groups of variables, coming from social studies of science and technology, the Risk perspective, and privacy and security studies. These variables are:

- 'Familiarity with SOSTs' and 'General Attitude Towards SOSTs: Technology Detractors vs Supporters' coming from STS literature;
- 'Perceived Intrusiveness and Perceived Effectiveness', 'Temporal, Spatial and Social Proximity', 'Perceived Level of Security Threat', and the variable 'security-privacy balance, from the risk perspective;
- 'Institutional Trustworthiness', from both STS contextual approach and the socio-cultural perspective in risk studies;
- 'Substantive Privacy Concern (Information and Physical Privacy Concern)' inferred from privacy studies.

The second part selects those variables more likely to have an impact on public acceptance of security technologies. The final outcome of this chapter is a theoretical model of the relationship between public acceptability and its more likely antecedents.

5.2 Understanding public acceptance and acceptability of SOSTs

5.2.1 Acceptability Vs. acceptance of SOSTs

We say that a technology is acceptable when it is capable or worthy of being accepted, which means that it is received favourably or with approval, and also capable of being endured, because it is tolerable, adequate and conforms to approved standards.³⁵⁸ Public acceptability does not (necessarily) imply acceptability from a legal or human rights perspective. Under specific circumstances SOSTs may enjoy high public acceptability but still be proportional and necessary in democratic societies or not pass further criteria of a permissible limitations test (see Chapter 4, D3.2)³⁵⁹. Public acceptability is therefore an essential necessary but by no means a sufficient condition for the implementation of particular SOSTs. In policy documents³⁶⁰ and in the academic literature,³⁶¹ the construct most widely preferred is *public acceptance*³⁶². Although widely used, this concept is never defined, and many authors

³⁵⁸ "Acceptable": Webster's Third New International Dictionary, Unabridged. Merriam-Webster, 2002. <http://unabridged.merriam-webster.com> (20 Jan. 2013).

³⁵⁹ Porcedda, M.G., M. Vermeulen et al. (2013). Report on regulatory frameworks concerning privacy and the evolution of the nrm of the right to privacy. Deliverable 3.2, SurPRISE Project. Florence, European University Institute. Also see Scheinin M. et al. (2009). Terrorism and the Pull of 'Balancing' in the name of security. Law and Security, Facing The Dilemmas. EUI Working papers Series, Law Department, 2009/1, pp.- 55-64.

³⁶⁰ European Commission, (2012) Action Plan for an innovative and competitive Security Industry" COM (2012) 417 final.

³⁶¹ For example see Siegrist, M. (2008) *op. cit.*

³⁶² See for instance, Venkatesh, V. Morris et al. (2003) "User Acceptance of information technology: Toward a unified view" MIS Quarterly, 27 (3) 425-478. Also see: <http://www.istheory.yorku.ca/Technologyacceptancemodel.htm>

chose the wording 'To what extent do you find acceptable the following technology for..?' for its empirical declination,³⁶³ leaving the concept unexplained.

In the questionnaire for his study on security systems, Sanquist defines 'Acceptability' as "the extent to which you approve of the security system and believe it should be implemented as a routine approach".³⁶⁴ Considering the adoption of SOSTs as a desirable or good-enough solution might be an appropriate definition within the context of this study. Another important distinction to make refers to the difference between 'acceptance' and 'acceptability'. In a not so recent article, addressing the public assessment of energy technologies, Renn suggested that there is often a discrepancy between behaviours and attitudes and that it is preferable to address, therefore, not so much how people actually behave, given that their behaviour is often influenced by a number of different factors which constrain citizens, but rather their attitudes, which reveals what they actually think and would do if they could freely choose. As a consequence, Renn suggested shifting the focus from acceptance to acceptability³⁶⁵. The public assessment of security technologies presents a similar situation, because SOSTs are usually imposed by public authorities on the citizens without the latter having really any choice on whether to adopt them or not. In other terms, these technologies are to be accepted even when citizens may not consider them acceptable. CCTV or biometric passports must be accepted or our freedom of movement will be seriously restricted, and yet citizens may well find these technologies unacceptable. Following Renn, thus, we consider more accurate referring to *acceptability*, rather than *acceptance*, within the context of this study. In fact, we are more interested in investigating those factors and criteria that make SOSTs acceptable, rather than describing what percentage of the population find SOSTs acceptable, which means how acceptance is statistically distributed in our sample. We will, of course, produce statistics describing what kind of people are more willing to find SOSTs acceptable, but we will mainly focus our attention on those factors that are likely to influence public acceptability of SOSTs.

To summarize, in order to understand citizen *acceptance* of SOSTs, which refers to public adoption of SOSTs, we propose to study those factors and criteria that primarily influence public *acceptability* of SOSTs, defined as the degree of public approval a certain security measure obtains at the time of being exposed to public scrutiny. For this reason we move the discussion from acceptance to acceptability, and especially to those factors and criteria that make a technology more or less desirable from a citizen's perspective. Thus, within the context of this study acceptability concerns the extent to which SOSTs are considered acceptable, while acceptance refers to the number of people who find SOSTs acceptable.

Acceptability is first and foremost an attitude expressed through an opinion, a preference or a judgement. In fact, considering something acceptable does not immediately imply an action to be taken. Nonetheless, if people find things acceptable, they are keen on proving them. In the case of genetically modified organisms (GMOs), people who found their development and use acceptable were more willing to buy GMOs food in contrast to people who did not find them acceptable.³⁶⁶

Understanding what characteristics make SOSTs acceptable is highly relevant if we want to prevent the waste of public money, citizen dissatisfaction and no security improvement. Focusing on attitude rather than behaviour is also important because a diverse mix of components influences them. We also need to take into account the complexities of acceptability, for the latter is not a monolithic concept: it could be rather framed as a continuum that goes from emphatic support, through indifference, to complete rejection and opposition.

³⁶³ Bronfman, N. C. and Vázquez, E.L. (2011). "A Cross-Cultural Study of Perceived Benefit Versus Risk as Mediators in the Trust-Acceptance Relationship", *Risk Analysis: An International Journal* 31(12): 1919-1934. Razzouk, N. Y., Seitz, V. et al. (2008). "Consumer concerns regarding RFID privacy: an empirical study", *Journal of Global Business & Technology* 4(1): 69-78.

³⁶⁴ Sanquist, T. F., Mahy, H. et al. (2008) "An Exploratory Risk Perception Study of Attitudes Toward Homeland Security Systems", *Risk Analysis: An International Journal* 28(4): 1125-1133.

³⁶⁵ Renn, O. (2010) "Public acceptance of energy technologies." Available at: <http://elib.uni-stuttgart.de/opus/volltexte/2010/5451/pdf/ren88.pdf>

³⁶⁶ Siegrist, M. (2008) *op.cit.*

The case of SOSTs, in fact, is much more controversial and it is almost impossible to identify an action we can equate to full acceptance. SOSTs are usually bought and managed by public authorities; thus, citizens face them only once they are adopted. As a result, when SOSTs trigger some collective outcry is usually too late in terms of investments and there are very few chances left to redesign the technology. So, we find more appropriate, within the context of this study, to investigate public acceptability of SOSTs as an attitude, rather than as behaviour.³⁶⁷

5.2.2 Distinction between factors and criteria influencing public acceptability of SOSTs

In investigating those elements that contribute to increasing or diminishing the degree of acceptability of a given SOST, we consider appropriate to distinguish factors from criteria influencing public acceptability of SOSTs. While a *factor* is *one of the elements contributing to a particular result or situation*, a *criterion* is *a standard on which a judgement or decision may be based*. Within the context of this study, criteria are those argumentations consciously used by citizens to explain their position vis-à-vis the acceptability of SOSTs. In contrast, factors represent those elements that influence people's opinions, but that people do not explicitly state or that they recognize only partially. Factors may be addressed by means of quantitative methods, while criteria can be better assessed qualitatively through table discussions and focus groups.

Risks associated with the technology, level of familiarity, gender and other personal features influencing opinions are all potential examples of factors affecting public acceptability. On the other hand, criteria are statements regarding conditions acceptable SOSTs should comply with. We can find some examples of criteria related to SOST in previous projects, like PRISE, which collected citizens' opinions through interview meeting,³⁶⁸ i.e. group interviews complemented by a questionnaire, in six European countries from May to July 2007. As stated in the project's report,³⁶⁹ the introduction of new SOSTs (a) should be gradual and transparent; (b) should occur always in a context of clear rules and widespread information; (c) should be focused on specific cases and places; (d) should be proportionate to the danger and the situation; and, finally, (e) should affect the private sphere of intimate life as little as possible.

In general, citizens' main concern was to avoid political abuses and a deterioration of the democratic framework of law and rights. Some participants questioned the appropriateness of using new SOSTs to address security problems, while others suggested restricting the adoption of new SOSTs *only* to specific crimes, in specific contexts and always under specific legal and institutional guarantees. Other participants acknowledged that SOSTs may be useful against terrorism, but expressed concern that an over-emphasis on terrorism may come at the expense of addressing other security threats that they perceive as more imminent and familiar.³⁷⁰

Anxieties regarding the professional and moral profile of SOSTs' operators led people to emphasize the importance of clear rules and reliable mechanisms of sanction in case of human errors. As someone suggested, a superficial or dishonest application of SOSTs might raise as many security concerns as the threats SOSTs were expected to address. Many participants insisted that the use of these technologies for commercial and political purposes was not acceptable. They were aware that *fear* could easily be exploited for both economic and political purposes; therefore they vividly expressed concern for potential political abuses, pointing at the difficulty of assessing when behaviour or an attitude of

³⁶⁷ Authors thank Prof Sally Dibb for her valuable contribution in raising this point.

³⁶⁸ Each meeting involves around 30 participants without any expert or professional knowledge about the technology at stake and of different ages and educational backgrounds. Before the meeting, participants had received informative material about the new technology and its potential implications. The meeting begins with an expert introducing the topic, where the main advantages and disadvantages of the technology are discussed and the participants have the opportunity to ask questions. Subsequently, the participants complete a questionnaire and then divide into focus groups of 6–9 people with a mediator.

³⁶⁹ Anders, J. and Holst, M. (2008) *D 5.8 Synthesis Report - Interview Meetings on Security Technology and Privacy*, PRISE Project, available at: http://www.prise.oeaw.ac.at/docs/PRISE_D_5.8_Synthesis_report.pdf

³⁷⁰ Pavone, V. and Degli Esposti, S. (2012) *op. cit.*

citizens may be defined as suspicious. In this respect, there was general awareness that errors may spring not only from the limits of the technologies but also from the limits of the people who operate them.

Citizens' apprehension about the introduction of SOSTs was often due more to their mistrust towards the institutions that were supposed to employ and regulate these technologies, than to their alleged lack of knowledge about science and technology. This outcome confirmed the validity of Brian Wynne's³⁷¹ emphasis on the importance of public participation in technology assessment, because the lay public assesses technologies not only on the basis of technical information, but also on the basis of other types of knowledge (institutional, legal, social, ethical), which are not technical but are nonetheless absolutely relevant when technologies jump from laboratory to policy and social domains. This complex, contextual form of assessment, therefore, is of great importance when policy decisions have to be taken but is often neglected by current assessment exercises, which are based merely on decontextualized, technical expertise.

Deliverables D3.2 and D3.3 address in details the legal and social criteria affecting public acceptability of SOSTs, therefore a detailed discussion of criteria would fall outside the scope of the present work. However, as we shall see later in the provisional model, some of these criteria need to be included in the research design of the Citizens Summit Event for extensive discussion during the space allocated for debate during the event, later to be analysed through qualitative methods. Examples of such criteria include, for instance, criteria of legal acceptability such as **necessity, proportionality** and **adequacy** (D3.2), but also social criteria of **convenience** and the availability of social alternatives, not necessarily based on technologies and/or surveillance (D3.3).

5.3 Factors influencing public acceptability of SOSTs

5.3.1 Familiarity with SOSTs

In the literature of risk analysis, it consistently emerged that the perceived risk of new technologies – which in our case is mostly but not entirely associated with SOSTs intrusiveness – is usually higher and more worrisome than the risk associated with already settled technologies. This is often due to the fact that we are more alert when it comes to assessing unknown risks. In fact, citizens usually tend to consider more acceptable risky technologies when the latter are familiar and form part of a daily practice. In the psychometric paradigm, when risk is a constant attribute of a technology, the perceived risk tends to fade owing to the process of increasing familiarization. Even though, technically speaking, the risk remains the same, with time and exposure citizens tend to gradually accept it.³⁷²

There is a distinction, however, between habituation and familiarization: the former occurs when citizens get used to being exposed to a risk, whereas familiarization occurs when citizens also are aware of the actual level of risk to which they are being exposed. New or exotic risks that have nothing to do with the known world are perceived as more dangerous. This is why some technologies often elicit resistance and prudent behaviour. Examples include nuclear power and genetic engineering. These examples cause additional problems in the habituation process because we are unable to perceive these risks with our five senses. Lay people are not able to control or observe such risks by themselves.

Another factor influencing familiarity is time. In contrast to immediate effects, delayed effects tend to hinder familiarity. The uncertainty of being exposed (or not) also influences familiarity. If we know we are exposed to a certain risk, we become familiar with it more quickly. Uncertainty plays a major role in risk perception. If a risk is known to science and/or to the affected public, then the contribution to familiarity is higher than if that risk is unknown³⁷³ In the case of the BSE infection crisis in Europe, a number of factors made it difficult to become familiar with that risk: the disease was relatively new, at

³⁷¹ Wynne, B. (2006) *op. cit.* Wynne, B. (2008) *op. cit.*

³⁷² Slovic P., Fischhoff B. and Liechtenstein S. (1986) *op. cit.*

³⁷³ Hazard B. and Seidel G. (1993) "Informationsbedingte und psychosoziale Ursachen für die Angst vor Gesundheitsschäden durch Radon" in: Aurand K., Hazard B and Tretter F. (eds.) *Umweltbelastungen und Ongste*. Opladen: Westdeutscher Verlag, pp. 113-132.

least to the public; it was not observable as contaminated and normal meat were indistinguishable to the consumer and the precise transmission of the disease and the danger of infection to humans were unknown to science. This was further aggravated by the long delay effect between actual infection and the outbreak of Creutzfeld-Jakob disease. Finally, the public didn't know if they were exposed or not, leading to a massive drop in beef sales. The table below summarizes the factors that increase or hinder familiarity with a certain risk.³⁷⁴

Increase		Hinder
Known to be exposed	↔	Unknown to be exposed
Known to science	↔	Unknown to Science
Immediate effect	↔	Delayed effect
Old risk	↔	New risk
Observable	↔	Not observable

Table 9. Factors that increase or hinder familiarity with certain risks

Familiarity is also linked with trust, as Siegrist and Cvetkivich explain.³⁷⁵ In their argument, when people are familiar with a given technology, no correlations between trust in scientific and/or public authorities and perceived benefits or risks are to be expected. In that case, people rely on their own knowledge in making judgements about risks and benefits and therefore social trust in experts or authorities is not needed.

5.3.2 General attitudes toward SOSTs: technology detractors Vs. supporters

A complex mix of personal characteristics, experiences, relationships with other people, knowledge and taste can lead a person to consider technological solutions in positive terms. Some people show a favourable attitude to technology, its development and implementation, even before knowing the new technology in any detail. In contrast, other people tend to be sceptical about the validity and appropriateness of technological solutions to fix problems or improve human conditions.

Cultural and local values also play a significant role on average. In a study about nanotechnology, Gaskell et al. compared the attitudes of European and US citizens, finding out that people in the US support nanotechnology within a set of pro-technology cultural values that link economic progress with technological advances. In contrast, in Europe there is more concern about the impact of technology on the environment, less commitment to economic progress and less confidence in regulation.³⁷⁶

Individual as well as contextual factors may equally influence people's general attitude towards technology, no matter if this attitude is positive or negative. In the context of this study we need to assess and control for the variable 'general attitude toward SOSTs' in order to disentangle its effect from the effect of other variables in assessing what count more at the time of influencing public acceptability of SOSTs.

5.3.3 Perceived intrusiveness and perceived effectiveness

As risk perception research and the psychometric paradigm are useful approaches for quantifying attitudes regarding security systems and policies, and can be used to anticipate significant public acceptance issues, Sanquist uses a psychometric survey to explore the acceptance of homeland security

³⁷⁴ Schmidt (2004) *op. cit.*

³⁷⁵ Siegrist, M. and Cvetkivich, G. (2000) *op. cit.*

³⁷⁶ Gaskell, G., Eyck, T. et al. (2005) *op. cit.*

technologies.³⁷⁷ In studying the perception of risks associated with these technologies, he obtains judgements concerning risks and benefits of various homeland security systems currently in operation.

Psychometric rating data were obtained from 182 respondents on psychological attributes associated with 12 distinct types of homeland security systems. Respondents were provided with definitions of the following specific security systems that were rated in the survey: airport passenger and baggage screening; explosive detector canines; hidden camera surveillance of individuals for gait analysis and facial recognition; data mining of individual business and financial transactions; passports with radiofrequency tags; monitoring of Internet and email; location tracking through global positioning satellite (GPS) in cell phones and cars; travel tracking through Secure Flight and other risk assessment systems; trusted traveller programmes to speed up security screening; national identity card; citizen observers; radiation monitoring at border crossings. Of the 12 systems studied, airport screening, canine detectors, and radiation monitoring at borders were found to be the most acceptable, while email monitoring, data mining, and global positioning satellite (GPS) tracking were found to be least acceptable.

Participants were asked to rate each of these systems on 14 individual attributes, using a 7-point Likert scale. Definitions of each attribute were provided to the respondents, and they rated each attribute with respect to each security system. The attributes rated were: transparency; control; personal benefit; national security; accuracy; equitability; validity; risk of disclosure; risk of false identification as a security threat; risk of financial loss; risk of embarrassment; intrusiveness; risk of civil liberties infringement; acceptability. The attributes included both positive and negative aspects. Some attributes were more general, such as 'personal benefit', while others were more specific to security, such as 'risk of false identification'.

For the sake our analysis we focus our attention on acceptability and report only the correlation between each attribute and this variable. As displayed in table 9, the variables that are more correlated with acceptability are: validity, risk of civil liberties infringement (with a negative sign), personal benefit, and national security. These findings suggest that these attributes contribute to the overall perception of security system acceptability. The risk of civil liberties infringement shows high positive correlations with attributes such as risk of disclosure, intrusiveness, risk of false identification, risk of financial loss, and risk of embarrassment. The inverse correlation between acceptability and risk of civil liberties suggests that respondents consider systems more acceptable to the extent that they do not represent potential risks to civil liberties.

The correlation structure of all the above-mentioned attributes is then summarised by means of principal component analysis. The solution leads to the extraction of two components, which accounted for 56% of total variance. The acceptability attribute is the only one showing a strong relationship with both components. In fact, it cross-loads positively with *perceived effectiveness*, but negatively with *perceived intrusiveness*. 72% of the variance in the acceptability attribute is accounted for by the two principal components, one capturing the positive aspects (perceived effectiveness) and the other the negative aspects (perceived intrusiveness).

Perceived effectiveness is related to overall perception of how worthwhile a particular security measure might be, greatly influenced by those attributes reflecting improvement in national security and addressing a valid threat. In this case, effectiveness encompasses both perceptions of technical performance (e.g. national security benefit, accuracy) and more general acceptability-orientated attributes (i.e. equitability, transparency, control). In contrast, perceived intrusiveness reflects the potential invasiveness of a security system.

³⁷⁷ Sanquist, T. F., Mahy, H., et al. (2008) *op. cit.*

	Acceptability
1. Transparency	0.38
2. Control	0.25
3. Personal benefit	0.64
4. National security	0.60
5. Accuracy	0.55
6. Equitability	0.49
7. Validity	0.65
8. Risk of disclosure	-0.54
9. Risk of false identification as a security threat	-0.46
10. Risk of financial loss	-0.39
11. Risk of embarrassment	-0.33
12. Intrusiveness	-0.54
13. Risk of civil liberties infringement	-0.65

Table 10. Correlation between acceptability and each attribute of the security system

The study demonstrated orderly relationships between specific security systems and psychological attributes related to their application. Principal components analysis showed that the largest percentage of variance is explained by a factor that captures the extent to which people believe the systems are effective. This includes enhancing national security, validity, deriving a personal benefit, accuracy, and general acceptability. Other significant attributes of perceived effectiveness include equitable application, transparency, and degree of control.

The other principal component extracted involves the intrusiveness of the technologies. This includes the risk of civil liberties infringement, general intrusiveness, embarrassment, risk of financial loss, the prospect for disclosure, and false identification as a security risk; acceptability is negatively correlated with this component.

5.3.4 Temporal, spatial and social proximity

Studies adopting the psychometric paradigm reveal a complex and ambiguous relationship between proximity to a hazard and risk perception³⁷⁸. Recent studies have established associations between residential proximity to potentially hazardous industry and concern.³⁷⁹ However, in a discussion of the relationship between spatial proximity to industrial plants and concern, Moffatt et al. actually suggests the contrary relationship.³⁸⁰ For instance, a study by Wiegman et al. in the Netherlands showed that residents living close to a chemical complex were less concerned than those living at least 15km away.³⁸¹ The authors attributed this to a 'social learning' effect based on day-to-day experience of the site. Indeed, in a study of accounts of risks associated with living close to potential sources of pollution,

³⁷⁸ Bickerstaff, K.; Simmons, and P. Pidgeon, N. (2006) *Public perceptions of risk, science and governance: main findings of a qualitative study of six risk cases*. Understanding risk working paper. Available at www.psych.cf.ac.uk

³⁷⁹ Irwin A, Simmons P and Walker G (1999) "Faulty environments and risk reasoning: the local understanding of industrial hazards", *Environment and Planning* 31: 1311-1326. Moffatt S, Bush J, Dunn C, Howel D, and Prince H (1999) *Public awareness of air quality and respiratory health and the impact of health advice*. Newcastle: University of Newcastle. Moffatt S, Hoeldke B, Pless-Mulloli T (2004) "Local environmental concerns among communities in North-East England and South Hessen Germany: the influence of proximity to industry", *Journal of Risk Research* 6: 125-144.

³⁸⁰ Moffatt et al (2004) *op. cit.*

³⁸¹ Wiegman, O, Gutteling, J M, Boer, H (1991) "Verification of information through direct experiences with an industrial hazard", *Basic and Applied Social Psychology*, 12: 325-339.

Burningham and Thrush observed a similar response within local communities.³⁸² They argue that while a problem may be apparent to 'outsiders' looking in on a neighbourhood, the 'insider' view can often be very different. However, such responses cannot be explained purely in terms of social learning. Rather they seem also linked to a more psychological form of denying one's own vulnerability. In other words when individuals or communities are exposed to chronic risks they either suppress an explicit recognition of the unsatisfactory situation with which they are faced, or create boundaries around familiar and secure areas of experience, in order to avoid unsettling psychological disruptions to daily life. These authors also found that it was much easier for people to characterize distant pollution as problematic and as an issue that demanded redress than it was for them to regard pollution within their own neighbourhood.

Another characteristic to be taken into account when it comes to explain the ambivalence of the proximity factor is related to the strategies employed by people to distance themselves (or their neighbourhoods) from risk. In his study of Cumbrian sheep farmers following contamination from the Chernobyl fire (1992) Brian Wynne showed how the farmers he interviewed expressed fears and suspicions about the effects of radiation while, at the same time, recognized their social dependence on the plant³⁸³. In other words the industry's regional dominance had led to something of a 'dependency syndrome', which manifested itself in local people 'burying' of a range of personal ambivalences and anxieties about the nuclear industry³⁸⁴.

Proximity could also generate a "Not In My Back Yard" effect in citizen's attitudes related to social rejection of facilities, infrastructure and services location, which are socially necessary but have a negative connotation. Different factors can generate a NIMBY effect, especially fear of loss of the perceived quality-of-life status and economic value of property. The NIMBY effect could be considered 'normal' owing to perceived risk and nuisances associated with some social and environmental facilities³⁸⁵. It includes fear of both objective and subjective risks (attributed risks) fear of loss of achieved well being and quality-of-life status; and fear of loss of the economic value of property. Literature analysing the phenomenon shows a constant mix of NIMBY triggering factors, which relate NIMBY both to previous causal factors -such as suspicion of management or technology- and to consequences which stem more from fear than from fact (fear of effects on health, fear of loss of economic value of property, economy or well-being).³⁸⁶ For instance, applying multivariate analysis, Hunter and Leyden argued that the NIMBY effect, rather than being attributable to concerns such as property values and aesthetics, depends mainly on two factors: fear of potential health effects -a consequence- and distrust in government management- an antecedent.³⁸⁷ Matheny and Williams³⁸⁸ in USA found that both distrust in technology and distrust in the capacity to maintain correctly working technological facilities and their management by public entities are NIMBY triggering factors.

In a qualitative study of six risk cases, Bickerstaff Simmons, and Pidgeon³⁸⁹ highlight five conclusions about the relation between proximity and social acceptability of risk technologies. First, in making sense of risk, in particular at an affective level, people used a series of 'local' framings. Those living in communities with an immediate spatial and temporal connection to the risk issue (particularly radioactive waste, mobile phone masts and GM crops) were more able to draw on a range of

³⁸² Burningham, K. and Thrush, D. (2004) "Pollution concerns in context: a comparison of local perception of risks associated with living close to a road and a chemical factory", *Journal of Risk Research* 7: 213-232.

³⁸³ Irwin et al. (1999) *op. cit.*

³⁸⁴ Wynne (1984) *op. cit.*

³⁸⁵ Pol, E., Di Masso, A. Castrechini, A. Bonet, M.R. and Vidal, T. (2006) "Psychological parameters to understand and manage the NIMBY effect", *Revue Européenne de Psychologie Appliquée* 56: 43-51.

³⁸⁶ Pol, E., Moreno, E., Guàrdia, J. and Iñiguez, L., (2002) Identity, quality of life and sustainability in an urban suburb of Barcelona: adjustment to City-Identity- Sustainability network structural model. *Environmental Behaviour*. 34 (1), 67-80.

³⁸⁷ Hunter, S. and Leyden, K., (1995) "NIMBY: Explaining opposition to hazardous waste facilities," *Police Studies Journal* 23 (4), 601-619.

³⁸⁸ Matheny, A. and Williams, B. (1985) "Knowledge vs NIMBY: Assessing Florida's Strategy for Siting Hazardous Waste Disposal Facilities", *Policy Studies Journal*. 14 (1), 70-80.

³⁸⁹ Bickerstaff, K.; Simmons, P. and Pidgeon, N. (2006) *op. cit.*

experiential resources to make sense of the problem. Second, people with some greater proximity to, or familiarity with, the relevant technologies and/or their impacts tended to adopt more pragmatic and often ambivalent positions, revealing both fears and anxieties about the risks as well as a recognition of the social and economic necessity of the technologies. They also held more consistent discursive positions than those dealing with the issue as new, or as geographically and temporally remote. Third, where the spatial and temporal aspects of risks (and benefits) were more immediate, most people were able to engage with or localize the technology at hand. These technologies and their implications were, or could be connected with, everyday salient issues. Fourth, proximity does engender a degree of familiarity with the relevant technology in a way that is consistent with 'social learning'. We have, however, argued such responses may also embed more complex psychosocial processes of fear, denial and economic dependence. Finally, while risks may share certain characteristics in terms of spatial and temporal proximity, the accessibility of cultural resources is critical to them becoming socially salient. In other words people use available symbols, ideas, images and metaphors to mediate their relationship with the technology and more broadly with the risk associated with the technology at stake.

In this work, proximity is composed of three dimensions: social proximity, space proximity and time proximity. The first one refers to the ambivalence associated with the acceptability of some SOSTs: for instance, if video surveillance focuses on criminals and not on common citizens it comes to be considered more acceptable than when it does not make distinction between criminals and common citizens. As the NIMBY syndrome suggests, space proximity is also relevant when it comes to establish where it is more acceptable to have surveillance-orientated security technologies (public spaces) and where it is not acceptable (private homes, private spaces). Finally, temporal proximity focuses on the possibility of misuses in the future, that is, the lack of trust about the future use of the information retrieved through SOSTs, which may negatively affect the acceptability of them.

5.3.5 Perceived level of security threat

It would be impossible to understand the level of acceptance of SOSTs without taking into account the seriousness of those threats that these technologies try to address and prevent. However, we are not interested in measuring objective level of threat -by means of crime statistics or equivalent figures -but to assess how people perceive threats around them. A number of contextual features or events can obviously influence public perception of threat.

Events that are more readily available in memory³⁹⁰ and that arouse negative feelings³⁹¹ lead to the exaggeration of risk. Risks are also exaggerated for events that are highly vivid, widely reported in the news, involuntary, responsible for a large number of deaths, and unusual.³⁹²

In October 2001, after 9/11 terrorist attacks, polls conducted in the US showed a stress reaction reflected in a steep rise, with respect to other years, of perceived security risk values.³⁹³ This kinds of situations may lead to the need of psychiatric support,³⁹⁴ especially among teenagers, who manifested very high levels of fear of dying after the attack.³⁹⁵

Personal threat and fear leads to a change in personal behaviour, which is called 'constrained behaviour',³⁹⁶ designed to minimize exposure to risk. For example, perceived risk of a hurricane

³⁹⁰ Thaler, R. H. (1983) "Illusions and mirages in public policy", *Public Interest* 73: 60–74. Lichtenstein, S., Slovic, P., Fischhoff, B., Layman, M., and Combs, B. (1978). Judged frequency of lethal events. *Journal of Experimental Psychology: Human Learning and Memory* 4: 551–578.

³⁹¹ Johnson, E. J., and Tversky, A. (1983) "Affect, generalization and the perception of risk," *Journal of Personality and Social Psychology* 45: 20–31.

³⁹² Huddy, L. Feldman, S. Capelos, T. and Provost, C. (2002) *op. cit.*

³⁹³ Gallup (2002) *Terrorism in the United States*, Poll Topics and Trends, available at: <http://www.gallup.com/poll/4909/terrorism-united-states.aspx>

³⁹⁴ Katz, C. L., Pellegrino, L., Pandey, A., Ng, A., and DeLisi, L. E. (2002) "Research on psychiatric outcomes and interventions subsequent to disasters: a review of the literature", *Psychiatry Research*, 110, 201-217.

³⁹⁵ Halpern-Felsher, B. L., & Millstein, S. G. (2002) "The effects of terrorism on teens' perceptions of dying: the new world is riskier than ever", *Journal of Adolescent Health*, 30, 308-311.

³⁹⁶ Ferraro, K. A. (1996) "Women's fear of victimization: Shadow of sexual assault?" *Social Forces*, 75:

improved hurricane preparedness,³⁹⁷ while perceived risk of crime increases the chances of owning a gun.³⁹⁸ Personal threat is much more likely than national threat to elicit fear, anxiety, and related somatic symptoms such as depression and insomnia.

Between the end of October and the beginning of November 2001 a survey of 1.221 residents of Long Island in Queens, New York, explored the degree to which personal and national threat affect perceptions of the consequences of terrorism.³⁹⁹ We must underline some peculiarities of this survey: 54% of people interviewed said that they, or someone in their family, knew someone who was missing, hurt, or killed in the 9/11 attacks. Women, Hispanic, white-collar workers and people with lower levels of education were most worried about being directly affected by new terroristic attacks.⁴⁰⁰ In addition, individuals who saw a future terrorist attack on US soil as more likely were more pessimistic about the future of the economy and the stock market.

Findings also show that personal threat influences people to change their behaviours. A significant numbers of people reported that they had exercised greater caution in handling the mail (as a consequence of the anthrax case), had spent more time with their families, had cancelled or postponed air travel, had altered vacation plans, had driven into Manhattan less, or had avoid public transportation. Thus, consistent with the crime victimization thesis, individuals who perceive themselves as the likely victims of crime tend to change their behaviour in ways that minimize their risk.⁴⁰¹ Thus, personal threat can motivate support for policies that minimize threat as well as lead to a distorted view of the magnitude of threat and its impact. On the basis of these considerations, we introduce the variable 'perceived level of personal security threat' in our model.

5.3.6 Security benefits and privacy risks: Discussing the 'trade-off' approach

Although privacy and security are framed often, both in academia and among policy makers, as inversely related categories -i.e. in a trade-off where more security always implies less privacy,⁴⁰² no empirical evidence to prove this assumption has ever been provided. In 2012, Pavone and Degli Esposti unpacked the implicit assumptions behind the trade-off model and ran an exploratory analysis on data collected as part of the PRISE project.⁴⁰³ In their study the authors consider that citizens find themselves in a trade-off position, where they are expected to trade part of their privacy for higher security, only when they perceive SOSTs as both security enhancing and privacy infringing. As presented in table 10, when confronted with SOSTs people can have at least four different reactions.

- They can consider SOSTs as useful in terms of security and with no risk for their privacy. This group, characterized by a high level of confidence in the context implementing SOSTs, consider security the main issue.

667–690.

³⁹⁷ Sattler, D. N., Kaiser, C. F., and Hittner, J. B. (2000) "Disaster preparedness: Relationships among prior experience, personal characteristics, and distress", *Journal of Applied Social Psychology*, 30: 1396–1420.

³⁹⁸ Smith, D. A. and Uchida, C. D. (1988) "The social organization of self-help: A study of defensive weapon ownership". *American Sociological Review*, 53, 94–102.

³⁹⁹ Huddy, L. Feldman, S. Capelos, T. and Provost, C. (2002) *op. cit.* *Personal threat* was assessed by two questions: "How concerned are you personally about you yourself or a family member being the victim of a future terrorist attack in the United States?" and "How worried are you that you yourself or someone in your immediate family might receive a letter in the mail at home or at work contaminated with the anthrax bacteria?" *National threat* was assessed by two questions: "How concerned are you that there will be another major terrorist attack on U.S. soil in the near future?" and "How concerned are you that there will be a major terrorist attack in the U.S. involving biological or chemical weapons?"

⁴⁰⁰ Women, older respondents and respondents with a low level of education gave larger risk ratings also in a study conducted in Sweden in 2002, wherein 294 respondents rated perceived risk of terrorism as low or very low. Source: Sjöberg, L. (2004) "The Perceived Risk of Terrorism" *Working Paper Series in Business Administration* 2002(11).

⁴⁰¹ Ferraro, K. A. (1996) *op. cit.*

⁴⁰² Pavone, V. and Degli Esposti, S. (2012) *op. cit.*

⁴⁰³ <http://www.prise.oew.ac.at/>

- They can consider SOSTs as a useless solution to enhance security, but as a very risky option for their privacy. This group, characterized by an overall concerned attitude towards SOSTs, gives priority to the protection of privacy as the fundamental issue at stake.
- They can consider SOSTs as useful in terms of security, but risky in terms of privacy. This is the group of people who consider that any increase in security can only come at the expense of privacy. They will, therefore, have to decide whether they are willing to trade some of their privacy in exchange for more security.
- Finally, they can consider SOSTs both useless to increase security and innocuous in terms of privacy. These people can either find the debate uninteresting or they could use alternative, unexplored categories to frame the relationship between privacy and security.

People in the third group are likely to adopt the trade-off model to frame the relationship between privacy and security, by considering them as exchangeable goods that can be traded. However, this does not imply that all people that see SOSTs as both privacy infringing and security enhancing would necessarily be willing to trade their privacy in exchange for more security. Some may, for instance, consider that the security increase is negligible compared to the privacy loss or some may feel that their security level is already sufficient. As a result, not all people that adopt a trade-off approach should be considered equally willing to trade. It is reasonable to hypothesise that adopting the trade-off approach is a necessary but not sufficient condition for people to be willing to trade privacy for security: other factors are, thus, likely to affect their ultimate willingness to trade privacy for security. Moreover, there are also people who think that privacy and security cannot be exchanged or traded as commodities. These people do not assess SOSTs in abstract terms, but in relation to the characteristics of the context where SOSTs are implemented. From this embedded viewpoint, citizens either expressed concern about the government's surveillance power and considered SOSTs mainly as privacy infringing, or trusted political institutions and believed that SOSTs effectively enhanced their security without necessarily infringing their privacy. In our analysis, which in the case of the trade-off will be performed at a general level, we aim at identifying in which category people cluster themselves, and how their position in any of the four clusters affects the way they consider SOSTs more or less acceptable. Conversely, we will also try to understand how the perceived levels of intrusiveness and effectiveness affect the way people identify themselves with any of the four possible clusters.

<i>Surveillance-orientated security technologies interpreted as ...</i>		
<i>... Security enhancing devices</i>	<i>... Privacy infringing devices</i>	
	Risky (Highly Intrusive)	Harmless (Not Intrusive)
Useful	<i>Trade-off position</i>	<i>Trusting attitude</i>
Useless	<i>Concerned attitude</i>	<i>Uninterested</i>

Table 11. Interpretation of SOSTs in relation to privacy and security

Another recent opinion poll study, run by Medián in September 2012, adds information about the size of each group above identified through a representative sample of the Hungarian population (N = 1000). According to this study, 44% of the Hungarians interviewed accepted balancing privacy and security, while 52% gave priority to privacy over security.⁴⁰⁴ Opinions of those who regularly use mobile and Internet technology were strongly divided and shown three main approaches to the relationship between privacy and security. 44% of respondents believe that people who do not have anything to hide, should not worry about their privacy. This group also says to trust national authorities in dealing

⁴⁰⁴ Medián Opinion and Market Research included a few questions on surveillance, privacy and security in its monthly Medián Omnibus data collection in September 2012. The sample of 1000 respondents was nationally representative for the population aged 18+.

with security issues. 32% of respondents are concerned about their privacy and do not trust national authorities in managing surveillance technologies. Finally, 24% of respondents say that they are not concerned about their privacy, though they did not generally trust national authorities in dealing with surveillance-related issues, because they did not believe that modern technologies, such as digital profiling, have enhanced the surveillance capacity of the government.

In terms of demographic characteristics, it is worth noting that people who are not worried at all about being observed, or by extension do not mind being under surveillance, have low education, neither very high nor very low household income, are relatively young (under 40) or very old (over 70), and prefer conservative over liberal thinking. Also those, who do not use tracking devices such as mobile phones and do not use the Internet, belong to this group.

5.3.7 Trust and institutional trustworthiness

The socio-cultural approach in risk analysis and the contextual approaches in the studies on the public assessment of new technologies converge on one important point: the acceptance and acceptability of new technologies depend on trust in institutions. However, some specifications are needed: citizens may trust the police in general, but they can still find a particular SOST applied by the police useless to improve security and/or harmful to my private sphere. It may work also the other way around: citizens can mistrust the police but they can still accept that police has to apply particular SOSTs, which citizens may perceive as useful to combat crime. Moreover, the fact that private agents, on behalf of the State or of the police, can implement SOSTs adds some complexity in the issue of trust and trustworthiness. Whereas citizens may trust the police, they may be much more suspicious towards private agents implementing for example CCTV systems.

Cultural theory has also made a valuable contribution by showing that people are not only concerned about the risks that are imposed on them but also about the process by which the decisions have been taken. In particular, these studies came to the conclusion that it would better for science, politics and democracy that those affected by a decision will also have the opportunity to be involved in the decision-making process. We also know from the public engagement literature that insufficient public involvement is often a cause for litigation and political protest.

Inspired by deliberative theories, cultural approaches replaced the conventional risk equation from the technical approach $R = PM$ with the equation $R = TLC$ shifting the emphasis to trust (T), liability (L) and consent (C). With an emphasis on fairness, Ortwin Renn and his colleagues⁴⁰⁵ proposed to anchor democratic procedures on a correct process based on building trust, including representativeness, generating non-distorting communication, and reaching open consensus. The key issues here are inclusiveness and consensus building. Although this literature is vast and to a certain extent controversial, these are the core outcomes:

- *Trust* is only possible if interested parties feel connected, respected, included and listened to.
- *Representativeness* is only possible if all participants are networked to all their constituent interests. This can best be achieved by the kinds of social impact connectors outlined earlier, and undertaken by local 'facilitators'. These are invaluable people who bridge individuals to their respective interest groupings by raising their awareness rising and by promoting direct communication.
- *Inclusiveness* is only possible when all the relevant parties are connected and trust one another. Inclusiveness is an outcome, not an input. It cannot be designed; it can only be achieved through a successful process.
- *Fairness* comes out of empowerment, which in turn is a product of genuine respect, and the revelation that other interests are part of one's own self-interest. To achieve fairness, therefore, there is need to achieve agreement about what principles underlie justice and appropriate treatment amongst the various social groups involved. This is unlikely to be

⁴⁰⁵ Renn, O., Webler, T. et al. (1995). *Fairness and competence in Citizen Participation*, London: Kluwer.

reached without a process of consensus building, the result of confidence in the process and in one another, and appropriate use of compensation or liability rules.

In terms of trust, a first lesson to be learned from socio-cultural and psychological approaches to risk perception is that the latter is located in two sets of psychosocial processes⁴⁰⁶. As *individuals* we look for pools of supportive attitudinal perceptions when responding to information, or communication, about risks. These pools are generally stable, but may 'pour' into other pools if the nature of the communication requires some sort of 'conclusive' reinterpretation. This took place for many in the early days of the BSE crises, and, we believe, is now occurring for many in light of the genetically modified organisms (GMO) controversy. However, as cultural types, we develop different outlooks about the world, and these provide us with a set of judgements about the fairness and reliability of communication about risk, which in turn affect our sense of trustworthiness of public institutions handling and communicating risk.

In more recent studies, authors have demonstrated that social trust towards those who manage a hazard is strongly correlated to judgements about the hazard's risk and benefits. When an individual lacks knowledge about a hazard, social trust of authorities managing the hazard determines perceived risks and benefits. When an individual has personal knowledge about a hazard and therefore does not need to rely on managing authorities, social trust is unrelated to judged risks and benefits. Results suggest that the lay public relies on social trust when making judgements of risks and benefits when personal knowledge about hazards is lacking.⁴⁰⁷

Social science research has demonstrated that technical experts and laypeople often differ in their conclusions about the risks and benefits of hazards⁴⁰⁸. Recent discussions have recognized the importance of social trust to judgements about risks and benefits and the acceptability of technologies⁴⁰⁹. Social trust will be significantly related to judgements of risk and benefits for hazards about which an individual has little knowledge.

In the absence of sufficient knowledge decision and judgements are guided by social trust⁴¹⁰. The function of trust, here, is to reduce the complexity people need to face. In other words, instead of making rational judgements based on knowledge, social trust is employed to select experts who are trustworthy and whose opinions can be considered accurate and reliable. It has been suggested that people have trust in experts who share the values that they believe are important in a given situation. Trust, therefore, has a strong influence on perception of the specific technology⁴¹¹. People having trust in the authorities and management responsible for the technology perceive less risk than people who lack that sense of trust having trust in those members, although some studies seem to suggest that this is not always the case.⁴¹²

It is also been hypothesized that social trust simultaneously influences both perceived risks and perceived benefits. For most technologies, the associated risks and benefits are not directly visible; therefore, people rely on risk-benefit information provided by sources they trust⁴¹³. Trust in authorities, companies and scientists involved in regulating or using a technology was found to have a positive influence on perceived benefits and a negative influence on perceived risks.⁴¹⁴ In a recent study Siegrist uses a causal model (Figure 2) to explain public acceptance of gene technology.⁴¹⁵ It was hypothesized

⁴⁰⁶ Tenney, J. and O'Riordan, T. (1999) *op. cit.*

⁴⁰⁷ Siegrist, M. and Cvetkovich, G. (2000) *op. cit.*

⁴⁰⁸ Fischhoff, B. et al. (1982) *op. cit.*

⁴⁰⁹ Cvetkovich, G. and Löfstedt, R. (eds) (1999) *Social trust and the management of risk*. London: Earthscan. Earle, T.C. and Cvetkovich, G.T. (1995) *Social Trust: Toward a Cosmopolitan Society*. Westport, CT: Praeger.

⁴¹⁰ Earle, T.C. and Cvetkovich, G.T. (1995) *op. cit.* Luhmann, N. (1989) *Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität* Enke, Stuttgart

⁴¹¹ Bord, R.J. and O'Connor, R.E. (1992) "Determinants of risk perceptions of a hazardous waste site", *Risk Analysis* 12: 411-416.

⁴¹² Sjöberg, L. (1999) "Perceived competence and motivation in industry and government in risk perception." in Cvetkovich and Löfstedt (eds). *Social trust and the Management of risk* London: Earthscan. pp. 89-99.

⁴¹³ Siegrist, M. and Cvetkovich, G. (2000) *op. cit.*

⁴¹⁴ Pavone, V., and Degli Esposti, S. (2012) *op. cit.*

⁴¹⁵ Siegrist, M. (2000) *op. cit.*

that trust in institutions using gene technology or using modified products has a positive impact on perceived benefits and a negative influence on perceived risks of this technology. In other words, trust has an indirect influence on the acceptance of the technology. He found that people lacking knowledge about gene technologies relied on social trust to reduce the complexity of risk management decisions⁴¹⁶. Trust in scientific and regulatory institutions resulted in a positive evaluation of biotechnology. A study by Hoban, Woodrum and Czaja⁴¹⁷ yielded similar results on the negative side. Lack of faith in the information given by institutions involved in gene technology was a significant predictor of opposition to genetic engineering.

One of the open questions raised by research is the dimensionality of trust. Frewer et al.⁴¹⁸ have claimed that trust is a multidimensional construct; however in their study they investigated factors that have an influence on trust in a variety of information sources. The importance of trust for the explanation of risk perception has been demonstrated in several domains. Freudenburg⁴¹⁹ found that people who placed trust in current scientific and technical abilities to build safe nuclear waste disposal sites were less concerned about a hypothetical nuclear waste repository in their country than people with no trust in the relevant institutions. In another study investigating factors determining opposition to a radioactive waste repository, it was shown that trust in management had a strong influence on perceived risk⁴²⁰. A negative association between perceived risk and trust in experts, government, and industry was also observed in several other studies.⁴²¹

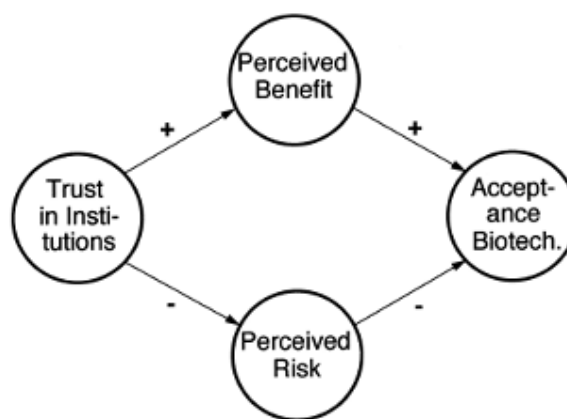


Figure 2. Model of Trust and Acceptance (Siegrist 2000)

When it comes to assessing new technologies, trust in public institutions is not determined merely by citizens' lack of knowledge or by the similarity of salient values between citizens and these institutions but also by their perceived trustworthiness. In other words, the extent to which an individual may engage with surveillance-orientated security technologies (SOSTs) will depend on the extent to which that individual perceives the security agency using the SOSTs as trustworthy. Akter et al (2010) define

⁴¹⁶ Earle, T.C. and Cvetkovich, G.T. (1995) *op cit.* Luhmann, N. (1989) *Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität* Enke, Stuttgart.

⁴¹⁷ Hoban, T., Woodrum, E. and Czaja, R. (1999) "Public opposition to genetic engineering" *Rural Sociology* 57: 476-493

⁴¹⁸ Frewer, L.J., Howard, C., Hedderley, D., Shepherd, R. (1996) "What determines trust and information about Food-Related Risk? Underlying Psychological Constructs," *Risk Analysis* 16: 473-486.

⁴¹⁹ Freudenberg, W.R. (1993) "Risk and Recreancy: Weber, the Division of Labor, and the Rationality of Risk Perceptions," *Social Forces* 71: 909-932.

⁴²⁰ Flynn, J., Burns, W., Mertz, C.M., Slovic, P. (1992) "Trust as a Determinant of Opposition to a High-level Radioactive Waste Repository: Analysis of a Structural Model" *Risk Analysis* 12: 417-429.

⁴²¹ Flynn, J., Slovic, P., Mertz, C.M. (1994) "Gender, Race, and Perception of Environmental Health Risks" *Risk Analysis* 14: 1101-1108. Cvetkovich, G. (1999) "The attribution of Social Trust" in Cvetkovich, G. and Löfstedt, R. (eds) *Social Trust and Management of Risk* London: Earthscan.

trustworthiness as a willingness to depend on a third party in a situation of risk. It can be distinguished from trust in two ways. First, trust refers to action whereas trustworthiness relates to a willingness to act. Trust relates to whether one actually relies on a third party in times of vulnerability, risk or crisis whereas trustworthiness relates to an individual's beliefs about whether that third party can be relied upon and hence their willingness to so rely on that party. In effect, trustworthiness refers to the properties of the trustee and how they serve the interests of the truster. Second, trust is something that is experienced at an interpersonal level, whereas trustworthiness can be experienced between individuals and other social entities, such as organizations. Accordingly, institutional trustworthiness is primarily conceptualized as an individual's willingness to trust in what the institution does and what it stands for rather than the people who work within it. Thus, institutional trustworthiness is discussed in terms of the roles, rules and norms of the institution rather than specific individuals.⁴²² Citizens cannot possibly know the interests, incentives and actions of the individual role holders of government institutions. Hardin (2002) suggests that citizens can form 'quasi trust', 'grounded in inductive expectations from past behaviour or reputation' about the trustworthiness of government'.⁴²³

As Searle et al. (2011) point out:⁴²⁴

'Carnevale⁴²⁵ defines it [trustworthiness] as the "faith that an institution will be fair, reliable, competent, and non-threatening". Thus, [institutional] trust hinges on the "collective characteristics of an administrative organization and top management group which are not reducible to features of individual actors and which ensure some continuity of activities and direction when those actors change".⁴²⁶

The risk-based definition of trustworthiness highlights its relevance in relation to SOSTs. SOSTs are deployed to manage particular risks and may render the individual who is subject to them vulnerable or at-risk because of the level of scrutiny to which they are subject. An individual's willingness to enter into a situation where they are at risk, or where the situation itself poses a threat, will be influenced by the degree to which they perceive the institutions charged with securing that situation as trustworthy. More generally, the expansion of the surveillance society by the gathering of data on populations for security purposes, as we see in, for example, financial services surveillance across Europe, certainly has the potential to impact institutional trustworthiness. This is first because to possess surveillance capacity is to possess great power, and to intensify it intensifies and centralizes that power. Second, the centralization of that power through increased information flows and information processing in databases may render that institution less transparent to the outside. Beliefs about the institution, its role and what it stands for may thus be transformed or distorted when surveillance is intensified and more or new information is demanded from citizens.

Recent developments in the measurement of institutional trustworthiness will be drawn upon in SurPRISE. To a degree these recent developments have emerged from a now well-established body of literature, which examines the antecedents of trusting behaviours. Although in this deliverable and in the model we focus on trust as a construct, we have to be aware that trust is a second order construct in that it is derived from a number of components relating to the characteristics of the trustee. In 1995, Mayer, Davis and Schoorman established that trusting behaviour is related to a truster's assessment of the ability, benevolence and integrity of the trustee.⁴²⁷ To use colloquial terms, trusting behaviour is related to whether the truster believes that the trustee is competent at what they do, acts kindly towards others and acts reliably, honestly and ethically. Searle et al (2012) argue that trustworthiness can be measured in these terms by focusing on the trustees' perception of these dimensions as

⁴²² Cook, K. S., Hardin, R. and Levi, M. (2005) *Co-operation Without Trust?* New York: Russell Sage Foundation.

⁴²³ Hardin, R. (2002) *Trust and Trustworthiness* New York: Russell Sage Foundation, p.135.

⁴²⁴ Searle, R.H., Den Hartog, D.N., Weibel, A., Gillespie, N., Six, F., Hatzakis, R. and Skinner, D. (2011) Trust in the Employer: The Role of High Involvement Work *International Journal of Human Resource Management* 22(5), pp 1069 – 1092.

⁴²⁵ Carnevale, D. G. (1995) *Trustworthy Government: Leadership and Management Strategies for Building Trust and High Performance* (1st ed.), San Francisco: Jossey-Bass Publishers, p. 11.

⁴²⁶ Whitley, R. (1987) "Taking Firms Seriously as Economic Actors: Towards a Sociology of Firm Behaviour. *Organization Studies* (Walter de Gruyter GmbH & Co. KG.), 8: 125-147, p. 133.

⁴²⁷ Mayer, R. C., Davis, J. H. and Schoorman, F. D. (1995) "An Integrative Model of Organizational Trust" *Academy of Management Review*, 20: 709-734.

characteristics of the truster. These authors also advise to taking account of procedural justice when assessing institutional trustworthiness. Procedural justice refers to the perceived level of bias in decision-making, and whether the trustee is perceived to take account of all relevant information and interests when making decisions. This perspective was also adopted by Sunshine and Tyler (2003)⁴²⁸ in a body of work examining the public perception of policing practices. Mayer, Davis and Schoorman's (1995) tripartite model has formed the basis of trustworthiness studies elsewhere in the social sciences: for instance, in the mobile-health information systems case,⁴²⁹ and the e-government context.⁴³⁰ Searle et al (2012)⁴³¹ and by Niehoff and Moorman (1995)⁴³² and Sunshine and Tyler (2003) have been established scales concerning institutional trustworthiness⁴³³ and concerning procedural justice. These scales will be adapted for the SurPRISE questionnaire⁴³⁴.

5.3.8 Privacy concern

In our concise typology of privacy dimensions and functions, presented in the previous chapter, we have claimed that general privacy can be divided into information and physical privacy. Physical privacy is then partitioned into four dimensions, which are: intimacy, solitude, anonymity and reserve. Each dimension identifies a portion of personal space which needs to be protected from intrusion. In detail: *Intimacy* refers to the protection of an individual's body and feelings; *Solitude* concerns the defence of one's geographical location; *Anonymity* implies the safeguard of social relationships and social behaviour; *Reserve* is about guarding communications from prying.

We have also said that information privacy crosses all dimensions of physical privacy, because the digital recording of human activities equally embraces medical information, geolocation data, social relational networks, and electronic communications. Table 11 provides some examples of situations that belong only to physical privacy, or that also belong to information privacy. In general, the recording of data is what triggers the intervention of the information privacy category.

Dimension	Strictly Physical	At the cross-road with Information Privacy
Intimacy	Genetic profile; blood type; feelings; psychological conditions; sex preference; etc.	Medical records; marriage certificate; etc.
Solitude	One's home; one's car; etc.	GPS coordinates; etc.
Anonymity	Personal behaviour; trade union membership; etc.	Online purchases; social media account
Reserve	Face-to-face conversations; letters, etc.	Emails; telephone communications; etc.

Table 12. Overlaps between physical and information privacy: some examples

⁴²⁸ Sunshine, J., and Tyler, T. R. (2003) "The role of procedural justice and legitimacy in shaping public support for policing" *Law & Society Review*, 37(3): 513–548. Whitley, R. (1987) *op. cit.*

⁴²⁹ Akter, S.K., D'Ambra, J. and Ray, P. (2011) "Trustworthiness In health Information Services: An Assessment Of A Hierarchical Model With Mediating And Moderating Effects Using Partial Least Squares", *Journal of the American Society for Information Science and Technology* 62(1): 100-116.

⁴³⁰ Smith, M. L. (2011) "Limitations to Building Institutional Trustworthiness through E-Government: A Comparative Study of Two E-Services in Chile", *Journal of Information Technology* 26: 78-93. Avgerou, C.; Ganzaroli, A.; Poulymenakou, A. and Reinhard, N. (2009) "Interpreting the Trustworthiness of Government Mediated by Information and Communication Technology: Lessons from Electronic Voting in Brazil" *Information Technology for Development* 15 (2): 133 – 148.

⁴³¹ Searle, R.H.; Den Hartog, D.N.; Weibel, A.; Gillespie, N.; Six, F.; Hatzakis, R. and Skinner, D. (2011) *op. cit.*

⁴³² Niehoff, B. P., and Moorman, R. H. (1993) "Justice as a Mediator of the Relationship between Methods of Monitoring and Organizational Citizenship Behavior" *Academy of Management Journal*, 36: 527-556.

⁴³³ Sunshine, J., and Tyler, T. R. (2003) *op. cit.*

⁴³⁴ The authors want to thank Kirstie Ball for contribution to drafting this section.

Once we have recalled and further explained our privacy typology, we need to move forward to its empirical translation. Since our concise typology serves to categorise real-life situations, but it does not say anything about people's attitude toward privacy, we need to select 'privacy concern' as variable, in order to draw insights from previous empirical work in the field.

Individual's concerns about organisational privacy practices, briefly called "Concern for Information Privacy" (CFIP),⁴³⁵ is a construct widely used in the literature, whose dimensions have been measured through four subscales of 3-4 items each. The four dimensions are: *Collection*: individuals often perceive that excessive quantities of data regarding their personalities, background, and actions are being collected and accumulated, and they often resent this. *Unauthorized Secondary Use*: it reflects the belief that sometimes information is collected from individuals for one purpose but is used for another, secondary purpose without authorisation. Concerns about secondary use are exacerbated when personal information is disclosed to an external party. *Improper Access*: individuals are afraid of having their personal information accessed by people who do not need or do not have to know information about them. *Errors*: it reflects anxieties about accidental errors in personal data due to poor data handling, supervision and retention of old, inaccurate records.

These four facets of individual fears for personal data mishandling, not only have been consistently measured across several studies,⁴³⁶ but it might also be claimed that they have found a policy response in those data protection principles enforced by the European 1995 Data Protection Directive.⁴³⁷ This would be coherent with findings that demonstrate that information privacy concern influences individuals' preferences for stricter regulatory environments.⁴³⁸ Moreover, CFIP, along with other factors, influences individuals' acceptance of technology: greater privacy concern leads in fact to lower intentions to use online services.⁴³⁹

For the sake of this study, we need to develop a new variable, which we call Substantive Privacy Concern, and that comprehends 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, wiretapping of personal communications, can

⁴³⁵ Smith, H. Jeff, Milberg, Sandra J., and Sandra J. Burke (1996) *op. cit.*

⁴³⁶ See for example Stewart, K. A., and Segars, A. H. (2002) "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research* 13(1), pp. 36-49.

⁴³⁷ "SECTION I - PRINCIPLES RELATING TO DATA QUALITY. Article 6: 1. Member States shall provide that personal data must be: (a) processed fairly and lawfully; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards; (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed; (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use". Source: EC (1995) "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", *Official Journal L 281*, 23/11/1995 P. 0031 – 0050, available at: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

⁴³⁸ Milberg, S. J., Smith, H. J., and Burke, S. J. (2000) "Information Privacy: Corporate Management and National Regulation," *Organization Science* 11(1), pp. 35-57.

⁴³⁹ Bélanger, F., Hiller, J. and Smith, W. J. (2002) *op. cit.* Chellappa, R. K. and Sin, R. G. (2005) "Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management* 6(6):181-202. Eastlick, M. A., Lotz, S. L. and Warrington, P. (2006) "Understanding Online B-to-C Relationships: An Integrated Model of Privacy Concerns, Trust, and Commitment," *Journal of Business Research* 59(8): 877-886. Pavlou, P. A., Liang, H. and Xue, Y. (2007) "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective," *MIS Quarterly* 31(1): 105-136. Resnick, M. L. and Montania, R. (2003) "Perceptions of Customer Service, Information Privacy, and Product Quality From Semiotic Design Features in an Online Web Store," *International Journal of Human-Computer Interaction* 16(2): 211-234. Malhotra, N. K., Kim, S. S. and Agarwal, J. (2004) "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* 15(4): 336-355.

affect the extent to which people are willing to accept, engage with or be monitored by the technology. As a result of what said, we expect to find strong negative association between Substantial Privacy Concern and Acceptability of SOSTs.

5.4 Theoretical model with directionality of relationships

In the previous sections we have revised and presented a number of variables that contributes to determine the level of acceptability of a given surveillance-orientated security technology (SOST). This concluding section is devoted to briefly sketch and explain relationships among these variables with the dependent variable, i.e. "acceptability of SOSTs".

According to the risk-benefit framework, the more beneficial and less risky a technology is perceived, the higher will be the level of acceptance. In the context of this study, perceived risks are enclosed in the variable "perceived intrusiveness", while perceived benefits are covered by the variable "perceived effectiveness". Following Sanquist,⁴⁴⁰ both constructs have four constitutive dimensions each.

Perceived intrusiveness is composed by:

- **Risk of Disclosure** – The likelihood that private information about you or some aspect of your life (such as your financial or medical records) would be disclosed without your knowledge or permission.
- **Risk of Embarrassment** – The likelihood that the application of the security system would lead you to feel ill-at-ease, uncomfortable, self-conscious or ashamed.
- **Intrusiveness** – The extent to which the security is forced upon you without invitation or permission.
- **Risk of Civil Liberties Infringement** – The extent to which you believe the security system might violate human rights.

Perceived effectiveness is formed by:

- **Perceived security as a personal benefit** – The extent to which there is a desirable outcome, such as feeling more secure or protected, that follows as a result of applying the security system.
- **Public Security** – Perception that the security system is able to reduce risks of terrorist or criminal activities.
- **Accuracy** – The extent to which the security system properly detects and identifies risks, or contains error-free records of your personal information.
- **Validity** – The extent to which the security system actually addresses a real threat, and uses appropriate data to identify that threat.

While perceived intrusiveness is expected to negatively influence acceptability, perceived effectiveness should have a positive effect on acceptability. In other words, the more SOST is perceived as intrusive and risky, the less acceptable it will appear. In contrast, the more effective, accurate, and capable of enhancing personal and public security SOST is perceived, the more acceptable it will be considered.

Contextual approaches and new perspectives promoting public engagement in science have demonstrated that technologies viewed as beneficial are usually associated with less risk, than technologies not viewed as especially beneficial. Different explanations for these findings are possible: the need for consistency in beliefs and the tendency to avoid cognitive dissonance may cause the negative association between perceived risks and benefits.⁴⁴¹ In other words, pressure towards

⁴⁴⁰ Sanquist, T. F. and H. Mahy, et al. (2008) op. cit.

⁴⁴¹ Alhakami, A.S. and Slovic, P. (1994) A psychological study of the inverse relationship between perceived risk and perceived benefit. *Risk Analysis* 14(6): 1085-96.

consistency causes devaluation of the risks and overestimation of the benefits of those technologies, which are perceived as beneficial for the society.⁴⁴²

Other factors are expected to hamper or foster the effects of potential risks (here measured through the 'Perceived Intrusiveness' variable) and benefits (here measured through the 'Perceived Effectiveness' variable) over the level of acceptability of SOSTs.

According to the risk-benefit framework, the more beneficial and less risky a technology is perceived, the higher will be the level of acceptance. In the context of this study, perceived risks are enclosed in the variable Perceived Intrusiveness, while perceived benefits are covered by the variable Perceived Effectiveness. While perceived intrusiveness is expected to negatively influence acceptability of SOSTs, perceived effectiveness should have a positive effect on acceptability. In other words, the more SOST is perceived as intrusive and risky, the less acceptable it will appear. In contrast, the more effective, accurate, and capable of enhancing personal and public security SOST is perceived, the more acceptable it will be considered.

The variables Substantive Privacy Concern, Temporal, Spatial, and Social Proximity, and Technology Detractors are expected to increase the degree of Perceived Intrusiveness and to decrease the level of Acceptability. On the other hand, the variables Perceived Level of Threat, Familiarity with SOSTs, Technology Supporters, and Institutional Trustworthiness contribute to enhance the level of perceived effectiveness of SOSTs and to increase the level of Acceptability. We will also test the hypothesis regarding the degree of reliance on the trade-off model in assessing security and privacy from an individual perspective. We will use the variable security-privacy balance to cluster respondents' opinions to test whether they may potentially rely on the trade-off model to assess the acceptability of SOSTs. The theoretical model at the end of chapter five summarises the relations so far outlined by showing variables and directionality of relationship among variables.

Finally the Figure 3 summarises the relations so far outlined by showing variables and directionality of relationship among variables. The figure also indicates which variables will be measured at SOST level and which variables will be measured as general attitudes of study participants.

⁴⁴² Frewem L.J., Howard, C. and Shepherd, R. (1997). "Public concerns in the United Kingdom about General and Specific Applications of Genetic Engineering: Risk, Benefit and Ethics," *Science, Technology and Human Values* 22(8).

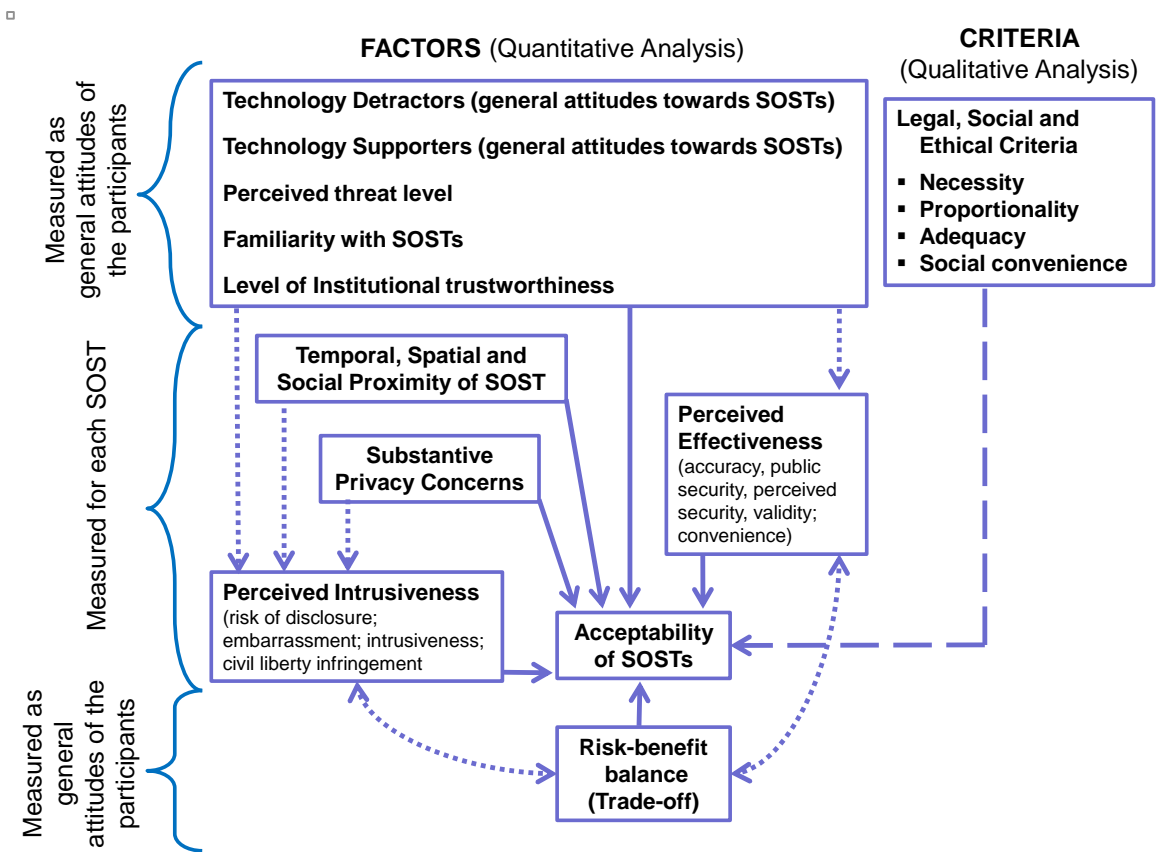


Figure 3. Theoretical Model

6 Criteria and factors determining acceptability of security technologies in Europe

6.1 Introduction

In the previous chapters, after a conceptual discussion of the recent trajectory of security and privacy, both as theoretical concepts and as policy objectives, we tried to identify the factors and criteria that, according to a variety of different scholarly literatures, had a potential to influence and determine the public acceptability of surveillance-orientated security technologies (SOSTs). Drawing from public engagement with science, privacy studies and risk analysis studies, we ended up with a quite exhaustive list of factors. Among those factors we also included the security-privacy balance, which, inspired by the trade-off approach, considers that SOSTs are simultaneously security enhancing but also privacy infringing and, thus, argues that an increase in security can only come at the expenses of privacy and liberty. We often see the trade-off approach underpinning much of security policies and security technologies development. Its validity has been questioned by a variety of conceptual and theoretical studies. Moreover, it has been recently suggested that it could also be empirically flawed but it was never tested empirically.⁴⁴³ Thus, we wanted to test whether participants in our citizen summits across Europe considered that the implementation of SOSTs effectively implies the need to balance security and privacy, and whether the adoption of this frame, which potentially forces participants to trade privacy for security, was likely to influence, positively or negatively, the acceptability of SOSTs. Finally, we set all these factors into a model of expected relations, amongst them and between them, with one main dependent variable, acceptability of SOSTs.

The model was later turned into a formal empirical model, with its own detailed set of hypotheses to be tested through statistical analysis. The citizen summits gathered all the relative data across Europe, both through a formal questionnaire and also through a more qualitative data gathering procedure that collected arguments, proposals, debates, statements and positions of the participants while they discussed the SOSTs in structured table discussions.

These data are outlined, analysed and discussed in this chapter, but they also constitute background information for the national reports on the nine citizen summits as summarised in 6.10. In this chapter, we focus specifically on the factors and criteria that have been found to influence acceptability of SOSTs. Thus, the main objective of this chapter is to test the hypotheses developed as part of D4.1 by using survey data gathered during the citizen summits (MS7). The dataset analysed here is the one produced in D5.3. The information contained in the dataset features answers to the questions, developed in D4.2, to measure the constructs and ideas presented in D2.4. However, in this chapter we also complement quantitative analysis and the relative results with relevant data and insights derived from the qualitative analysis of the table discussions that took place in the small-scale citizen meetings and in the large-scale citizen summits.

This chapter is divided into two main sections. The first section, which consists of two sub-sections 6.1 and 6.2, summarizes and outlines the participatory process whose outcomes have been analysed through quantitative and qualitative techniques. It also enumerates the operational definitions of all concepts present in the theoretical framework (D2.4) and refined in the empirical model (D4.1). Sub-section 6.2 also exhibits the survey items and measurement scales used to quantify each concept and their probability distributions.

⁴⁴³ Pavone, V., and S. Degli Esposti. 2012. "Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security." *Public Understanding of Science* 21 (5):556-572. doi: 10.1177/0963662510376886.

The second section, which consists of sub-subsection 6.3, 6.4 and 6.5, is devoted to the testing the hypotheses and identifying those factors and criteria shaping people's perceptions and opinions about surveillance-orientated security technologies (SOSTs). Three main issues are investigated in these subsections, each focusing on a specific research topic. The three main research questions investigated in these subchapters are:

- 1) What are the **factors** which play a major role in shaping public attitudes toward SOSTs?
- 2) What are the effects of relying on the privacy-security **trade-off model** in assessing SOSTs?
- 3) What are the **criteria** that should be adopted when introducing new SOSTs?

In order to answer these questions, sub-section 6.3 is dedicated to the analysis of all the direct and indirect effects exercised by all factors on the acceptability factor. The hypotheses stated in D4.1 are analysed as part of this sub-section. Sub-section 6.4 investigates the privacy-security trade-off and its effects on considering SOSTs acceptable. Finally, 6.5 is devoted to the qualitative analysis of factors and of the criteria adopted by citizen summits participants across Europe when assessing SOSTs.

Before presenting the survey instrument and the results, the next section very briefly illustrates the research design and the type of data collected as part of the Surprise large-scale participatory events. Further details on each public consultation can be found in the national reports (D6.1-9) and in the Synthesis Report (D6.10).

6.1.1 Data collected in the large scale participatory events

Between January and March 2014, citizen summits in 9 EU countries were held as part of the Surprise project. Their purpose was to gather lay public's opinions, ideas, knowledge and proposals on the use of surveillance-orientated security technologies (SOSTs), their privacy and human rights' implications, and the norms which should regulate their use. About 200 people participated to these events in each country.

To help people better understand the use of surveillance measures to tackle security problems three specific SOSTs were selected. These were i.e. smart CCTV (sCCTV), Deep Packet Inspection (DPI), and Smartphone Location Tracking (SLT) – were selected (D2.3).



Smart CCTV (sCCTV) features digital cameras, which are linked together in a system that have the potential to recognise people's faces, analyse their behaviour and detect objects.



Cyber surveillance using **Deep Packet Inspection (DPI)** works by detecting and shaping how messages travel on a network. DPI opens and analyses messages as they travel, identifying those that may pose particular risks.



Smartphone location tracking: By analysing location data from a mobile phone, information can be gleaned about the location and movements of the phone user over a period of time.

Two out of three SOSTs were discussed and used as an example in 6 of the 9 countries where the citizen summits were held. In other words, participants replied to questions concerning only two SOSTs during each summit. This decision was designed to reduce the risk that participants might have been too tired and distracted by the end of the six hours event.

In order to decide which SOST should be discussed in which country, countries were divided into three groups. Each group of country should have a Southern or East European country; a Northern country and a Central European country. SOSTs were there assigned to cluster of countries by taking into

account considerations related to both national characteristics and aspects of the technology such as the level of penetration and familiarity of citizens of a country with a certain system.

SOSTa	North		South/East	Central	Region
	SLT & sCCTV	1. Denmark	2. Hungary	9. Germany	
	DPI & SLT	3. Norway	5. Italy	8. Switzerland	
	sCCTV & DPI	7. UK	4. Spain	6. Austria	

Table 13. SOSTs assigned to group of countries

SLT & sCCTV: Aarhus, Denmark (18/Jan/14); Budapest, Hungary (25/jan/14); Kiel, Germany (29/Mar/14).

DPI & SLT: Oslo, Norway (01/Feb/14); Florence, Italy (8/Feb/14); Switzerland (Zürich 8/Mar/14, Iverdu 22/mar/14 and Lugano 29/Mar/14).

sCCTV & DPI: Madrid, Spain (01/Feb/14); Vienna, Austria (22/Feb/14); Birmingham (1/mar/14 & 15/Mar/14).



Figure 4. Map of Citizen Summits

The functioning and use of each SOST were explained in a booklet participants received before the summit. Further information related to the advantages, disadvantages and controversial issues of each SOST was also presented in three short documentary films produced as part of Surprise by the Open University in collaboration with the film maker TwoCatsCan (D4.3).⁴⁴⁴

Participants were divided in small groups of 8 people and seated around a table in a large room with one or more big screens showing the questions. At each table a facilitator was present to help participants. Participants in the citizen summits were asked by the head facilitator to answer questions by means of remote control devices called “clickers”, after having watched the documentary films and sharing their opinions with other fellow participants. After discussing each SOST, summit participants were also be given the chance of agreeing as a group on a specific recommendation to be given to policy makers. People could also write their comments, remarks or individual recommendations on postcards prepared for the event.

⁴⁴⁴ Pdf versions of the booklet in 8 languages and the films can be found on the Surprise project webpage at: <http://surprise-project.eu/events/citizen-summits/>

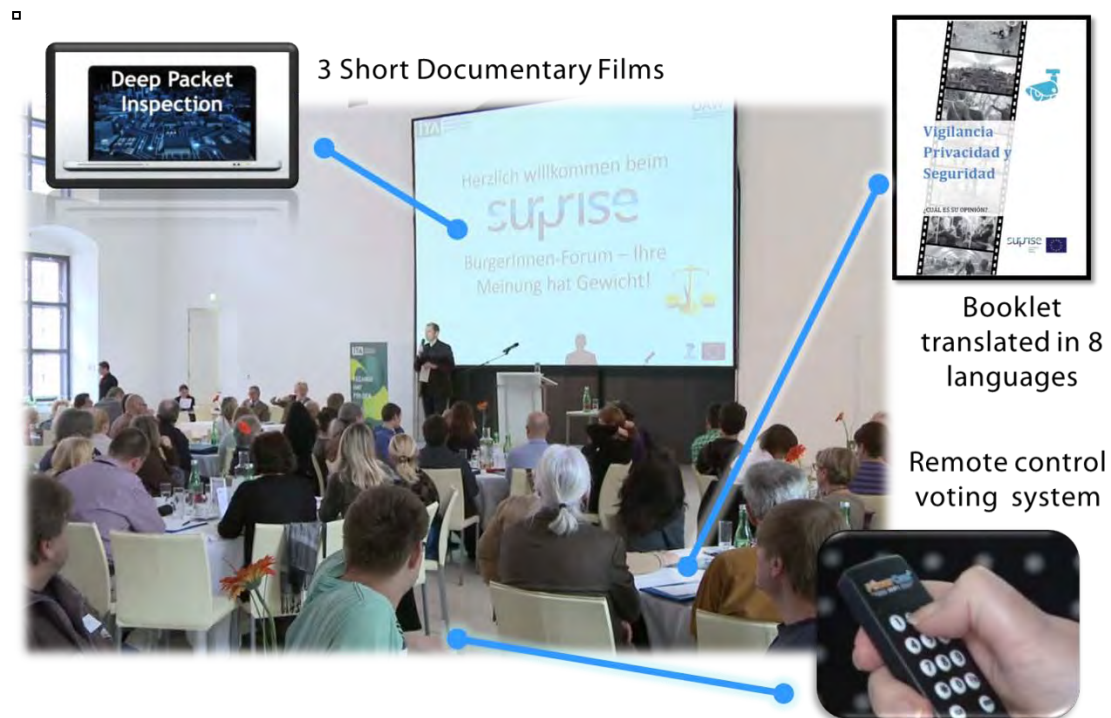


Figure 5. Citizen summit key elements

The data presented in this chapter are the result of running the same event in all 9 countries. The quantitative data presented in section 6.2 and analysed in section 6.3 and 6.4 are the data gathered through the remote control voting system. As displayed in the following table, more than 1,000 people answered questions on each specific SOST.

SCCTV	DPI	SLT
Denmark	Norway	Denmark
Hungary	Italy	Hungary
Spain	Spain	Norway
Austria	Austria	Italy
UK	UK	Switzerland
Germany	Switzerland	Germany
No of participants		
1.198	1.202	1.144


Table 14. Total participants answered questions on each specific SOST and countries.

Participants' comments and reflections, as presented and discussed in the national reports (D6.1-9), have been summarised in the last section of this chapter. The comments, arguments and suggestions written by participants on the postcards, on the group recommendation sheets (see fig 6), or reported by table facilitators and table secretaries, were written or shared in 8 different languages. As a result, whilst these comments, arguments and suggestions have been analysed and discussed at length in each of the national reports (6.1-6.9), the criteria influencing acceptance and acceptability of SOSTs, presented at the end of this chapter, draw directly from the interpretation and explanations given in

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

surprise

7
SEVENTH FRAMEWORK
PROGRAMME



Terminale Recommendation round

What is the overall message of your table's recommendation?

What is the background for this recommendation? // What is the problem?

Your recommendation // What should be done? // How can the problem be solved?

surprise

7
EUROPEAN
COMMISSION

EUROPEAN
COMMISSION

Figure 6. Surprise postcards and recommendation forms

9:30	Citizen Check-in
10:00	Welcome 10:00 Prominent speaker could deliver an opening speech (5-6 minutes) 10:05 The head facilitator welcomes everyone and shortly introduces the idea behind SurPRISE and the summit, the summit programme, the different staff members, the principles and purpose of deliberation, voting procedures, practicalities, etc. (10 minutes).
10:20	Introduction to clickers 10:20 Voting system and clickers are introduced. Voting on demographic questions with short feedback on each question (<u>2 questions in total</u>) (10 minutes) 10:30 A short introductory round at the tables (10 minutes) 10:40 Questions on institutional trustworthiness, perceived level of threat, general attitudes toward technology to foster security, and substantive privacy concerns with short feedback. (10 minutes)
10:50	SOST no. 1 10:50 Introduction of the procedure and theme by the meeting facilitator, and voting on the initial questions about SOST 1 (<u>2 questions in total</u>) followed by a video presentation (15 minutes) 11:05 Voting on the first set of questions about SOST1 with short feedback on each question (<u>8 questions in total</u>) (10 minutes). 11:15 Discussions at the tables (45 minutes) and presentation of a few headlines from the discussions and/or presentation of results from other meetings (5-7 min) 12:00 Voting on SOST 'discussion points' questions with short feedback on each question (<u>13 questions in total</u>) (20 minutes).
12:20	Lunch
13:05	SOST no. 2 13:05 Introduction of the procedure and theme by the meeting facilitator, and voting on the initial questions about SOST 2 (<u>2 questions in total</u>) followed by a video presentation (15 minutes) 13:20 Voting on the first set of questions about SOST1 with short feedback on each question (<u>8 questions in total</u>) (10 minutes) 13:30 Discussions at the tables, (45 minutes) and presentation of a few headlines from the discussions and/or presentation of results from other meetings (5-7 min) 14:15 Voting on SOST 'discussion points' questions with short feedback on each question (<u>13 questions in total</u>) (20 minutes).
14:35	Recommendation round 14:35 At each table the citizens are asked to debate and agree on one recommendation that they would like to pass on to the European politicians, including 5-7 min for presenting recommendations from 3-4 tables (45 minutes).
15:20	General questions Citizens will vote on the last General Attitudes questions with short feedback (<u>14 questions in total</u>) (20 minutes)
15:40	Demographic questions Before the evaluation, there are some last demographic questions (<u>7 questions in total</u>) (10 minutes)
15:50	Evaluation Lastly the citizens will evaluate the day by voting on a group of evaluation questions. Feedback will follow each vote. (5 minutes)
15:55	Closing remarks The head facilitator informs the citizens about the next steps in the SurPRISE, practical issues (transportation, etc.), and thanks the citizens for their participation. (5 minutes)
16:00	End of meeting

Table 15. Programme of a typical Surprise Citizen Summit

6.2 Constructs measured in the questionnaire

This section presents all constructs used in the quantitative part of the study and operationalized in the questionnaire (D4.2) that citizen summit participants filled in during the events. Concepts' definitions, corresponding questionnaire items and scales of measurements are laid out for each construct. Frequency distributions for each variable or group of variables are also displayed for each construct. Some constructs, such as the dependent variable "acceptability", have been measured by set of items both at the SOST and general levels. In other words, the same question was asked by referring to the use of surveillance-orientated security technologies (SOSTs) in general, or to specific SOSTs, such as smart CCTV (sCCTV), Deep Packet Inspection (DPI) or Smartphone Location Tracking (SLT). However, the large majority of variables were measured by single or multiple items and only at general or at SOST level.

In the following graph, all constructs measured in the empirical model are displayed as well as their expected effects on the dependent variable, which we name "SOSTs Acceptability". The same model is tested for each SOST discussed in the citizen summit. As explained in this section, each construct was measured by taking into account its constitutive internal dimensions. For example, in measuring "Institutional Trustworthiness" we asked citizen summits' participants to what extent they considered the security agencies managing the system to be capable, honest and demonstrating goodwill. For more details please read section 6.2.2.9.

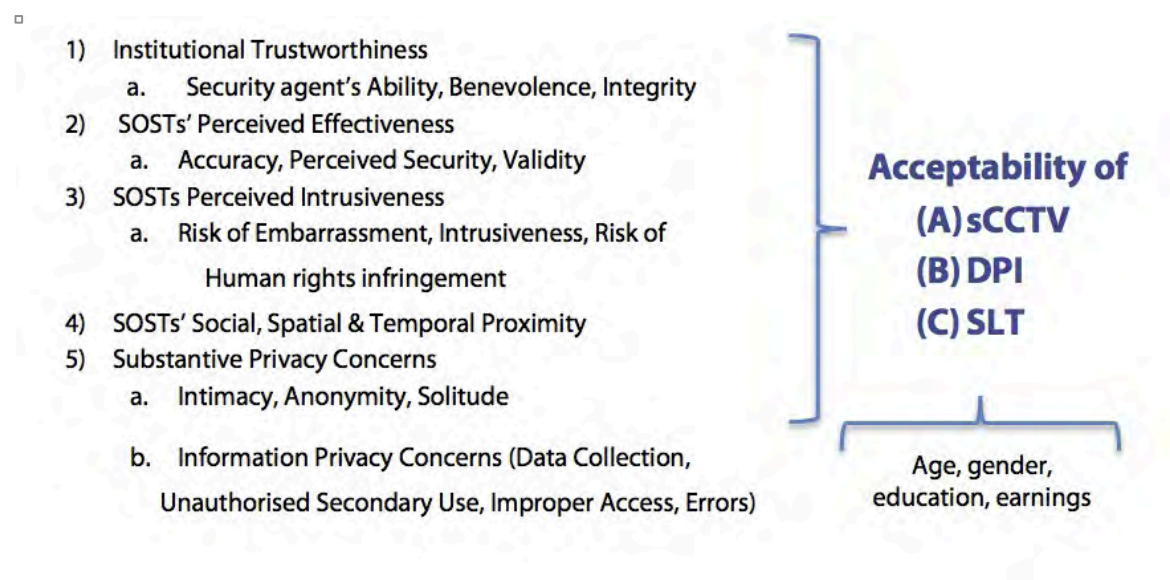


Figure 7. Factors expected to exert an influence on SOSTs Acceptability

6.2.1 Constructs measured at general level

Acceptability of SOST in general

Acceptability is the extent to which a specific SOST is considered acceptable. Key factors in acceptability are: (a) the SOST is received favourably or with approval; (b) its adoption is considered a desirable or 'good-enough' solution; and (c) the SOST it may be endured, because it is tolerable, adequate and conforms to approved standards and societal values.

ACC1: "Overall I believe surveillance-orientated security technologies should be routinely implemented to improve national security." (*Question asked before and at the end of the event*).

Overall I believe surveillance-orientated security technologies should be routinely implemented to improve national security.

(Question asked at the beginning and at the end of the citizen summit)

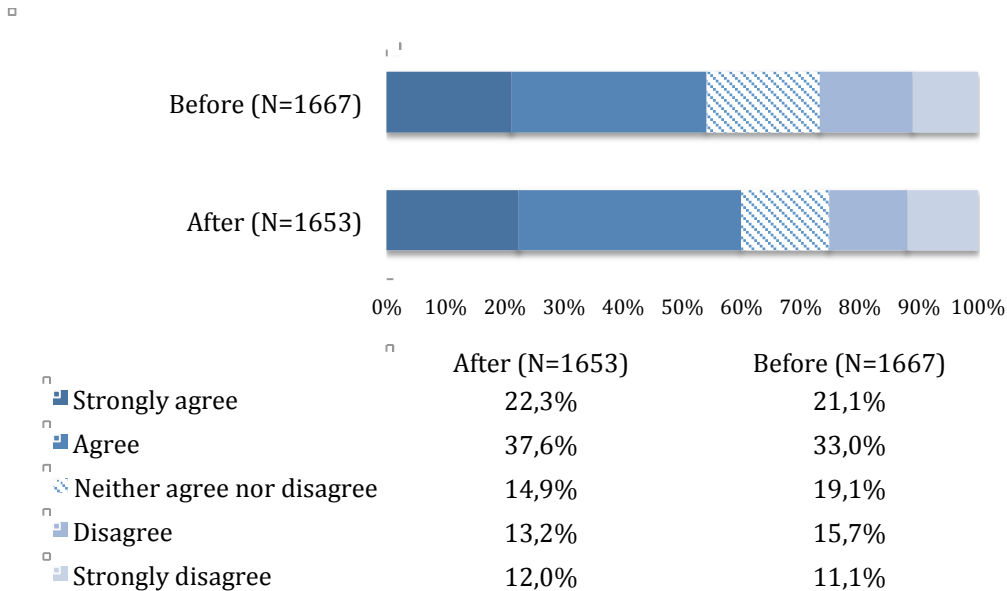


Figure 8. : Frequency distribution (%): Acceptability of SOST in general

Perceived Level of Threat

Perceived level of threat refers to the extent to which individual feel in danger because they believe their personal safety or the security of the context in which they live is threatened by people with malicious intent.

The concept has two dimensions:

- 1) Personal security – the extent to which people feel that nothing bad can happen to them.

THR1: "I generally feel safe in my daily life."

THR2: "I worry about security when I am online."

- 2) Public security – the extent to which the location where the person lives is perceived to be safe.

THR3: "I feel that this country is a safe place in which to live."

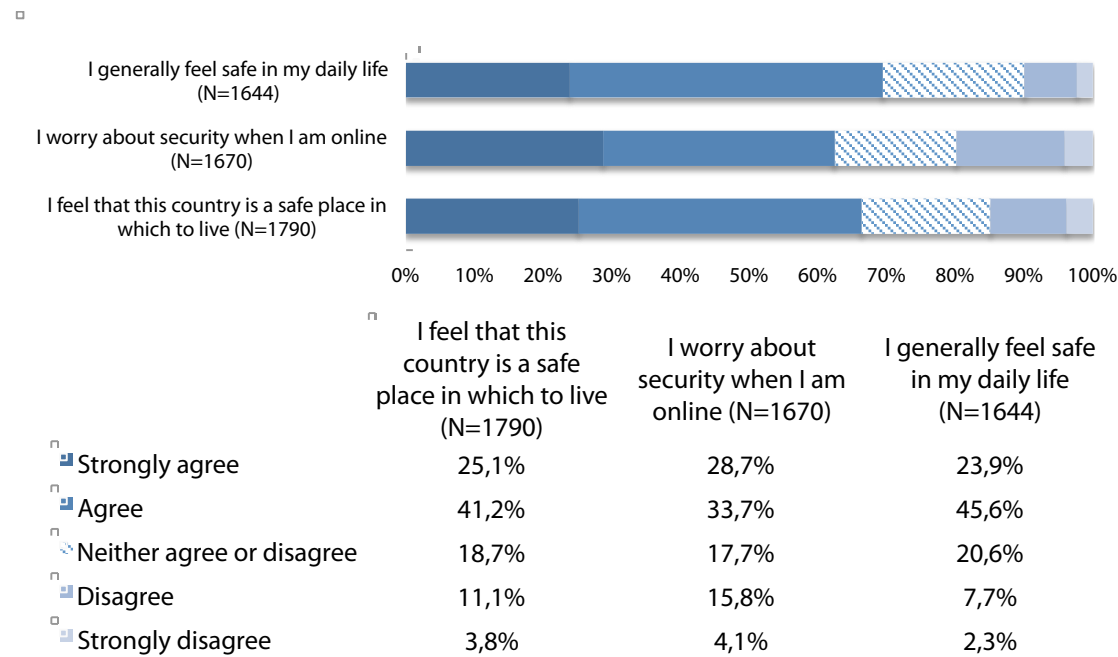


Figure 9. Frequency distribution (%): Items measuring Perceived Level of Threat

General attitudes towards technology to foster security

General attitudes toward technology refer to the extent to which a person is overall either in favour or against the use of technology to foster security. The concept has two dimensions:

- 1) Technology supporters, which reflect a generally positive belief about the ability of technology to enhance security.

TEC1: "The use of surveillance-orientated security technologies improves national security."

TEC3: "If you have done nothing wrong you do not have to worry about surveillance-orientated security technologies."

TEC4: "If surveillance-orientated security technology is available national governments might as well make use of it."

- 2) Technology detractors, which reflect a generally negative belief about the ability of technology to enhance security.

TEC2: "Surveillance-orientated security technologies are only used to show that something is being done to fight crime."

TEC5: "Once surveillance-orientated security technologies are in place they are likely to be abused."

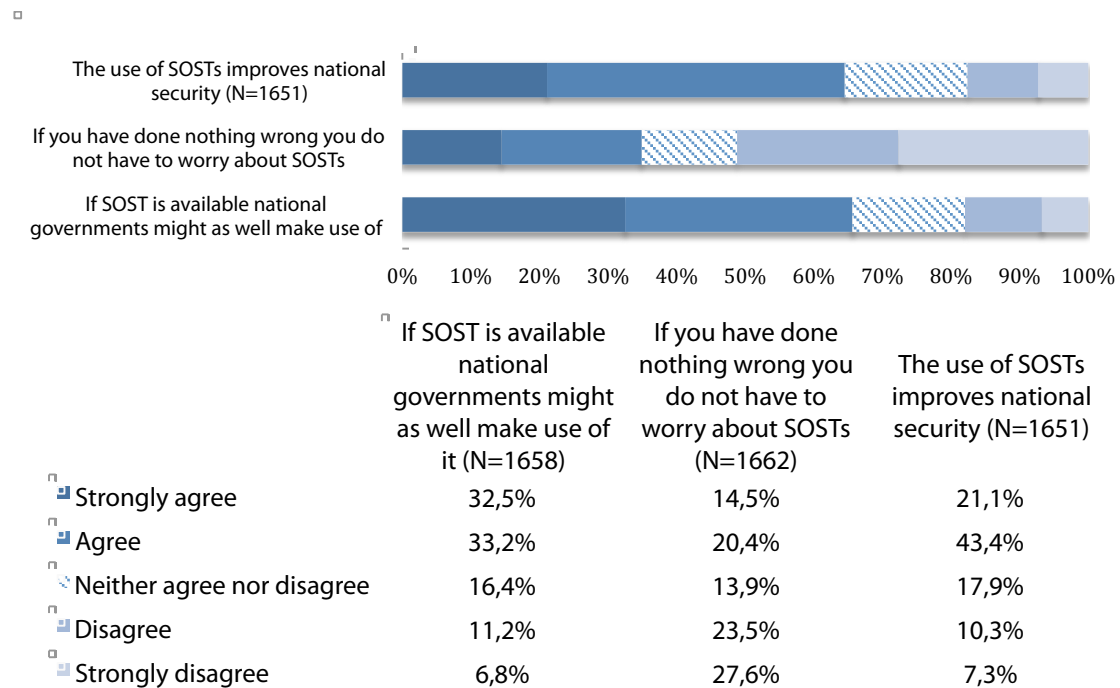


Figure 10. Frequency distribution (%): Technology supporters

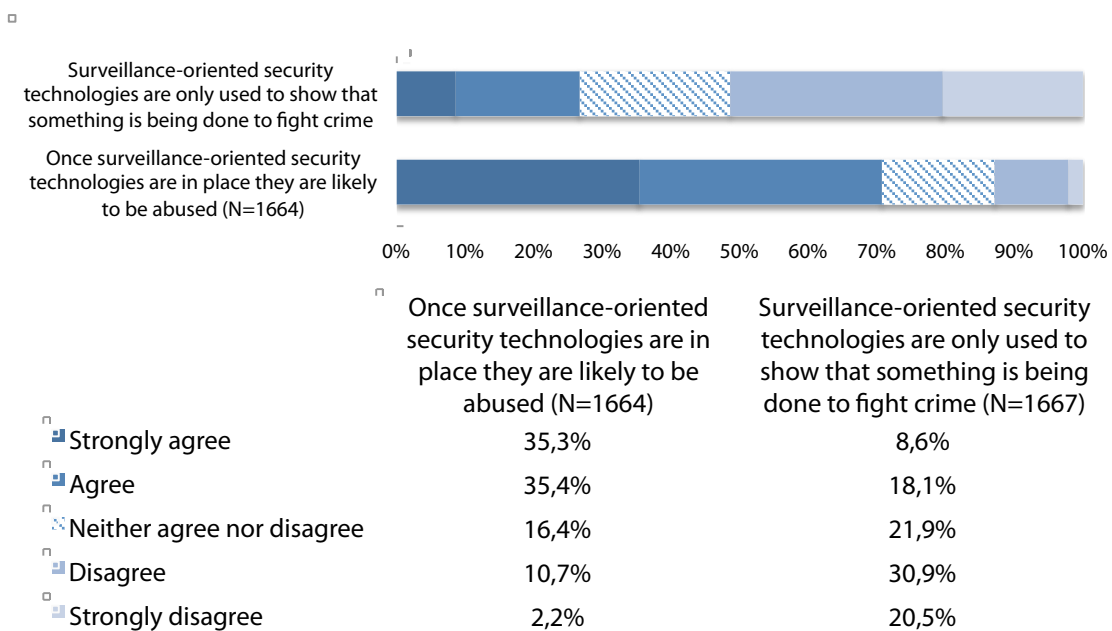


Figure 11. Frequency distribution (%): Technology detractors

Substantive Privacy Concerns

Substantive privacy concerns refer to people's concerns about the impact of a specific SOST on their physical and information privacy, whereas privacy refers to the safeguard of a person's freedom to freely act and move in the space as well as the freedom to control the flow of information about oneself. Substantive privacy concerns comprehend both information privacy concerns, as explained below, and physical privacy concerns, as explained a subsequent section. The two parts of the constructs have been divided because they have been measured at different SOST level: questions measuring information privacy have been asked for any SOST in general, while questions measuring physical privacy concerns have been asked for each specific SOST.

Information Privacy Concerns

The scale *Individuals' Concerns about Organizational Information Privacy Practices* [CFIP],⁴⁴⁵ also known as *Information Privacy Concerns* scale, has been used to measure the dimension we called *reserve* in the description of the theoretical framework. Reserve refers to the capacity of maintaining communications confidential and controlling information management and sharing. *Reserve* comprehends four dimensions of information privacy concerns: they include the disproportionate collection of data, the chance of facing unauthorized secondary use of data or improper access to data, and the presence of errors in data.

Each of the four dimensions was operationalized by one questionnaire item.

- 1) "Collection" refers to the amount of personal data collected.

IPC1: "I am concerned that too much information is collected about me."

- 2) "Unauthorised Secondary Use" refers to the use of personal data for purposes different from the ones for which the information has been collected.

IPC2: "I am concerned information held about me may be inaccurate."

- 3) "Improper Access" indicates if personal information is voluntarily or accidentally disclosed to people who should not have had access to that information.

IPC3: "I am concerned that my personal information may be shared without my permission."

- 4) "Errors" refer to the retention of – and reliance on – old, inaccurate personal data.

IPC4: "I am concerned that my personal information may be used against me."

⁴⁴⁵ Bélanger, France, and Robert E. Crossler. 2011. "PRIVACY IN THE DIGITAL AGE: A REVIEW OF INFORMATION PRIVACY RESEARCH IN INFORMATION SYSTEMS." *MIS Quarterly* 35 (4):1017-A36. Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke. 1996. "Information Privacy: Measuring Individuals' Concerns About Organizational Practices." *MIS Quarterly* 20 (2):167-196.

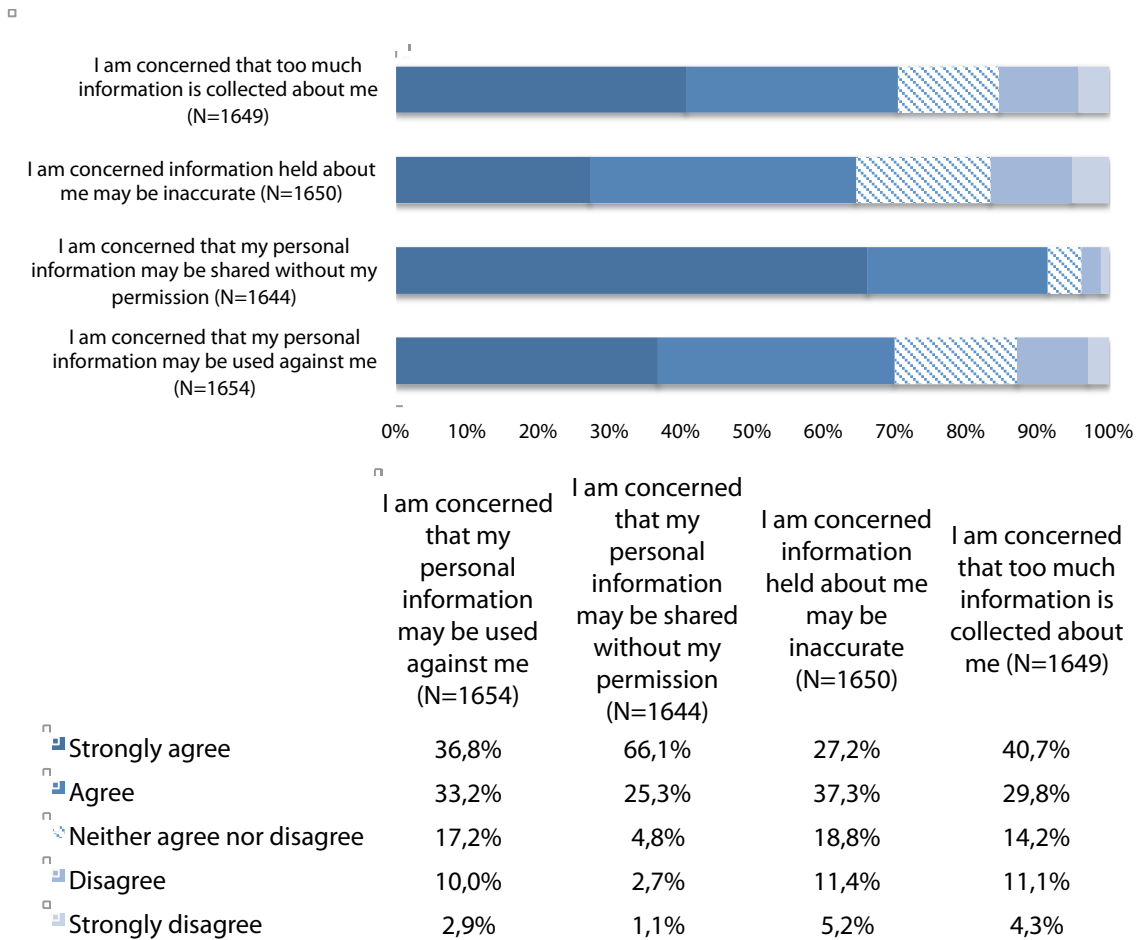


Figure 12. Frequency distribution (%): Information Privacy Concerns scale

6.2.2 Constructs measured at SOST level

Acceptability of specific SOSTs

At SOSTs level, acceptability measures the extent to which a specific SOST is considered as a desirable, adequate and endurable security measure.

ACC_CCT1: "Overall I support the adoption of Smart CCTV as a national security measure."

ACC_DPI1: "Overall I support the adoption of Deep Packet Inspection as a national security measure."

ACC_SLT1: "Overall I support the adoption of Smartphone Location Tracking as a national security measure."

"Overall I support the adoption of sCCTV/DPI/SLT as a national security measure: overall results."

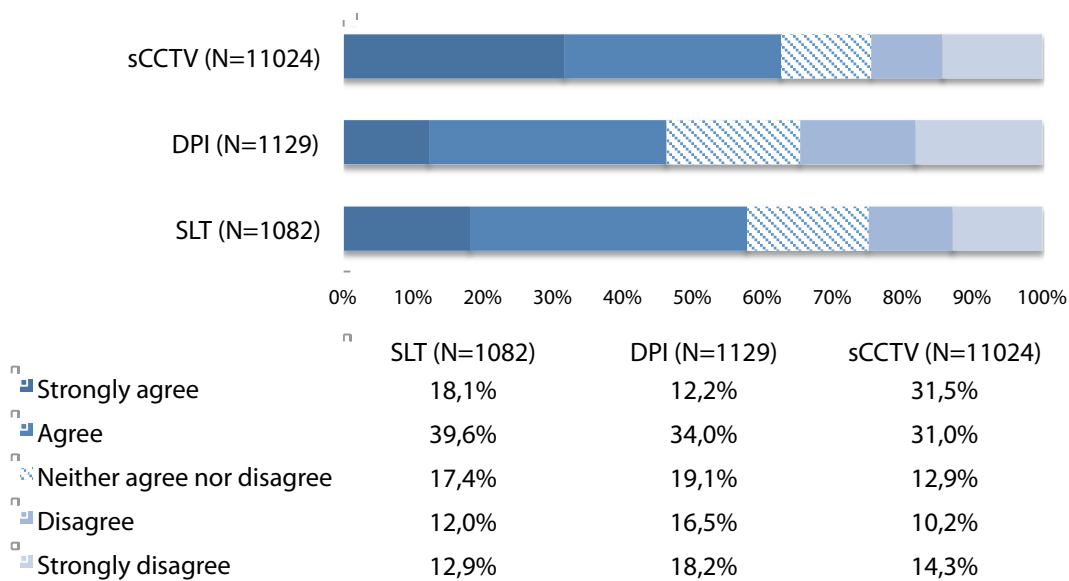


Figure 13. Frequency distribution (%): Acceptability of specific SOSTs

Avoidance of specific SOSTs

Avoidance measures the extent to which people would change their behaviour to avoid being monitored by a specific SOST.

ACC_CCT2: Active avoidance of smart CCTV.

Measurement scale: 5-point scale reported below.

- 1) "I would definitely not change my behaviour because of it."
 - 2) "I do not think I would change my behaviour because of it."
 - 3) "I would change my behaviour in areas where smartCCTV is used."
 - 4) "I would avoid going into areas where smart CCTV is used."
 - 5) "I would never go into areas where smart CCTV is used."
- "Don't know/don't want to answer."

ACC_DPI2: Active avoidance of DPI.

- 1) "I would definitely not change my behaviour online."
 - 2) "I do not think I would change my behaviour online."
 - 3) "I would change how I behave online because of DPI."
 - 4) "I would avoid going online because of DPI."
 - 5) "I would not go online because of DPI."
- "Don't know/don't want to answer."

ACC_SLT2: Active avoidance of smartphone location tracking."

- 1) "I would definitely not change my behaviour because of SLT."
- 2) "I do not think I would change my behaviour because of SLT."

- 3) "I would change how I behave because of SLT."
- 4) "I would avoid using a smartphone because of SLT."
- 5) "I would not use a smartphone because of SLT."
- "Don't know/don't want to answer."

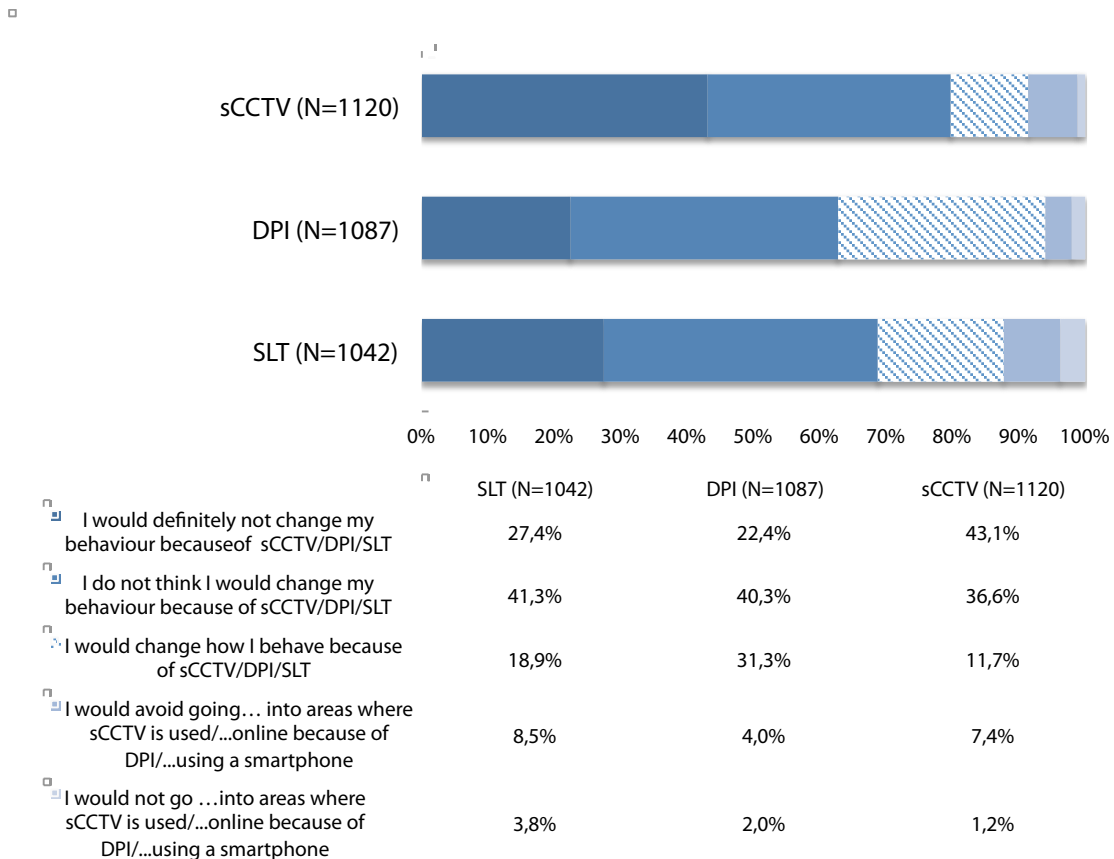


Figure 14. Frequency distribution (%): Active avoidance of sCCTV/DPI/SLT

Resistance to specific SOSTs

Resistance measures the extent to which people would find ways to oppose or challenge the use of a specific SOST.

ACC_CCT3: Challenging the use of smart CCTV for security purposes.

ACC_DPI3: Challenging the use of DPI for security purposes.

ACC_SLT3: Challenging the use of smartphone location tracking for security purposes.

Measurement scale: 5-point scale reported below.

- 1) "I do not oppose it at all."
- 2) "I would like to find out more how to protect my privacy."
- 3) "I would support others who were protesting against its use."
- 4) "I am prepared to campaign actively against its use."

5) "I am prepared to use any means I can to prevent its use."

"Don't know/don't want to answer."

"These questions concern whether you would actively challenge the use of sCCTV/DPI/SLT for security purposes. Choose the option which best reflects your opinion."

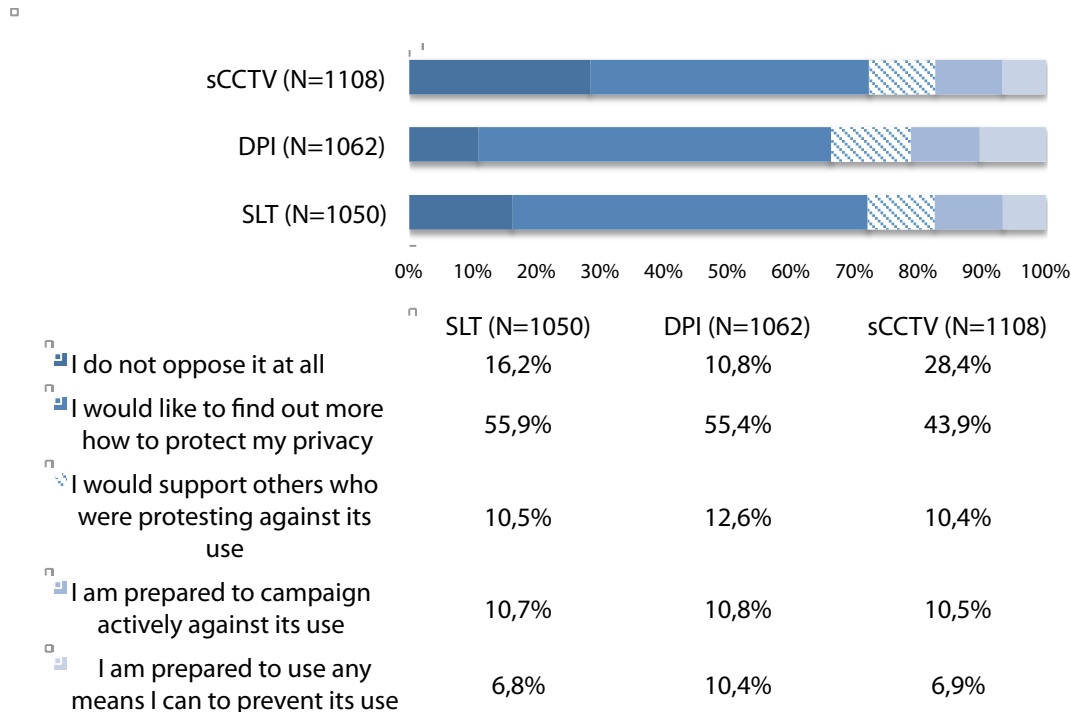


Figure 15. Frequency distribution (%): Resistance to specific SOSTs

Familiarity with SOSTs

Familiarity with a particular technology, such as a SOST, refers to the extent to which a person is used to or familiar with that technology. The concept has three dimensions:

1) *Awareness* refers to the extent of awareness of a SOST's existence and use.

This dimension was not measured because summit participants received information about all three specific SOSTs in preparation of the event.

2) *Habituation* refers to the extent to which an individual is "in touch" with SOSTs in their daily life and has become used to these technologies.

FAM_CCT1: "In the area where you live, how often do you see CCTV cameras?"

FAM_DPI1: "How often do you use the internet?"

FAM_SLT1: "How often do you use mobile devices, such as mobile phones or smartphones?"

Measurement scale: 5-point scale reported below.

- 1) "Never"
- 2) "Rarely"
- 3) "Sometimes"
- 4) "Often"

5) "All of the time"

"Don't know/don't want to answer."

"How often do you ...see cameras/ use internet/use mobile devices?"

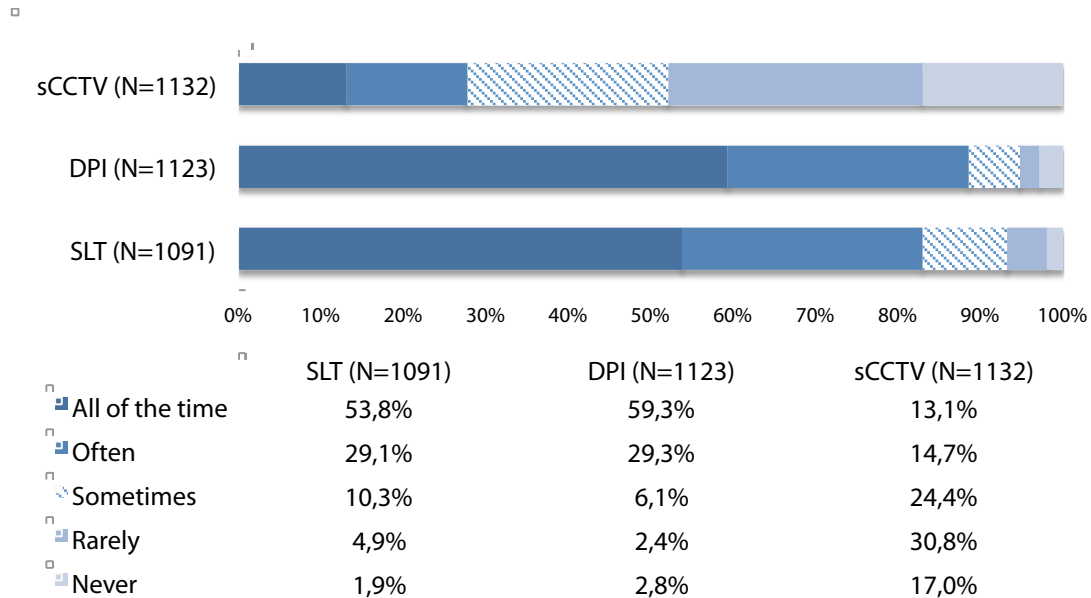


Figure 16. Frequency distribution (%): Familiarity – Habituation

3) *Knowledge* indicates the extent of knowledge of how the technology works and why it is used;

FAM_CCT2: "I understand what smart CCTV is."

FAM_DPI2: "I understand what Deep Packet Inspection is."

FAM_SL2: "I understand what smart Smartphone Location Tracking is."

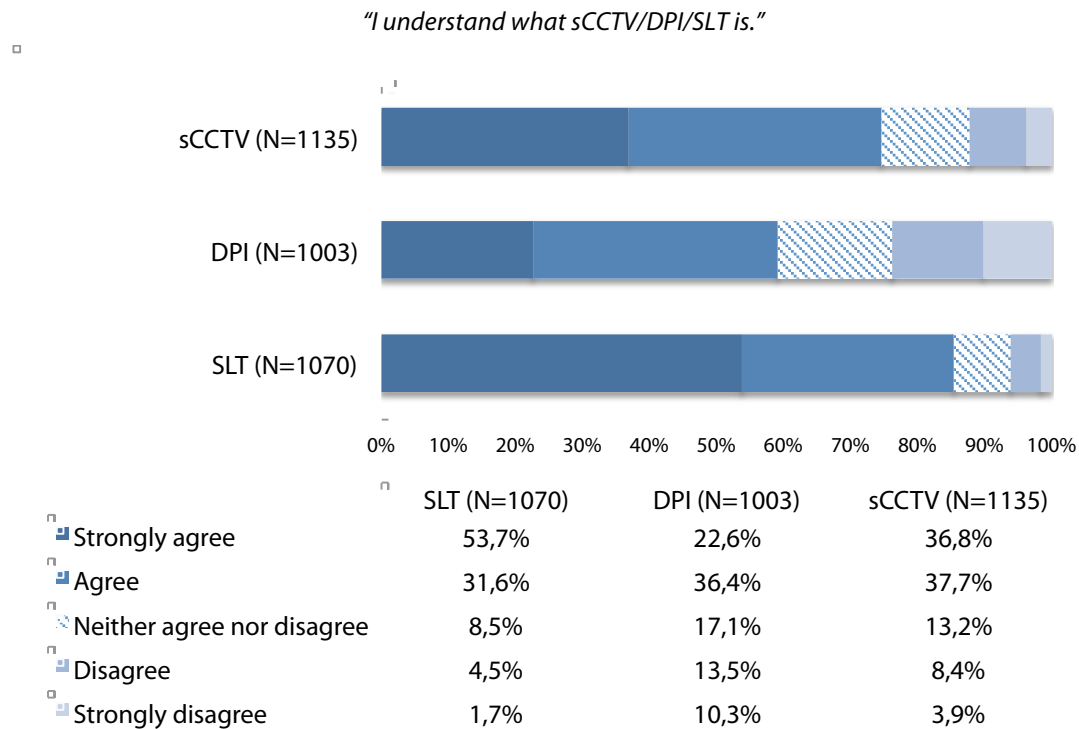


Figure 17. Frequency distribution (%): Familiarity

Perceived effectiveness of SOSTs

Perceived Effectiveness refers to the extent to which a particular SOST is considered to be effective in achieving a security goal.

PEF_CCT1: "I believe that Smart CCTV improves national security."

PEF_DPI1: "I believe that DPI improves national security."

PEF_SLT1: "I believe that SLT improves national security."

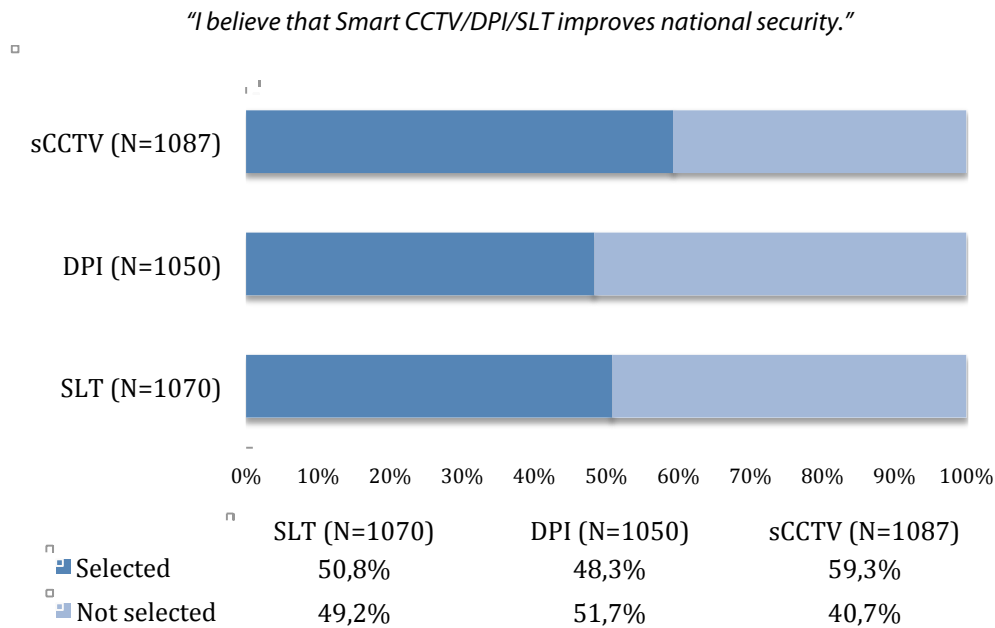


Figure 18. Frequency distribution (%): Perceived Effectiveness

The concept *perceived effectiveness* has three dimensions:

- 1) *Accuracy* indicates the extent to which the security system properly detects and identifies risks, or contains error-free records of your personal information.

PEF_CCT2: "In my opinion, Smart CCTV is an effective national security tool."

PEF_DPI2: "In my opinion, DPI is an effective national security tool."

PEF_SLT2: "In my opinion, SLT is an effective national security tool."

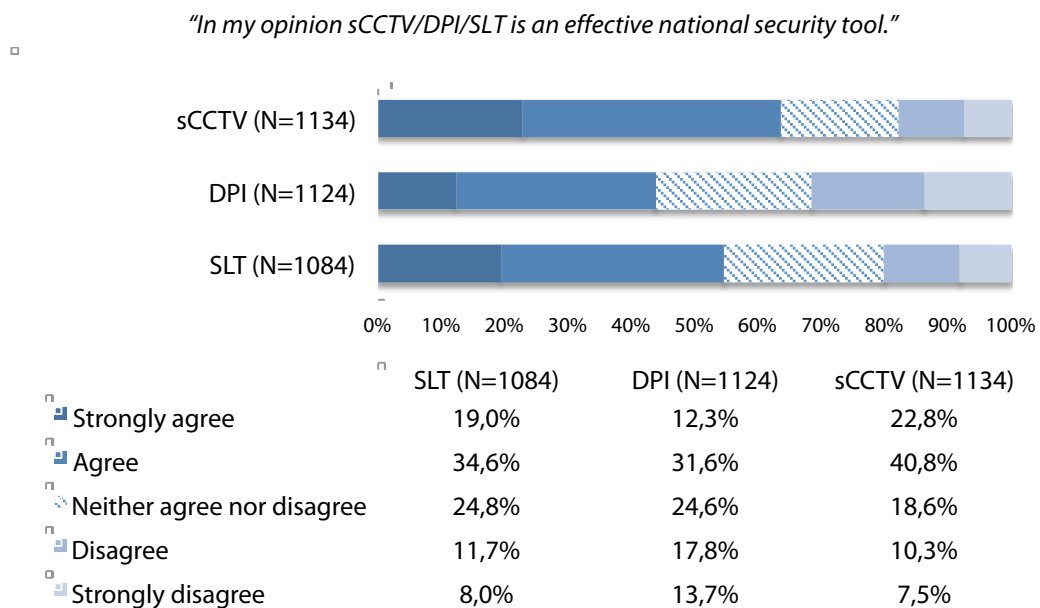


Figure 19. Frequency distribution (%): Perceived Effectiveness – Accuracy

- 2) *Perceived security* refers to the extent to which there is a desirable outcome, as an increase in personal safety follows application of the security system **PEF_CCT3**: "I feel more secure when smart CCTV is in operation."

PEF_DPI3: "I feel more secure when DPI is in operation."

PEF_SLT3: "I feel more secure when SLT is in operation."

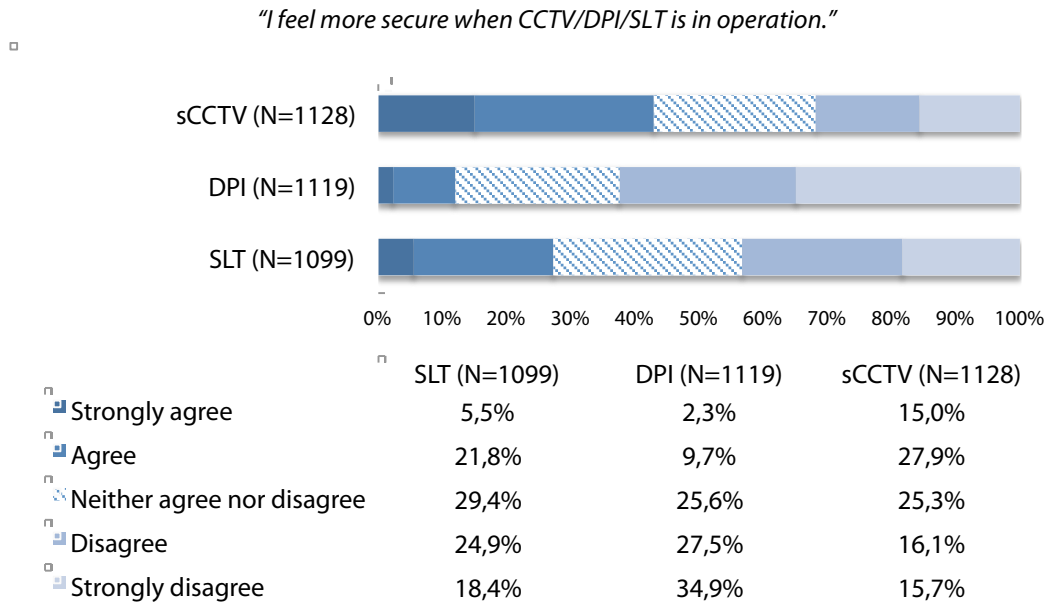


Figure 20. Frequency distribution (%): Perceived Effectiveness – Perceived security

- 3) *Validity* indicates the extent to which the security system actually addresses a real threat, and uses appropriate data to identify that threat.

PEF_CCT4: "Smart CCTV is an appropriate way to address national security threats."

PEF_DPI4: "DPI is an appropriate way to address national security threats."

PEF_SLT4: "SLT is an appropriate way to address national security threats."

"sCCTV/DPI/SLT is an appropriate way to address national security threats."

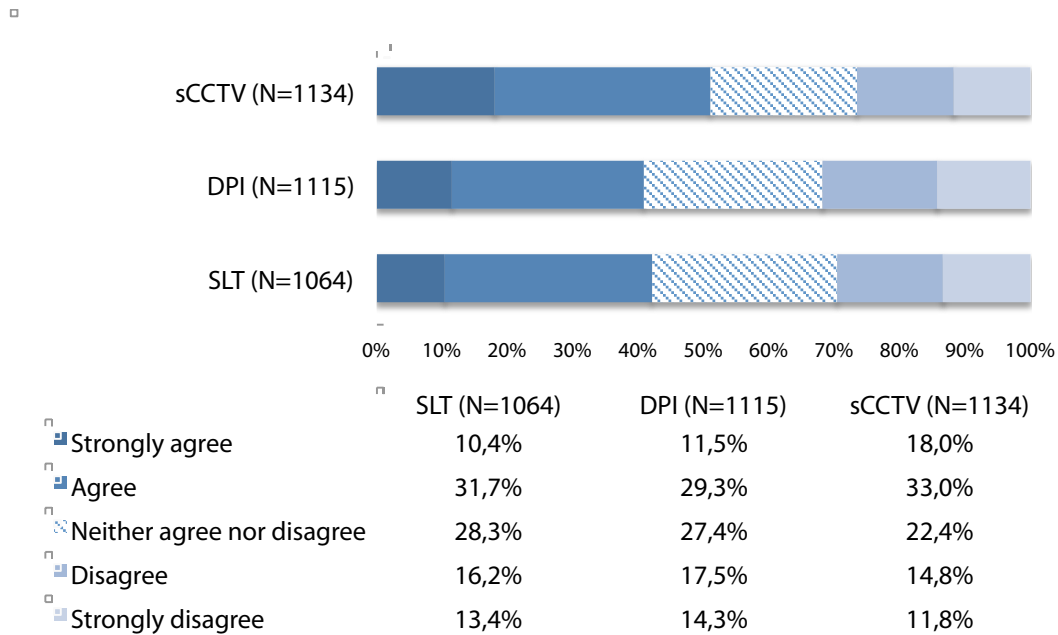


Figure 21. Frequency distribution (%): Perceived Effectiveness – Validity

Perceived Intrusiveness of SOSTs

Perceived Intrusiveness refers to the extent to which a particular SOST is perceived to intrude into an individual's personal sphere.

PIN_CCT1: "I believe that Smart CCTV is intrusive."

PIN_DPI1: "I believe that DPI is intrusive."

PIN_SLT1: "I believe that SLT is intrusive."

"I believe that sCCTV/DPI/SLT is intrusive."

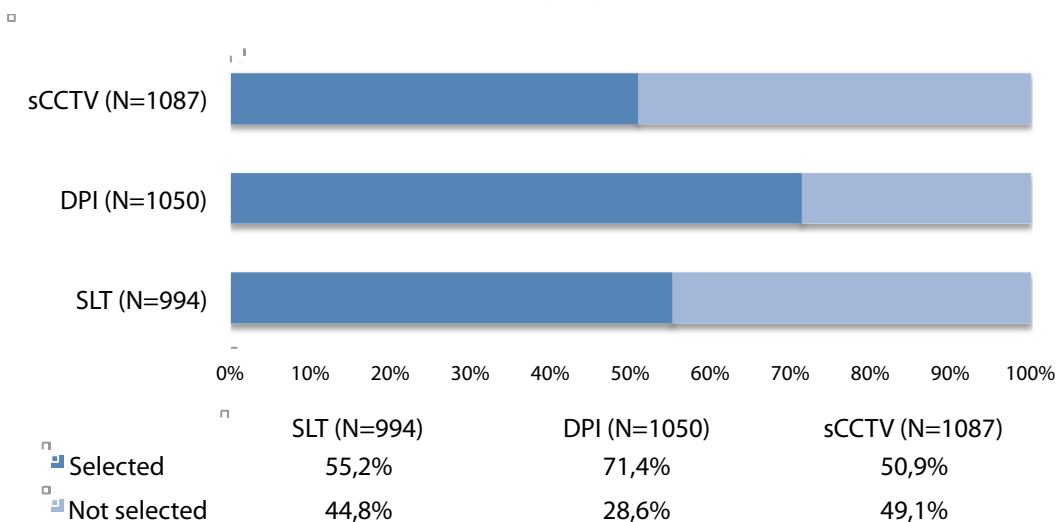


Figure 22. Frequency distribution (%): Perceived Intrusiveness

The concept perceived intrusiveness has three dimensions:

- 1) *Risk of embarrassment* refers to the likelihood that the application of the security system would lead a person to feel ill-at-ease, uncomfortable, self-conscious or ashamed.

PIN_CCT3: "The idea of smart CCTV makes me feel uncomfortable."

PIN_DPI3: "The idea of DPI makes me feel uncomfortable."

PIN_SLT3: "The idea of SLT makes me feel uncomfortable."

"I feel that sCCTV/DPI/SLT is forced upon me without my permission."

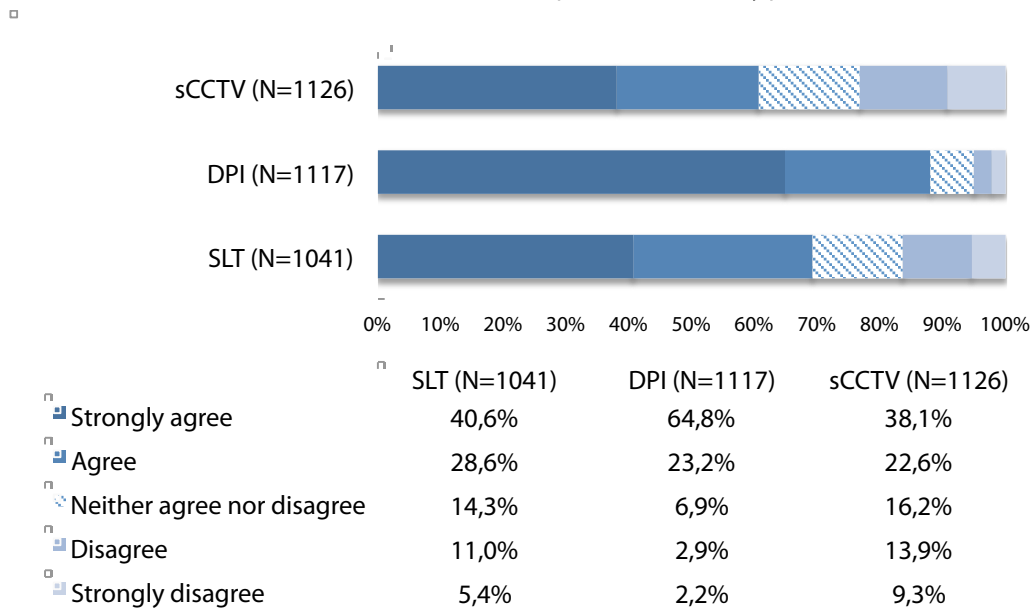


Figure 23. Frequency distribution (%): Perceived Intrusiveness – Risk of embarrassment

- 2) *Intrusiveness* refers to the extent to which the security system is forced upon a person without invitation or permission.

PIN_CCT2: "I feel that smart CCTV is forced upon me without my permission."

PIN_DPI2: "I feel that DPI is forced upon me without my permission."

PIN_SLT2: "I feel that SLT is forced upon me without my permission."

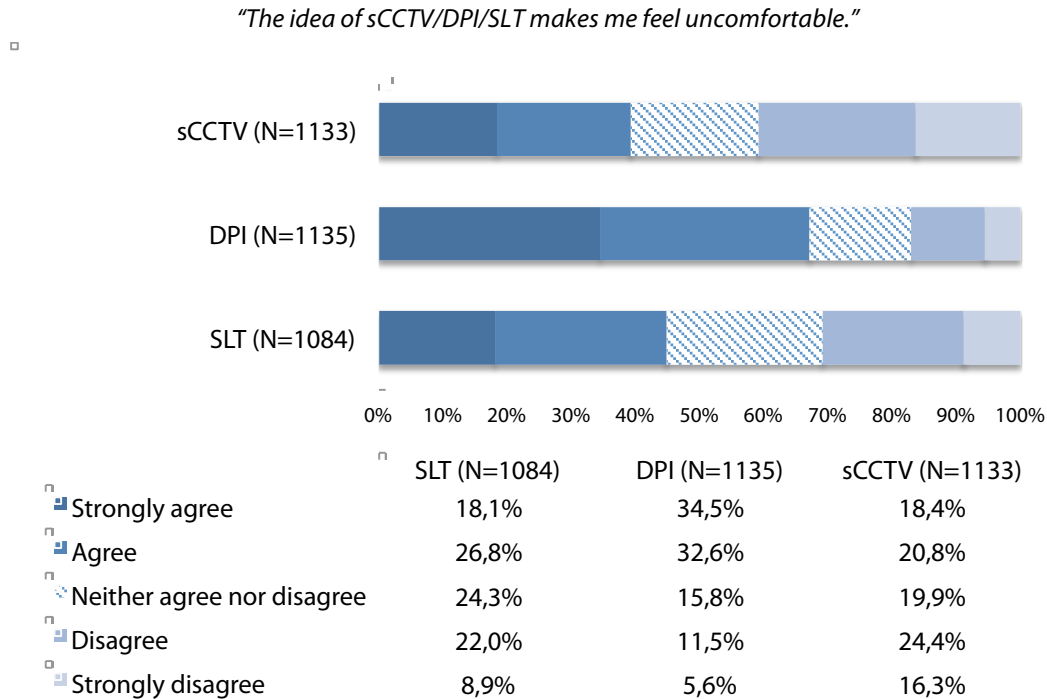


Figure 24. Frequency distribution (%): Perceived Intrusiveness – Intrusiveness

- 3) *Risk of human rights infringement* refers to the extent to which a person believes the security system might violate their human rights.

PIN_CCT4: "Smart CCTV worries me because it could violate my fundamental human rights."

PIN_CCT5: "Smart CCTV worries me because it could violate everyone's fundamental human rights."

PIN_DPI4: "DPI worries me because it could violate my fundamental human rights."

PIN_DPI5: "DPI worries me because it could violate everyone's fundamental human rights."

PIN_SLT4: "SLT worries me because it could violate my fundamental human rights."

PIN_SLT5: "SLT worries me because it could violate everyone's fundamental human rights."

"sCCTV/DPI/SLT worries me because it could violate my fundamental human rights."

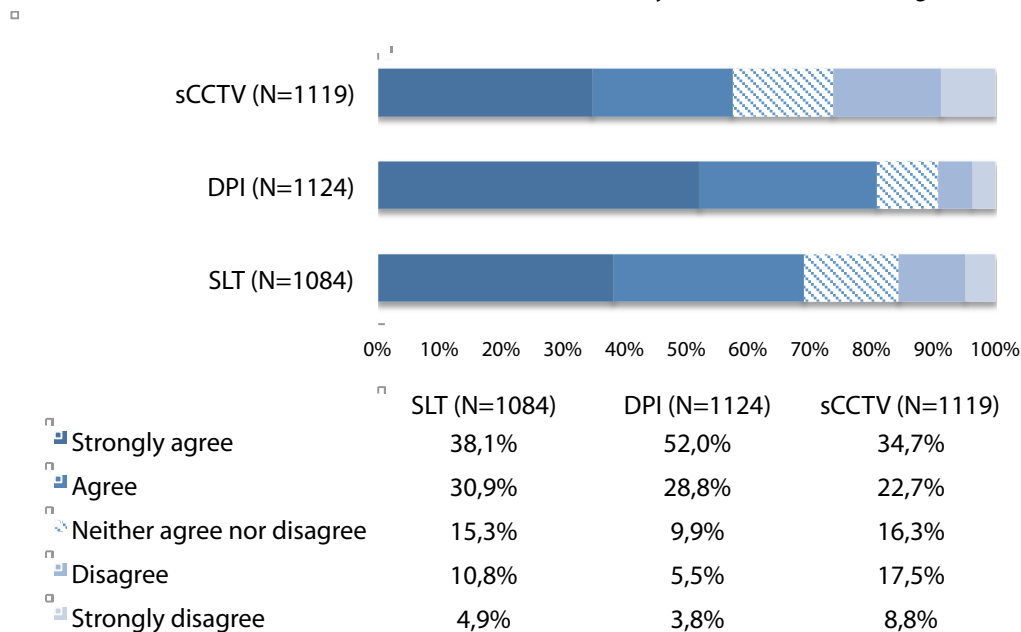


Figure 25. Frequency distribution (%): Perceived Intrusiveness – Risk of human rights infringement (I)

"sCCTV/DPI/SLT worries me because it could violate everyone's fundamental human rights."

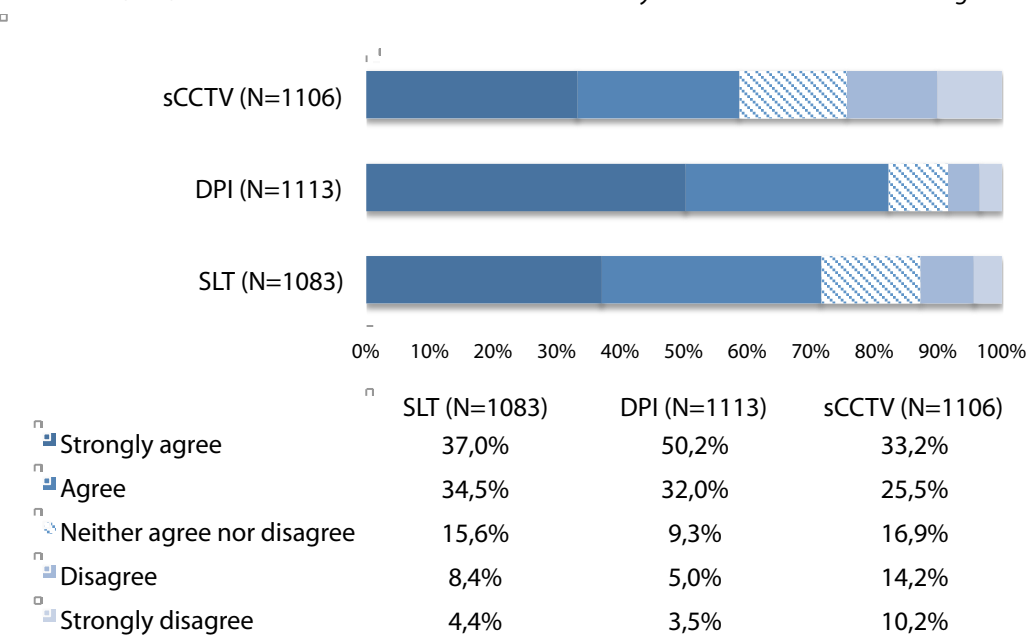


Figure 26. Frequency distribution (%): Perceived Intrusiveness – Risk of human rights infringement (II)

Temporal proximity of SOSTs

Temporal proximity refers to the extent to which future negative consequences are likely to arise out of the implementation of a given SOST.

TPRX_CCT: "I worry about how the use of smart CCTV could develop in the future."

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

TPRX_SLT: "I worry about how the use of smartphone location tracking could develop in the future."

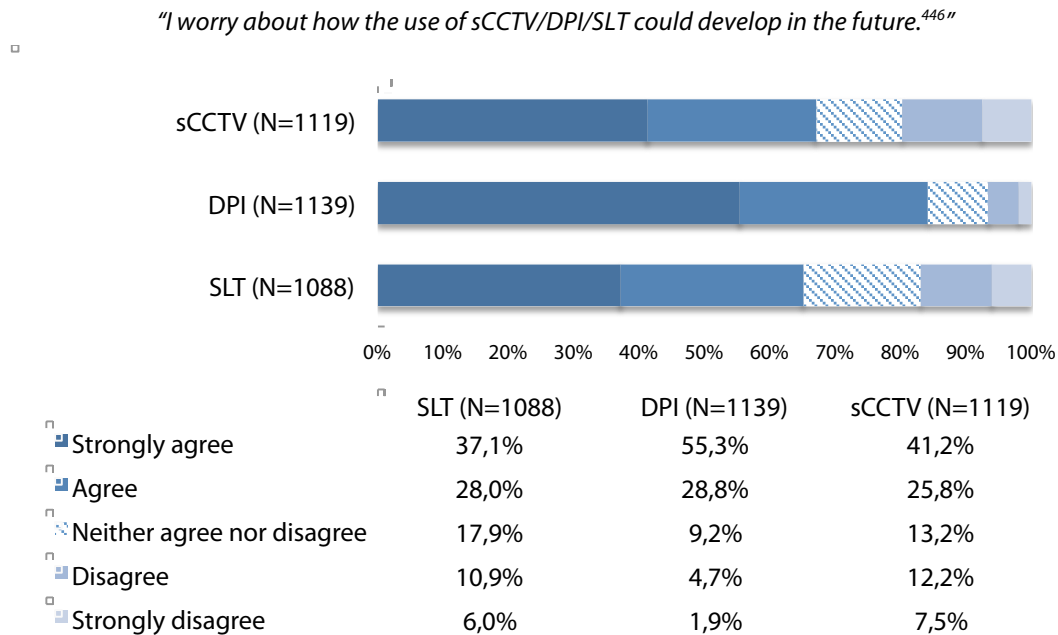


Figure 27. Frequency distribution (%): Temporal proximity

Spatial proximity of SOSTs

Spatial proximity refers to the extent to which a given SOST features in the day-to-day experience of a person. It might be that the SOST has been implemented in the neighbourhood where the person lives or in familiar places, such as the airport, the train station or even on the Internet.

SPRX_CCT: "Smart CCTV only bothers me if it is used in the areas where I live and work."

SPRX_DPI: "DPI only bothers me if it is used to track my online activities."

SPRX_SLT: "Smartphone location tracking only bothers me if it is used to track my own smartphone."

⁴⁴⁶ This table combines the results of the three SOSTs across the nine countries.

"sCCTV/DPI/SLT/ only bothers me if it is used.. in areas where I live and work/ to track my online activities/ to track my own smartphone."

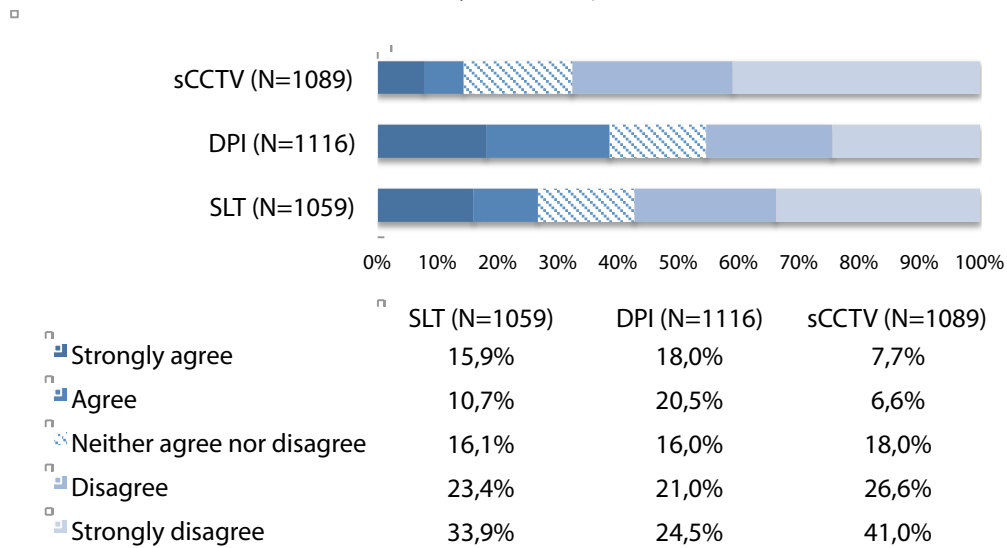


Figure 28. Frequency distribution (%): Spatial proximity

Social Proximity of SOSTs

Social proximity refers to the extent to which a given SOST has a well-defined target or whether it treats everyone as potential suspects.

SOCX_CCT: "Smart CCTV does not bother me as long as it only targets criminals."

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

SOCX_SLT: "Smartphone location tracking does not bother me as long as it only targets criminals."

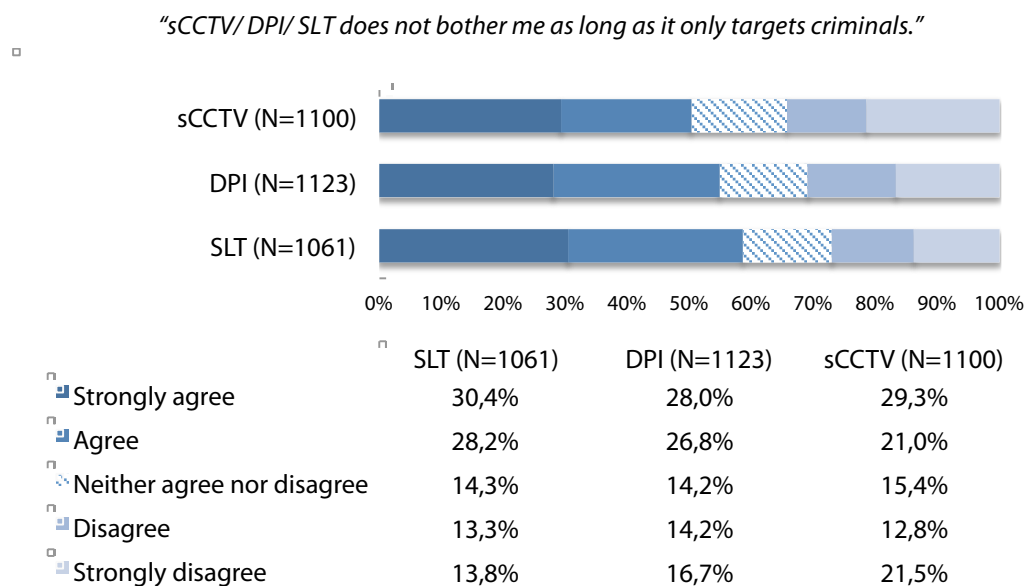


Figure 29. Frequency distribution (%): Social proximity

Physical Privacy Concerns

Concerns related to physical privacy mainly refer to three central aspects, which are: anonymity, intimacy and solitude. More details on this typology can be found in section 4.4.2 of this report.

Anonymity, a word which refers to the possibility of acting without being identified, here is used to identify a situation where individual behaviour is protected against collective pressure and performative social expectations. Westin emphasised the importance of anonymity because it was crucial to protect from social pressure those people who wished to interact in public but could feel intimidated or constrained in case their identity would be known to the public. The reason for safeguarding this dimension of privacy stems from the need to preserve social interaction of all kinds: the impossibility of being identified encourages freedom of expression, disconnects the act from the actor and prevents misinterpretation. In this respect, anonymity fosters 'autonomy' and self-determination, which are enabled by the chance of not being identified. This dimension also protects people and makes them free to experience new behaviours, make mistakes and act in an autonomous way without any concern of being judged, misinterpreted or discriminated. In the operationalization of this dimension, we chose not to make reference to the broader concept, but rather to this specific aspect – that is the possibility provided by anonymity to act without being identified and, thus of being misinterpreted.

SPC_CCT1: "Smart CCTV worries me because it could result in my behaviour being misinterpreted."

SPC_DPI1: "DPI worries me because it could result in my behaviour being misinterpreted."

SPC_SLT1: "Smartphone location tracking worries me because it could result in my behaviour being misinterpreted."

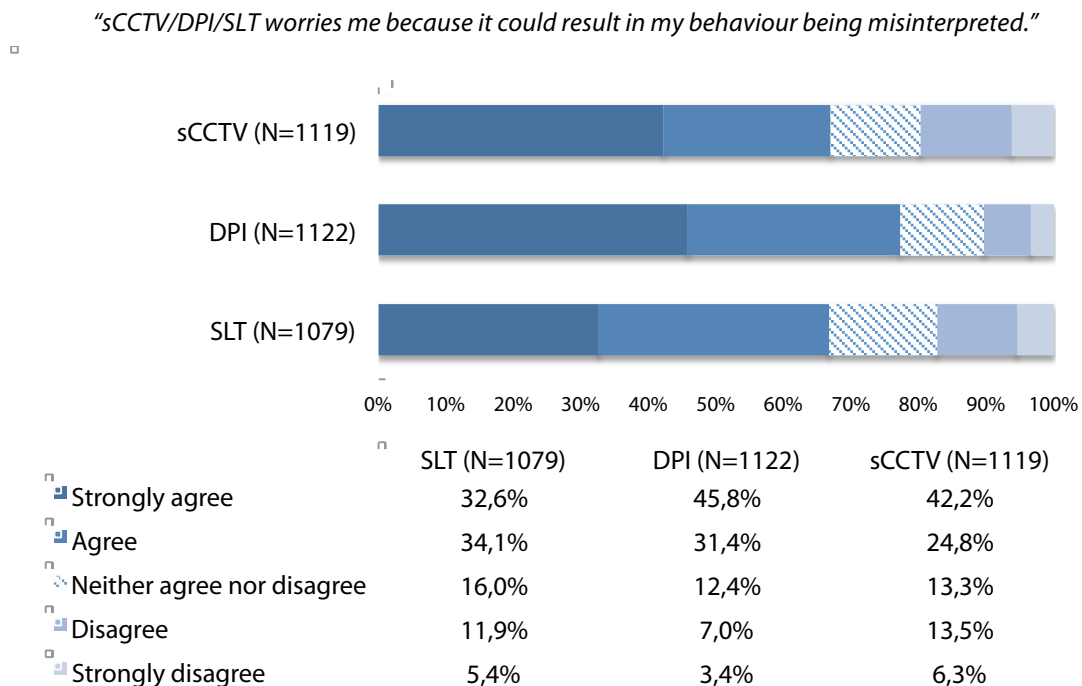


Figure 30. Frequency distribution (%): Substantive Privacy Concerns. – Anonymity

Intimacy refers to the safeguard of a person's body, feelings and emotions. This dimension not only reflects the sacredness of the physical self, but also the need of respecting the most intimate relationships, like the ones between lovers, family members or close friends.

SPC_CCT2: "Smart CCTV worries me because it could reveal sensitive information about me."

SPC_DPI2: "DPI worries me because it could reveal sensitive information about me."

SPC_SLT2: "Smartphone location tracking worries me because it could reveal sensitive information about me."

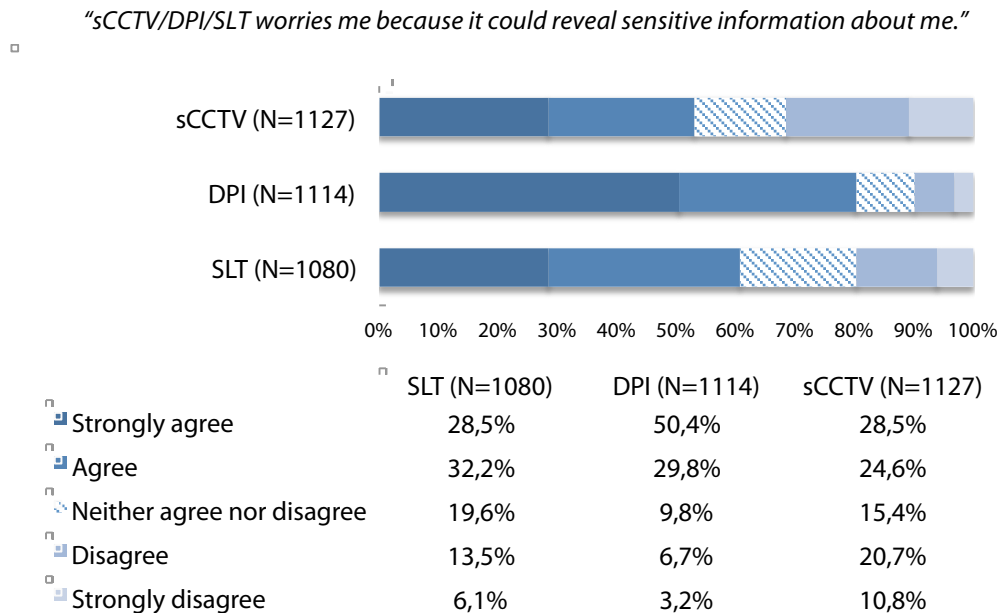


Figure 31. Frequency distribution (%): Substantive Privacy Concerns. – Intimacy

Solitude refers to the ability to physically withdraw from social interaction. This dimension concerns the right to move freely in the physical space, either to stay isolated and escape, or to go to places we like, without having to worry about being tracked or monitored.

SPC_CCT3: "Smart CCTV worries me because it could let strangers know where I am."

SPC_DPI3: "DPI worries me because it could let strangers know where I am."

SPC_SLT3: "Smartphone location tracking worries me because it could let strangers know where I am."

"sCCTV/DPI/SLT worries me because it could let strangers know where I am."

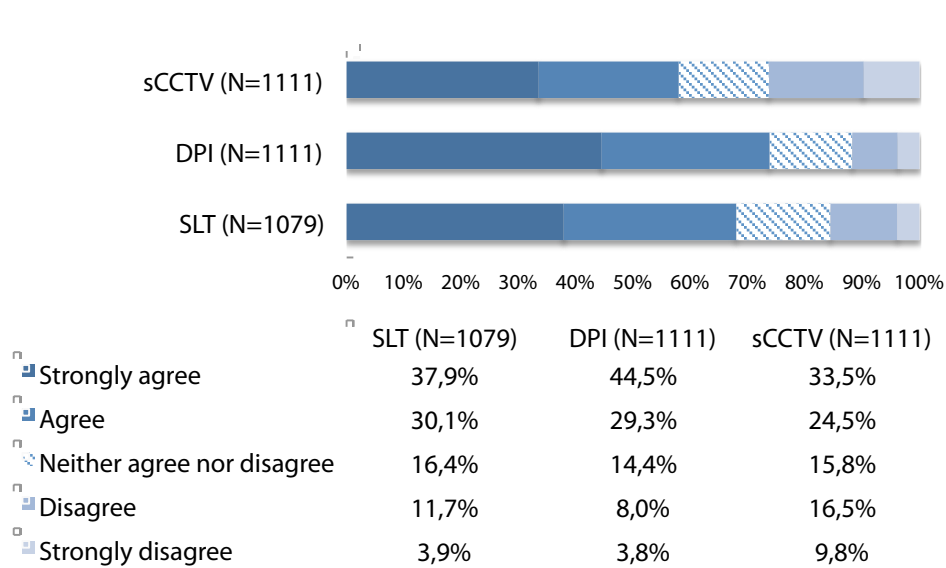


Figure 32. Frequency distribution (%): Substantive Privacy Concerns – Solitude

Institutional trustworthiness

Institutional Trustworthiness refers to the extent to which a particular institution is considered trustworthy, in the sense it is perceived that the institutions can meet its objectives, is concerned about the welfare of citizens and likely to act in good faith. In the context of this study we will investigate the level of trustworthiness of institutions that use SOSTs (i.e., security agencies).

TRU_CCT1: "Security agencies which use Smart CCTV are trustworthy."

TRU_DPI1: "Security agencies which use DPI are trustworthy."

TRU_SLT1: "Security agencies which use SLT are trustworthy."

"Security agencies which use sCCTV/DPI/SLT are trustworthy."

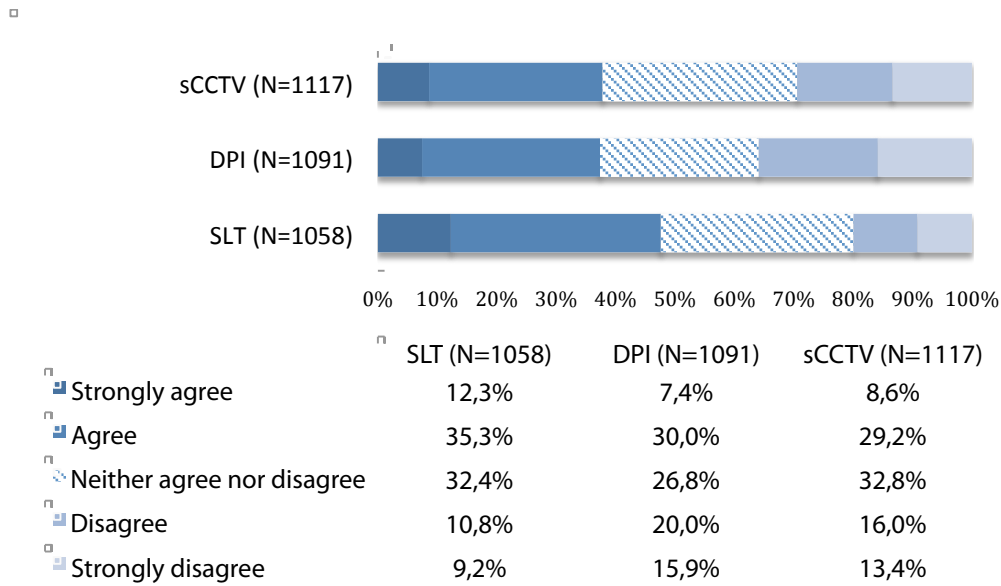


Figure 33. Frequency distribution (%): Institutional trustworthiness

The concept has three dimensions:

- 1) **Ability** – whether the institution is perceived to be able to do what it sets out to do.
TRU_CCT2: "Security agencies which use Smart CCTV are competent at what they do."
TRU_DPI2: "Security agencies which use DPI are competent at what they do."
TRU_SLT2: "Security agencies which use SLT are competent at what they do."

"Security agencies which use sCCTV/DPI/SLT are competent at what they do."

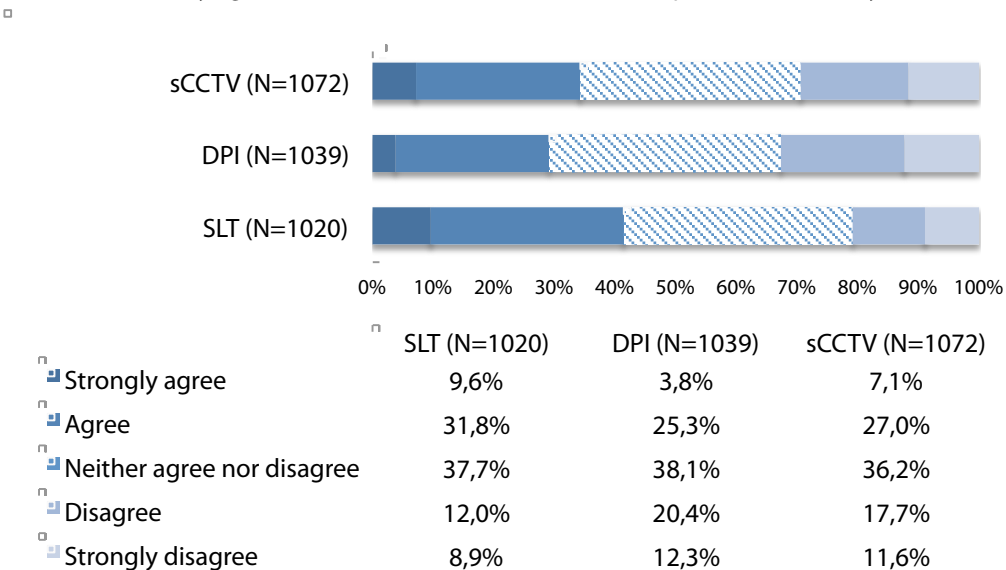


Figure 34. Frequency distribution (%): Institutional trustworthiness – Ability

- 2) **Benevolence** – whether the institution is perceived to be concerned about welfare and integrity.

TRU_CCT3: “Security agencies which use Smart CCTV are concerned about the welfare of citizens as well as national security.”

TRU_DPI3: “Security agencies which use DPI are concerned about the welfare of citizens as well as national security.”

TRU_SLT3: “Security agencies which use SLT are concerned about the welfare of citizens as well as national security.”

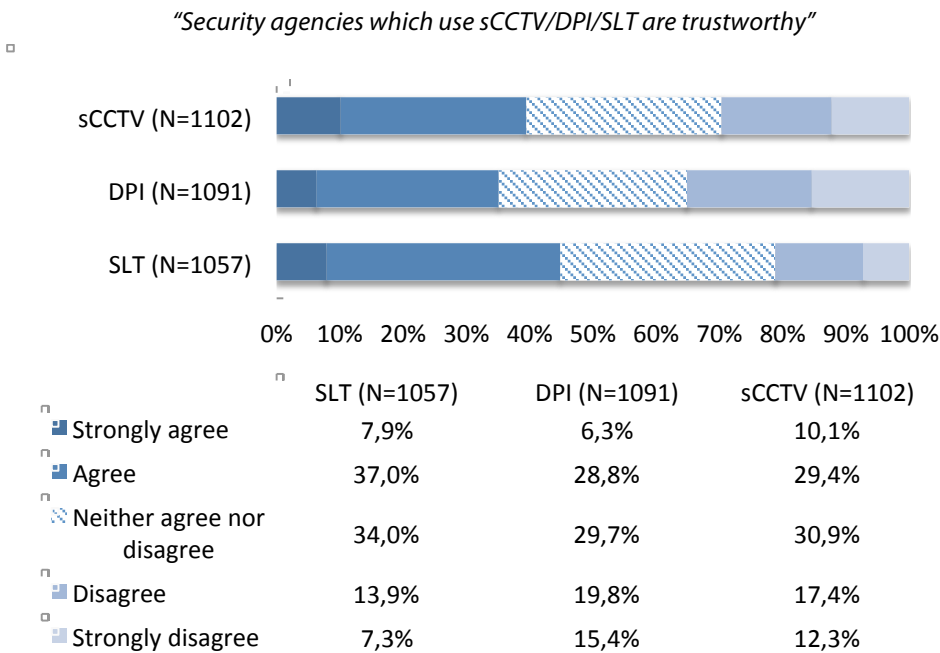


Figure 35. Frequency distribution (%): Institutional trustworthiness – Benevolence

- 3) **Integrity** – whether the institution is perceived to act in good faith and do not abuse their powers.

TRU_CCT4: “Security agencies which use Smart CCTV do not abuse their power.”

TRU_CCT4: “Security agencies which use Smart CCTV do not abuse their power.”

TRU_CCT4: “Security agencies which use Smart CCTV do not abuse their power.”

"Security agencies which use sCCTV/DPI/SLT do not abuse their power."

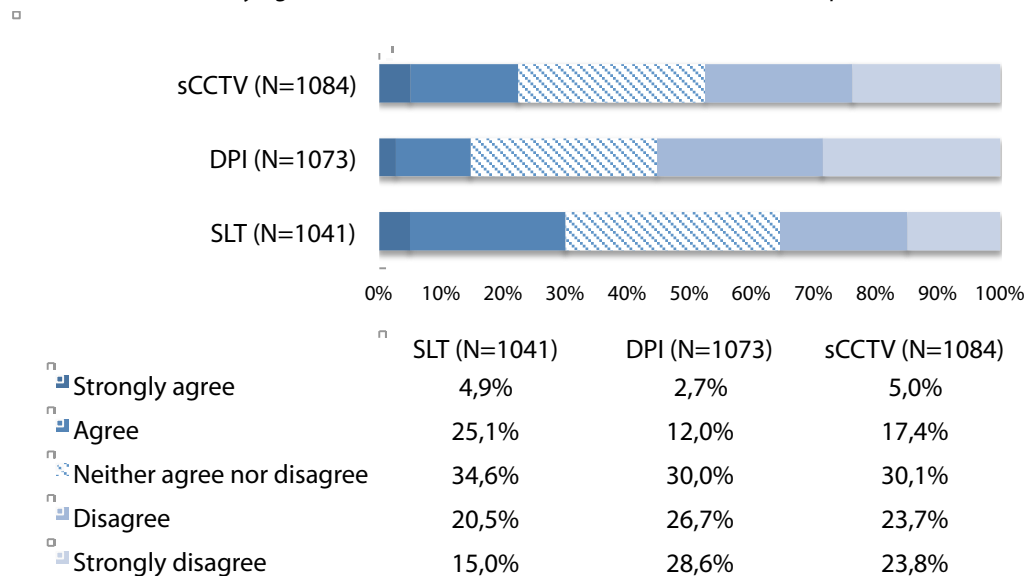


Figure 36. Frequency distribution (%): Institutional trustworthiness – Integrity

Regulation

Regulation refers to the perceived effectiveness of laws and regulations in ensuring that SOSTs are used in a lawful way and not abused or misused.

Participants were asked to select this option in case they agreed with the statement.

REG_CCT: "Laws and regulations ensure that smart CCTV is not misused."

REG_DPI: "Laws and regulations ensure that DPI is not misused."

REG_SLT: "Laws and regulations ensure that smartphone location tracking is not misused."

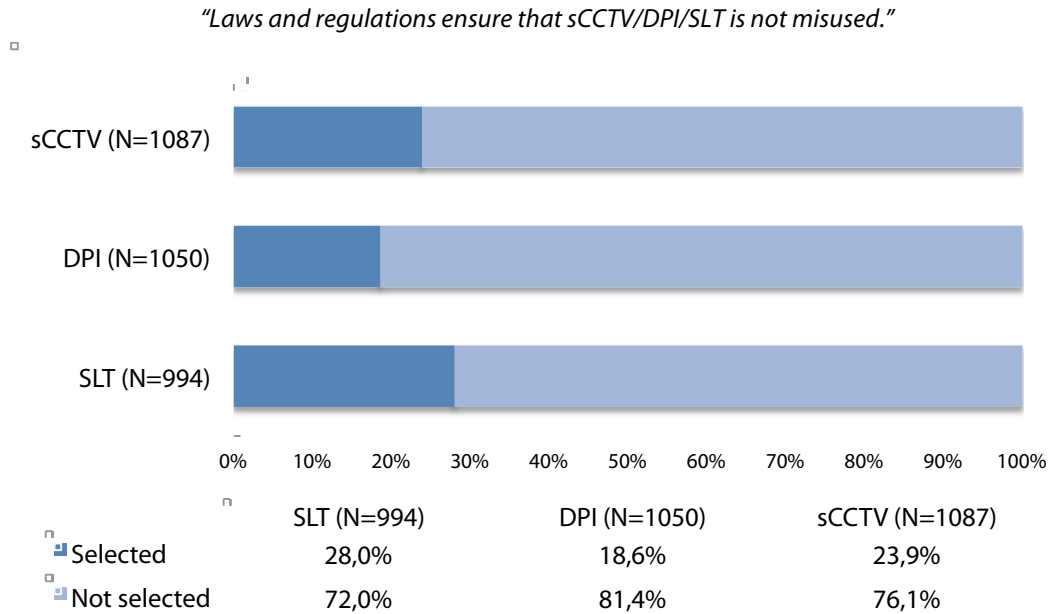
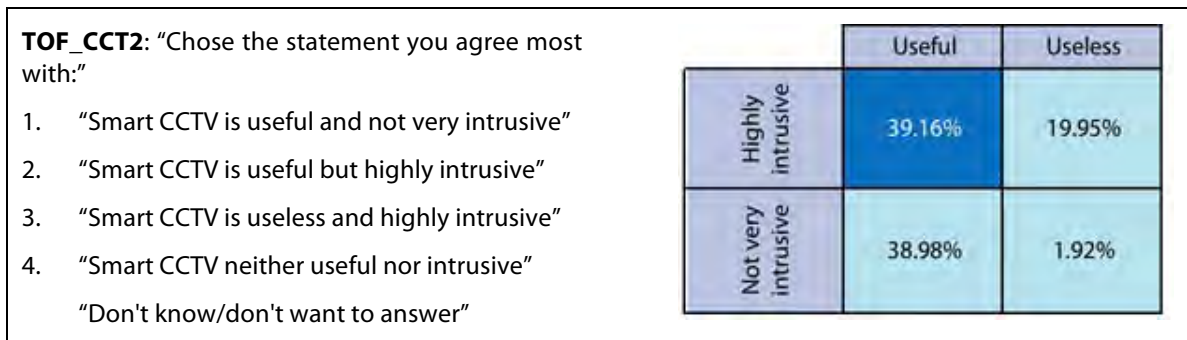


Figure 37. Frequency distribution (%): Regulation

Security and Privacy: a risk-benefit balance

The risk-benefit balance refers to the trade-off framework for assessing the acceptability of a specific SOST. Specifically, it is the extent to which a specific SOST is considered useful or useless, in terms of security, and/or risky or harmless in terms of privacy

Figure 38. Frequency distribution (%): Risk-Benefit balance – sCCTV (N=1093)⁴⁴⁷

⁴⁴⁷ The reason behind treating this variable in a different way, i.e., by addressing it in each SOST separately, is that this variable is a nominal variable with four options. Contrary to the other variables, it is not measured through a Likert scale. The variable proceeds from the matrix developed by Pavone and Degli Esposti (2012).

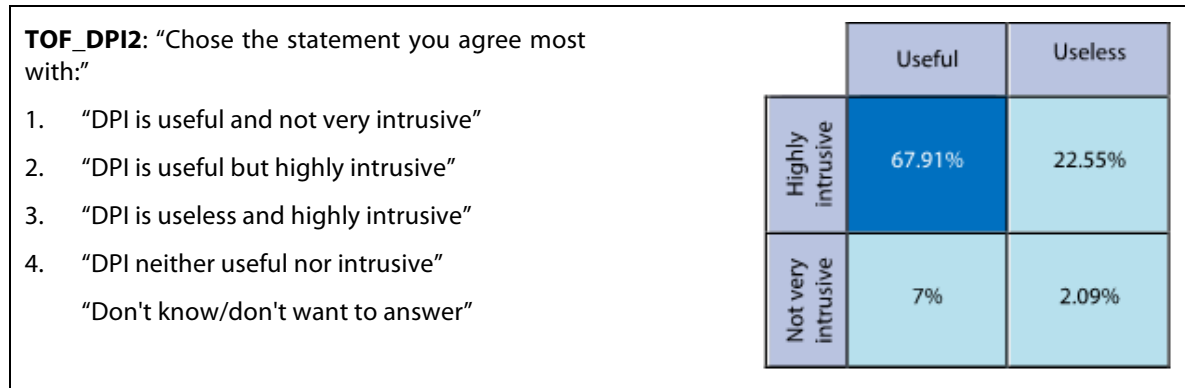


Figure 39. Frequency distribution (%): Risk-Benefit balance – DPI (N=1100)

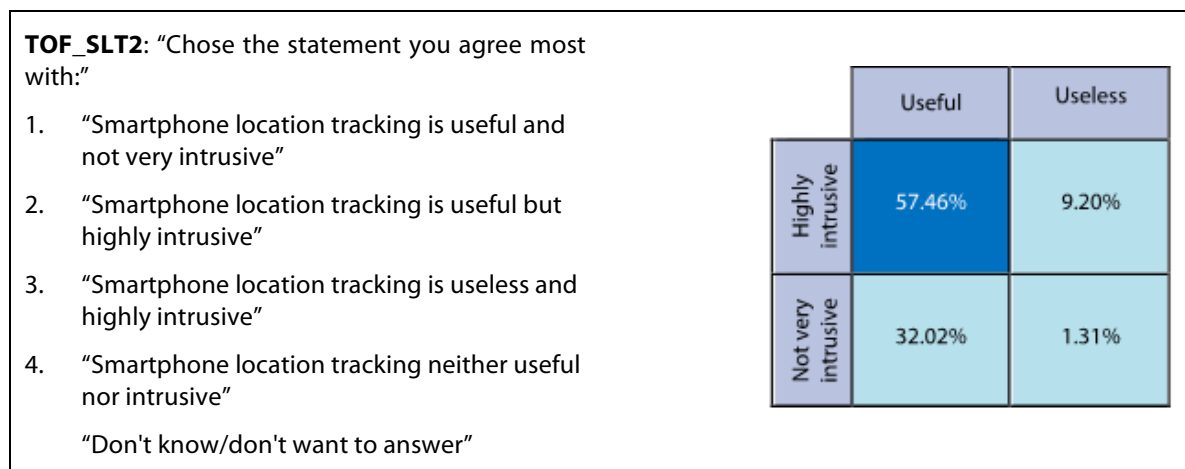


Figure 40. Frequency distribution (%): Risk-Benefit balance – SLT (N=1065)

Study of the relationship between interpreting privacy and security in terms of a trade-off on people's willingness to accept a specific SOST

In this section, we would like to draw from the data above presented in order to make a different consideration. As explained in section 5.3.6, when confronted with specific SOSTs, people can react in different ways. They can consider a certain SOST...

- 1) ...useful in terms of security and not privacy invasive
 - a. Useful and not intrusive
- 2) ...useful in terms of security, but risky in terms of privacy
 - a. Useful but highly intrusive
- 3) ...not very effective, while extremely annoying and privacy invasive
 - a. Not useful and highly intrusive
- 4) ...or unable to increase security or to diminish one's privacy.
 - a. Neither useful nor intrusive.

Case (1) above represents the optimal scenario: the SOST is perceived to improve personal safety without triggering any privacy-related conflict. In contrast, case (3) represents the worst scenario: The SOST generates public discontent without making people feel more secure. The category featuring an open controversy is represented in case (2), where people see clearly the inverse relationship linking effectiveness and intrusiveness, as exposed at the beginning of this chapter. A comparison of the charts

below, demonstrates the higher level of public discontent and outrage produced by DPI than for sCCTV or SLT. While in the case of sCCTV, 39% of participants in 6 countries considered the technology as effective and not very intrusive (32%, in the case of SLT), only 7% of participants said the same about DPI. Almost all participants found DPI to be highly intrusive (90%), while only more than the majority considered DPI effective (68%).

Examining national differences (see Deliverable 6.10), Danish (51%), Hungarian (63%) and British (51%) participants were the ones who supported sCCTV the most; in contrast German participants considered sCCTV highly intrusive and even useless (59%). While a good proportion of participants in all countries, and especially Austrian ones (42%), liked SLT, Danish participants considered SLT as highly intrusive (60%). DPI was rejected especially by Austrian participants, who considered it not only very intrusive, but also not very useful (50%). In contrast, the large majority of participants in all countries – especially German (90%) and Spanish (86%) participants – said to consider DPI useful but highly intrusive.

In this section, we suggest to use a different visualization of the results already shown in Fig.38 in order to make a different consideration. The green section of the three pies represents the percentage of people who consider a specific SOST useful and not intrusive. In contrast the red section indicates how many people think the technology as very intrusive and not useful. People who consider the SOST as both very useful and very intrusive potentially see a trade-off between the security benefits and the privacy risks: this group of people is coloured in blue. The point we want to make here is the visualisation provided by the pie graph can be used as a test to help policy makers choose between different alternative measures: the pie with the greatest green section would be preferable over the others, provided the reasons for the discontent expressed by the people in the red section are addressed. National and regional differences must also be taken into account.

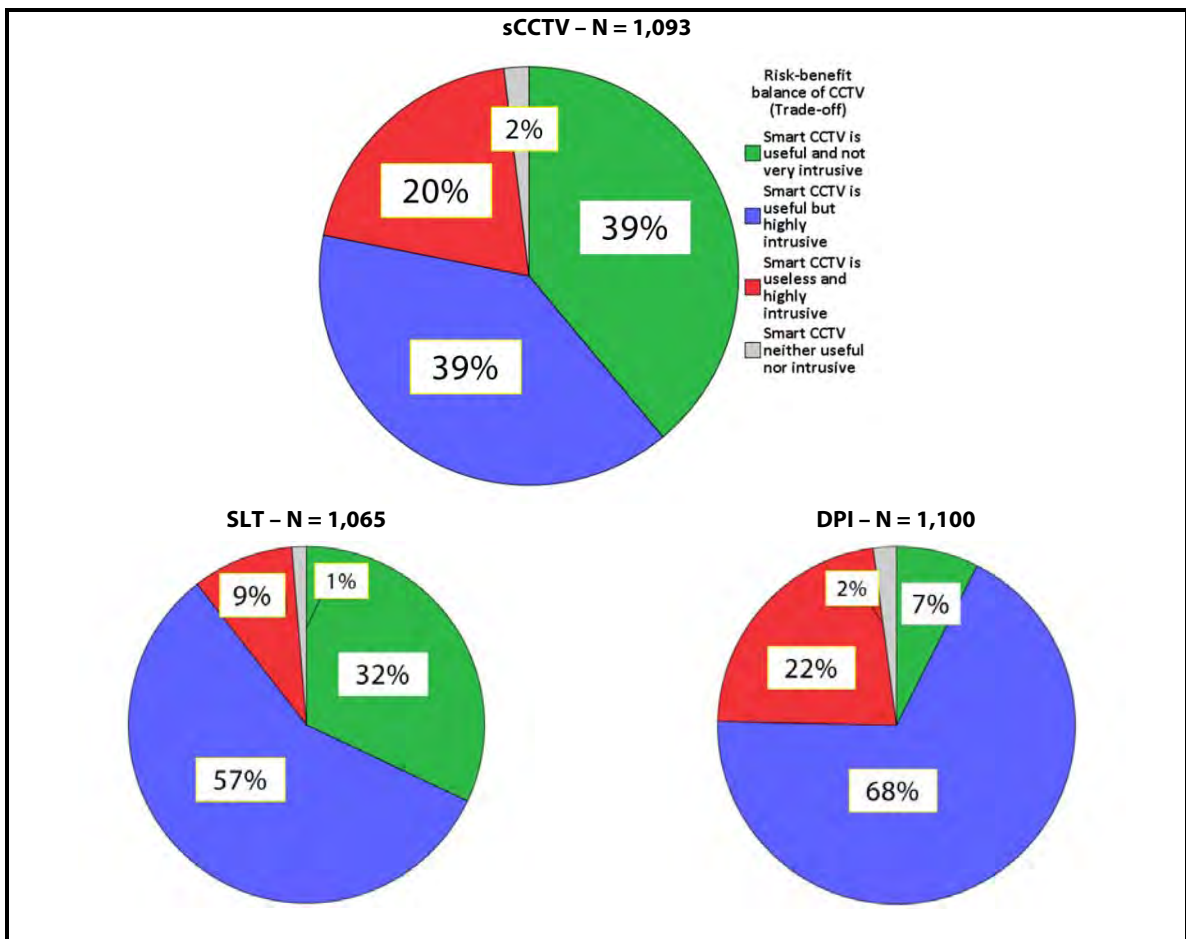


Figure 41: Perceptions regarding the risk-benefit balance of sCCTV, DPI and SLT in the overall sample (valid percent).

For instance, as explained above, most of the support for sCCTVs comes from the UK. The British example makes us think that, in terms of strategic decisions in the area of security product development, it could be considered a not-so-risky strategy to develop an add-on to an existing system, such as adding a smart component to a wide already existing CCTV network. We must be careful in attributing this outcome to people's familiarity with the technology though: it is the high degree of trust in the public security agencies managing the UK CCTV system, and its effectiveness in bringing evidence to court cases, which explains most of the support for sCCTVs in Britain rather than the level of familiarity with the system. Another more nuanced aspect emerging from the analysis of the qualitative data makes us think about the importance of specific sociological and cultural aspects: in a multicultural society where people often relocate, the CCTV camera might be seen as a replacement of the caring eye of what was, in the past, a family's friend or trusted neighbourhood resident.

6.3 Factors influencing acceptability of SOST

6.3.1 Summary of results

In chapter five, the theoretical model was developed by drawing insights from three streams of literatures: the public engagement with science literature, and privacy and risk analysis studies. The theoretical model (fig. 3), has been translated in this chapter into an empirical model. The empirical declaration (i.e. measured variables) of the concepts presented in chapter five has been presented in the previous sections of this chapter. This section presents the test of association used to assess the influence of several different factors on Acceptability, as well as the relationships among the same factors. An overview of these results is reported below, while a more in-depth discussion of these results is contained in the subsequent sections.

Before we move on presenting the results some clarifications are needed. During the development of the empirical model (D4.1) a map describing the relationship between each factor and Acceptability was drawn. Acceptability here represents the dependent variable; in other words the phenomenon we want to investigate.⁴⁴⁸ This map was used in building the statistical models and testing the actual propositions explained below. All hypotheses elaborated in D4.1 are listed in the subsequent section and progressively numbered (i.e. H#). The content of these hypotheses were further refined and transposed into more specific propositions. Each proposition has been progressively numbered (P#) and used either in the structural equation analysis model or in the quantile regression models (both explained in the appendix). In some cases, the same hypothesis H# may have been tested by means of two or more associated propositions (e.g.: P1, P2, and so on). Thus the proposition (P#) represents the exact formulation of the hypothesis *effectively tested*. The outcome of the test is reported in the tables displayed in the Appendix and also indicated by the expression "P# accepted/rejected". The expression "P# accepted", used in the following section, thus means that the content of the proposition has been confirmed by the statistical analysis.⁴⁴⁹ Relationships among different factors have also been studied and results are reported in the following sections.

For a comprehensive view of all propositions tested by means of the structural equation modelling (SEM) method please see figure 41. For details on the specific results obtained and the statistical technique used, please go to the Appendix, where all tables of results are displayed. For a summary of all tested propositions – either in the SEM model or by using quantile regression – please read table 16.

⁴⁴⁸ By dependent variable we mean the construct we want to investigate, while by independent variable (IV) we mean the factors likely to influence the DV.

⁴⁴⁹ Please bear in mind that the way terms such as "hypothesis" or "rejection" are used in inferential statistics differs from the use made here of these terms. For any inquiry related to the methodology used and the statistical analyses performed, please contact Sara Degli-Esposti (sara.degliesti@ismsforum.es).



Figure 41. Graph showing all not-rejected hypotheses according to SEM results

6.3.2 Effects of different factors on SOST Acceptability: Hypothesis testing

Acceptability was measured for each SOST (sCCTV, DPI and SLT) by computing an unweighted average of the standardised variables measuring Acceptance, Avoidance and Resistance (see section 6.6.1). This index was used in the SEM model. The questions asking about SOST acceptability in general have also been used as dependent variables in the quantile regression analysis (see section 6.6.2).

The main factors positively affecting the acceptability of new or controversial surveillance-based security technologies are: SOST's Perceived Effectiveness (P3); security agencies' perceived Trustworthiness (P11); and the fact that the measure clearly target criminals (Social Proximity – P7). SOST's Perceived Intrusiveness (P5) and a person's overall Privacy Concerns (P8) negatively influence the likelihood of considering SOST acceptable. Other factors which also play a role in determining SOSTs' acceptance are: Positive pre-existing Attitudes towards the use of Technologies to tackle security problems (P41-P43-P44). In addition, participants who considered a specific SOST as effective and not intrusive were more likely to support the implementation of the SOST (P48). In contrast, we found limited support in favour of the thesis that, when confronted with the choice of giving-up privacy for more security, people are willing to accept the exchange. In this study, participants who recognised the need to give up some of their privacy for better security were more willing to accept the SOST only in the case of DPI. We did not find similar results in the case of Smart CCTV and SLT. At this stage we can only speculate on the possible reasons explaining this outcome: it could be that seeing SOSTs as both privacy infringing and security enhancing makes SOSTs more acceptable ONLY under special conditions, possibly present in the case of DPI, which should be further investigated in future studies. We also found limited support for the fact that the perceived level of Threat increases the likelihood of considering SOSTs to be acceptable (see section on 'Factor no. 3' and P39-40).

Furthermore, SOSTs perceived as highly intrusive tend to be considered as less effective (P15). The more people are concerned about their privacy, the more they also tend to see SOSTs as intrusive (P26). SOSTs which are considered to be accurate and effective are less likely to trigger privacy concerns (P31). SOSTs which are managed by trustworthy agents are also perceived to be more effective (P29). SOSTs which clearly target criminals and are not part of blanket surveillance strategies are also perceived as

both less intrusive (P25) and more effective (P17). People who are concerned about future risks of a SOST and about the way it may evolve in the future are more likely to find SOSTs intrusive (P28) and to be concerned about their privacy (P35). The fact that SOSTs are implemented in areas where people live and work, also raises privacy concerns (P34). People who understand how SOSTs work are also more likely to consider SOSTs as intrusive (P23). Finally, old people tend to accept SOSTs more than young people. Other personal characteristics, such as gender, education level, or income seem not to influence SOST acceptability. In the following sections we discuss these results in further details.

FACTOR no. 1: General Attitudes towards Technology to foster Security

H1a. The more that citizens approve of technology to foster security, the more likely they are to find SOSTs acceptable.

Technology Supporters – **P41:** The more that people believe that the use of SOSTs improves national security the more likely they are to find SOSTs acceptable. [P41 accepted in all cases].

Technology Supporters – **P43:** The more that people believe that “if you have done nothing wrong you do not have to worry about surveillance-orientated security technologies”, the more likely they are to find SOSTs acceptable. [P43 accepted in all cases].

Technology Supporters – **P44:** The more that people believe that “If surveillance-orientated security technology is available national governments might as well make use of it”, the more likely they are to find SOSTs acceptable. [P44 accepted in two cases].

H1b. The less citizens approve of technology to foster security, the less likely they are to find SOSTs acceptable.

Technology Detractors – **P42:** The more that people believe that “surveillance-orientated security technologies are only used to show that something is being done to fight crime”, the less likely they are to find SOSTs acceptable. [P42 accepted only in one case].

Technology Supporters – **P45:** The more that people believe that “once surveillance-oriented security technologies are in place they are likely to be abused”, the less likely they are to find SOSTs acceptable. [P45 rejected].

General attitudes toward technology refer to the extent to which a person is overall either in favour or against the use of technology to foster security. The concept has two dimensions: ‘technology detractors’, which reflect a generally negative belief about the ability of technology to enhance security; and ‘technology supporters’, which reflect a generally positive belief about the ability of technology to enhance security.

In line with the results of the PRISE project, people who are generally positive about the ability of technology to enhance security endure in their belief that SOSTs are adequate solutions to tackle security problems. People who consider that SOSTs improve national security (P41) and people who think that “they have nothing to hide” feel comfortable with the idea of implementing SOSTs (P43). The same availability of SOSTs becomes a compelling argument for supporters of technological solutions to security problems (P44). In contrast, people who are more critical about technology being the solution to security issues tend to be more suspicious and sceptical about the appropriateness of investing in security technologies (P42).

FACTOR no. 2: Familiarity with SOST

H2. The more citizens are familiar with SOSTs, the more likely they are to find them acceptable.

Familiarity with SOST (i.e. Understanding) – **P23:** The fact that citizens understand the way a particular SOST works does not exercise a direct effect on acceptability, though it does increase one’s perceptions of SOST being intrusive. (see section 6.3.3)

In other words, people who know about the functioning of a particular SOST can better appreciate its risks and potential intrusiveness. This effect is compensated, though, by agents’ perceived

trustworthiness: trust in the ability, integrity and benevolence of the security agents, operating the security system, reduces in fact the likelihood of perceiving a given SOST as highly intrusive (P29).

As discussed and studied in the risk analysis literature, the familiarity with a technology has often been considered a crucial factor positively affecting the acceptability of such technology, and that familiarity with a given set of technologies would make new, similar technologies more acceptable. However, in our study this hypothesis was rejected. To the contrary, we found that the degree of understanding of the way a specific SOST operates may increase its perception of being intrusive, which in turn decreases the likelihood of considering it acceptable.

In the analysis of qualitative data, though, we observed that in the case of Smart CCTVs, participants relied on their understanding of traditional CCTVs to express opinions on 'smart' CCTV. As a result, in those countries where people were more familiar with traditional CCTVs, they were also more supportive toward the introduction of smart CCTV. Yet, in countries where CCTVs were known but still considered a controversial solution, barely accepted, people were particularly cautious about the possibility of using smart CCTVs for security purposes. The peculiarities of smart CCTV over traditional CCTV systems – such as its algorithmic and automatic decision-making components – were also elements taken into consideration to highlight differences between traditional and smart CCTV systems.

FACTOR no. 3: Perceived Level of Threat

H3. The more citizens are concerned about threats to their security, the more likely they are to find SOSTs acceptable [Hp Rejected].

Personal Online Security – **P39:** The more people worry about security when they are online, the more likely they are to consider SOSTs acceptable [P39 accepted only in one case].

Public Security – **P40:** The more people feel that the country where they live is a safe place, the less likely they are to consider SOSTs acceptable [P40 accepted only in one case].

SOSTs generally are technologies are supposed to reduce the risk of crimes and violence. Evidence gathered in Security Studies show that in the case of SOSTs, which are technology developed to reduce security risks, people tend to become more positive about their use in the aftermath of a major security accident, such as in the case of a terrorist attack. This effect seems to disappear fairly quickly over time. So, we investigated whether the existing perceived level of security threats would make SOSTs more acceptable.

In the context of this study, we found that risks to personal online safety and public security only influenced the perceived acceptability of SOST at the beginning of the large-scale events (see Table 20). In testing H3 we used the general Acceptability question asked at the beginning and at the end of the event as dependent variable (see section 6.2.1, variable ACC1). The outcome suggests that a higher level of security concerns makes SOSTs more acceptable. The perception of insecurity online (P39) has a positive and significant impact on acceptability of SOSTs. These considerations stopped playing a role, though, by the end of the event, probably being replaced by other considerations. In contrast, opinions such as the ones shared by Technology Supporters remained constantly influential along the event (P41; P43; P44).

The analysis of the qualitative data, though, showed that in some countries, where people felt especially safe, the desire for more security measures was still strong. In some cases, the more secure people feel the more security measures they ask for. It may sound like a paradox, or it may be that people feel reassured by the existing security measures and would thus welcome more of them. We do not have enough information here to explain what looks like a paradox but more information can be found in the national reports. However, it seems clear that this issue needs to be further investigated.

FACTOR no. 4: Institutional Trustworthiness

H4. The higher citizens perceive the trustworthiness of institutions responsible for SOSTs, the more likely they are to find them acceptable.

Institutional Trustworthiness – **P11:** The higher citizens perceive the trustworthiness of institutions responsible for SOSTs, the more likely they are to find them acceptable. [P11 accepted]

The variable Institutional Trustworthiness measures whether participants considered security agents in charge of managing each SOST under study (i.e. smart CCTV; DPI; and SLT) to be trustworthy, capable, honest and benevolent. The analysis here presented showed the overall, strong positive effect of institutional trustworthiness on acceptability.

Institutional trustworthiness has become a key factor in the studies of people's acceptability of controversial technologies, discussed both in the contextual approaches to public understanding of science and in the socio-cultural approaches to risk analysis. Institutional trustworthiness was the main factor that contextual approaches used to criticise the traditional deficit model, which underpinned most of public understanding of science studies. This perspective suggested that it was not so much the degree of people's knowledge about, or familiarity with, a technology that makes them more or less hostile to new technologies, but rather the degree of trust they had in the institutions managing such technologies. **The more people trust scientific and political institutions, in this case security agents, the more acceptable a technology would be.** Our study clearly confirms this hypothesis.

In practical terms, this means that, when it comes to SOSTs, security agencies and institutions should be significantly more concerned about the degree of trust they enjoy than about how well technologies are known to the public or how familiar people are with those technologies. If we wanted to know more about the effect of each sub-dimension of institutional trustworthiness on acceptability, we might look at other analyses of these data reported in other publications and notice how security agents' ability, integrity and benevolence play a more or less important role in the case of each specific SOST.⁴⁵⁰

FACTOR no. 5: Perceived Effectiveness of SOSTs

H5. The more citizens perceive SOSTs to be effective, the more likely they are to find them acceptable.

Perceived Effectiveness – **P3:** The more citizens perceive SOSTs to be effective, the more likely they are to find them acceptable. [P3 accepted]

FACTOR no. 6: Perceived Intrusiveness of SOSTs

H6. The more citizens perceive SOSTs to be intrusive, the less likely they are to find them acceptable.

Perceived Intrusiveness – **P5:** The more citizens perceive SOSTs to be intrusive, the less likely they are to find them acceptable. [P5 accepted]

Previous studies on people's assessment of homeland security systems⁴⁵¹ suggests that both the perceived effectiveness and intrusiveness of a given security system would significantly affect people's opinions and willingness to accept the system. The present study confirms these results: the degree of intrusiveness and the degree of effectiveness of SOSTs perceived by the public play a major role in determining the level of acceptability of SOSTs. Yet, whilst the **perceived effectiveness of SOSTs increases the acceptability of SOSTs, their perceived intrusiveness reduces it.**

However not all SOSTs are perceived as equally intrusive or equally effective. To better understand the relationship between these two dimensions – i.e. SOST's perceived intrusiveness and effectiveness – the variable Risk-Benefit Balance was introduced and its effect on Acceptability tested. The results are displayed in Tables 21-23. **Basically, if the SOST is perceived as highly effective and not intrusive, the SOST is considered highly acceptable** (P48). Considering a SOST as highly intrusive and not effective has no effect of Acceptability instead (P50). Finally, relying on the privacy-security trade-off model in assessing the acceptability of SOST, and thus believing that the SOST is both intrusive and effective, makes the SOST more acceptable only in the case of highly controversial technologies, such as in the case of DPI (P49). Further explanations are provided in the following section.

⁴⁵⁰ Degli Esposti, Sara (2014) "A Roadmap for developing acceptable surveillance-based security measures". Proceedings of the 9th Security Research conference » FUTURE SECURITY«, Institutes of Fraunhofer (Group for Defense and Security VVS), Berlin, September 16–18, 2014, pp. 71-80.

⁴⁵¹ Sanquist, Thomas F, Heidi Mahy, and Frederic Morris. 2008. "An exploratory risk perception study of attitudes toward homeland security systems." Risk analysis 28 (4):1125-1133.

FACTOR no. 12: Risk-Benefit Balance

H12. The more that citizens perceive the benefits of SOSTs to outweigh the risks, the more likely they are to find them acceptable.

P48: The more that people consider SOST to be effective and not intrusive, the more likely they are to find SOST acceptable. [P48 accepted].

P49: The more that people consider SOST to be effective as well as intrusive, the more likely they are to find SOST acceptable. [P49 accepted only in the case of DPI].

P50: The more that people consider SOST not to be effective but highly intrusive, the less likely they are to find SOST acceptable. [P50 rejected].

As expected, people who see only benefits in the use of SOSTs will support them the most. More intriguing is the result of proposition 49. It appears that only in the case of DPI, the participants who considered DPI as both highly intrusive and highly effective were more willing to accept this SOST. In general, though, seeing a technology as both intrusive and effective does not positively influence the acceptability of SOSTs. Finally, we do not find evidence to confirm the hypothesis that people who consider SOSTs very intrusive but hardly effective will be more likely to oppose them. This finding needs to be further investigated.

FACTOR no. 7: Temporal Proximity

H7. The more citizens perceive that SOSTs will affect their future lives, the less likely they are to find them acceptable.

This hypothesis has been rejected. **Temporal proximity does not directly influence SOSTs' acceptability.** However, we found that it has an effect on SOST Perceived Intrusiveness and Substantive Privacy Concerns, which, in turn, decrease the likelihood of considering a SOST acceptable.

Temporal Proximity exercises an indirect effect on Acceptability through Substantive Privacy Concerns and Perceived Intrusiveness. It not only increases the perception of SOST being intrusive (P28), but it also raises a person's overall Privacy Concerns (P35), which in turn increases the perception of intrusiveness (P26). See section 6.3.3 for further details.

FACTOR no. 8: Spatial Proximity

H8. The more citizens perceive SOSTs to be part of their day to day experience, the more likely they are to find them acceptable.

This hypothesis has been rejected. **Spatial Proximity does not directly influence SOST Acceptability either.** However, we found that it has an effect on Substantive Privacy Concerns, which decreases the likelihood of considering SOST acceptable.

Spatial Proximity exercises an indirect effect on Acceptability through Substantive Privacy Concerns (P34), though it does not directly influence Acceptability.

FACTOR no. 9: Social Proximity

H9. The more citizens perceive SOSTs to be targeted at others rather than themselves, the more likely they are to find them acceptable.

Social Proximity – **P7:** The more citizens perceive SOSTs to be targeted at others rather than themselves, the more likely they are to find them acceptable. [P7 accepted].

Spatial proximity is one of most discussed factors in risk analysis studies and has often been one of the most powerful arguments used by policy makers to de-activate hostility from civil society towards the implementation of new technologies. Also known as the NIMBY ("not in my backyard"), this factor suggests that people may find a risky technology more acceptable if it is implemented far from their meaningful network of places familiar to them. This factor has been extensively explored in

relation to the implementation of nuclear power plants, dumping sites or liquid gas converters, producing mixed results. In this study we decided not only to investigate *spatial proximity*, i.e., the perceived geographical proximity of SOSTs to the participants, but also the *social proximity*, i.e., the degree to which participants feel targeted by SOSTs or, in contrast consider that SOSTs target other social groups; and *temporal proximity*, i.e., the possibility that SOSTs may affect participants' life in the future.

Social proximity has a direct and negative influence in the acceptability of SOSTs. **In other words, the more participants perceive SOSTs to be targeted at others rather than themselves, the more likely they are to find a SOST more acceptable.** However, as the analysis of the qualitative data shows, this result may not be equally valid in all countries: Austrian and German participants were highly critical and did not consider the targeted use of SOSTs to be an adequate response to their concerns.

FACTOR no. 10: Substantive Privacy Concerns

H10a. The more citizens are concerned about their information privacy, the less likely they are to find SOSTs acceptable.

H10b. The more that citizens are concerned about their physical privacy, the less likely they are to find SOSTs acceptable.

Substantive Privacy Concerns – **P8:** The more citizens are concerned about their privacy, the less likely they are to find SOSTs acceptable. [P8 accepted].

As proposed by several privacy scholars and advocates, the level of concerns regarding one's privacy can also affect the acceptability of SOSTs. Drawing from earlier studies, and considering the lively debate on the meanings and typologies of privacy, discussed earlier in Chapter Four of this report, we tested the effects of a person's overall privacy concerns, both information and physical privacy concerns, on acceptability. Interestingly, we can confirm that privacy concerns (both concerns for physical privacy and concerns for the privacy of personal communication and information), are likely to influence the acceptability of SOSTs. Thus, **higher levels of privacy concerns make SOSTs less acceptable.**

FACTOR no. 11: Regulation

H11. The more that citizens perceive the regulations governing SOSTs to be effective, the more likely they are to find them acceptable.

Regulation – **P47:** The more citizens think that "laws and regulations ensure that a specific SOST is not misused", the more likely they are to find SOSTs acceptable. [P47 rejected].

Regulation refers to the perceived effectiveness of laws and regulations play in ensuring that SOSTs are used in a lawful way and not abused or misused. We did not find evidence to support this hypothesis, probably due to its operationalization and the fact that this variable was not measured on an ordinal scale. From the table discussion emerged also a general lack of awareness and knowledge of the regulatory framework governing each SOST.

Demographic and cultural factors

Age – **P1:** The older citizens are, the more likely they are to find SOSTs acceptable. [P1 accepted].

Education – **P36:** Low educated people are more likely to find SOSTs acceptable. [P36 rejected].

Income – **P37:** High income people are more likely to find SOSTs acceptable. [P37 rejected].

We found out that the age of participants is a relevant factor influencing acceptability of SOSTs. All the other socio-demographic variables, such as gender, income and education, were not significant. Older participants in the summits showed a tendency to find SOSTs more acceptable than younger participants. This runs contrary to common wisdom, which expected younger people to be more open, due to their

familiarity with these technologies, and to be, thus, less concerned with privacy. On possible explanations for our results is that older participants, given their experience with European authoritarian regimes, are more distrustful, whereas younger people, who had not lived in surveillance states and had no first-hand knowledge of the consequences, are, accordingly, less concerned. There could be many explanations for this finding, and further research is needed.

However, the analysis of the qualitative data shows that younger generations spend much of their time using internet-based technologies, on smartphones, tablets and PCs, and are very accustomed to living part of their lives in and through social media. Their familiarity and understanding of digital technologies make them more aware about the risks and more prone to suffer from the negative consequences of personal data mishandling. Their identity as persons is intrinsically connected to online media and whatever constitutes a threat to their freedom of expression and digital life, effectively posits a threat to their identity and self-determination. This is, perhaps, the reason why they appear to be especially concerned about SOSTs.

Finally, country variables were used as control variables in some models (e.g. quantile regressions) and we saw that, as expected, citizens of German-speaking countries tend to be more critical and more concerned of their privacy than people from other countries. Yet we did not design questions to specifically investigate further cultural or historical dimensions, which nonetheless were briefly highlighted in some country reports.

6.3.3 Influence of some factors on other factors

As briefly mentioned in previous sections, we found that some factors did not have a direct influence on the main dependent variable, i.e., acceptability, but on other factors, which in turn influenced acceptability. In this section we briefly outline and discuss these relationships.

Factors influencing the variable Perceived Effectiveness

Perceived Intrusiveness – **P15**: The more citizens perceive SOSTs to be intrusive, the less likely they are to perceive SOSTs to be effective. [P15 accepted].

Social Proximity – **P17**: The more citizens perceive SOSTs to be targeted at others rather than themselves, the more likely they are to perceive SOSTs to be effective. [P17 accepted].

Institutional Trustworthiness – **P19**: The higher citizens perceive the trustworthiness of institutions responsible for SOSTs, the more likely they are to perceive SOSTs to be effective. [P19 accepted].

Some factors had an influence on perceived effectiveness. As an example, and according to what was expected as a result of the main analysis, **perceived intrusiveness was found to reduce the perception of effectiveness**. This result is also confirmed by the qualitative analysis, where it emerged clearly that blanket surveillance, is considered to be less effective than targeted surveillance, due to the amount of useless data retrieved. Along the same lines, we would expect social proximity also to have an impact on effectiveness, and effectively **we found out that, when they consider SOSTs to target other rather than themselves, participants tend to consider SOSTs more effective**. Finally, **institutional trustworthiness** not only makes SOSTs more acceptable, it also **encourages participants to consider SOSTs more effective, too**.

Factors affecting the variable Perceived Intrusiveness

Familiarity with SOST (Understanding) – **P23**: The more citizens understand how the technology works, the more likely they are to perceive SOSTs to be intrusive. [P23 accepted].

Social Proximity – **P25**: The more citizens perceive SOSTs to be targeted at others rather than themselves, the less likely they are to perceive SOSTs to be intrusive. [P25 accepted].

Substantive Privacy Concerns – **P26**: The more citizens are concerned about their information privacy, the more likely they are to perceive SOSTs to be intrusive. [P26 accepted]

Temporal Proximity – **P28**: The more citizens perceive SOSTs will affect their future lives, the more likely they are to perceive SOSTs to be intrusive. [Hp accepted].

Institutional Trustworthiness – **P29**: The higher citizens perceive the trustworthiness of institutions responsible for SOSTs, the less likely they are to perceive SOSTs to be intrusive. [P29 accepted].

Perceived intrusiveness was also influenced by a variety of factors. **Temporal proximity, for instance, had a negative impact on perceived intrusiveness.** In other words, when participants considered that SOSTs could affect their future lives, they also tended to consider SOSTs to be more intrusive. Similarly to perceived effectiveness, **institutional trustworthiness also encouraged participant to assess SOSTs as less intrusive**, apart from more acceptable and more effective. Again, social proximity is also relevant here, as it is for perceived effectiveness. This works the other way around: **the more participants perceive SOSTs to be targeted at others rather than themselves, the less intrusive SOSTs will appear to them.** Quite consistently with expectations, privacy concerns also affect perceived intrusiveness: **the more participants are concerned about their information privacy, the more likely they are to perceive SOSTs to be intrusive.** Finally, to a better understanding of SOST's operations and functionalities correspond a more profound appreciation of its risks and perceived intrusiveness.

Factors affecting Substantive Privacy Concerns

Perceived Effectiveness – **P31**: The more citizens perceive SOSTs to be effective, the less likely they are to be concerned about their privacy. [P31 accepted].

Spatial Proximity – **P34**: The more citizens perceive SOSTs to be part of their day-to-day experience, the more likely they are to be concerned about their privacy [P34 accepted].

Temporal Proximity – **P35**: The more citizens perceive SOSTs will affect their future lives, the more likely they are to be concerned about their privacy. [P35 accepted].

Finally, the factor named Substantive Privacy Concerns also seems to be affected by other factors.

Temporal Proximity and Spatial Proximity positively influence participants' privacy concerns. If participants consider that SOSTs are likely to affect their future life or their day-to-day experiences, they tend to be more concerned about the risks the SOST may posit to their privacy.

The Perceived Effectiveness of SOSTs negatively influences Substantive Privacy Concerns instead. Participants seem to suggest that **SOSTs, which are considered to be more effective, are also more likely to be perceived as less privacy intrusive.** This is an important result and stands directly in contrast to the basic assumptions of the trade-off model, which considers that for SOSTs to be really effective they must inevitably infringe on privacy. Moreover, it also suggests to technology developers that the implementation of Privacy-by-Design principles, which ensure full usability and privacy-protection, can become an important ally in the design of highly acceptable and effective security technologies.

No	Test	Dependent Variable	↔ Independent Variable
P1	SEM	Acceptability (SOST level)	↔ Institutional Trustworthiness
P2	SEM		↔ Substantive Privacy Concerns
P3	SEM		↔ Perceived Effectiveness
P4	SEM		↔ Perceived Intrusiveness
P5	SEM		↔ Social Proximity
P6	SEM		↔ Temporal Proximity
P7	SEM		↔ Education

P8	SEM		⇔ SOST Understanding
P9	SEM		⇔ Gender
P10	SEM		⇔ Age
P11	SEM		⇔ Age moderating the effect of Trust on Acceptability
P38	QR	Acceptability (General level)	⇔ Personal security (offline)
P39	QR		⇔ Persona security (online)
P40	QR		⇔ Public security
P41	QR		⇔ Technology Supporters (1)
P42	QR		⇔ Technology Detractors (1)
P43	QR		⇔ Technology Supporters (2)
P44	QR		⇔ Technology Supporters (3)
P45	QR		⇔ Technology Detractors (2)
P47	QR		⇔ Regulation
P48	QR		⇔ Privacy-security balance: category “useful, not intrusive”
P49	QR		⇔ Privacy-security balance: category “useful, highly intrusive”
P50	QR		⇔ Privacy-security balance : category “not useful, highly intrusive”
P36	QR		⇔ Education
P37	QR		⇔ Income
P46	QR		⇔ Gender
P12	SEM	Perceived Effectiveness	⇔ Institutional Trustworthiness
P13	SEM		⇔ Perceived Intrusiveness
P14	SEM		⇔ Social Proximity
P15	SEM		⇔ Age moderating the effect of Trust on Effectiveness
P16	SEM		⇔ Education
P17	SEM		⇔ Age
P18	SEM		⇔ Gender
P19	SEM	Perceived Intrusiveness	⇔ Institutional Trustworthiness
P20	SEM		⇔ Substantive Privacy Concerns
P21	SEM		⇔ Social Proximity
P22	SEM		⇔ Temporal Proximity
P23	SEM		⇔ SOST Understanding
P24	SEM		⇔ Age
P25	SEM		⇔ Gender
P26	SEM		⇔ Education
P27	SEM	Substantive Privacy Concerns	⇔ Perceived Effectiveness
P28	SEM		⇔ Temporal Proximity
P29	SEM		⇔ SOST Understanding
P30	SEM		⇔ Age
P31	SEM		⇔ Gender

Table 16. List of tested propositions

6.4 Factors and criteria emerging from the analysis of qualitative data

6.4.1 Qualitative factors

Whilst the statistical analysis of the data proceeding from the questionnaire has produced very interesting and robust results, it cannot provide insights into why and how given correlations exist and what are the arguments used by the citizens in their discursive assessment of SOSTs' acceptability. However, as an inherent part of the citizen summit participatory methodology, table discussions and written postcards and recommendations complemented the data proceeding from the electronic survey. The idea was to produce a moving picture of the complex process of technology assessment by lay participants, opening up a space for their voice to be heard and for their knowledge to be incorporated in both scientific research and policy making practices. Whilst an in-depth analysis of the most valuable information proceeding from these table discussions has been conducted in the single national reports (D6.1 to 6.9), we are presenting here some especially interesting outcomes that help to complement and understand the valuable insights derived by the statistical analysis. This section also takes into account the qualitative findings of the five small-scale citizen meetings (D7.2) organised in five different countries, which supplemented the large-scale research.

Institutional Trustworthiness

The statistical analysis confirms what has been often discussed and suggested by the contextual approaches in public engagement in science, i.e. that trust in the agencies operating a given technology makes the latter more acceptable. However, the qualitative analysis reveals that, in the case of security technologies, important national variations have to be considered. Participants in the Nordic countries, for instance, tend to trust their own national security agencies because they consider that these agencies operate under known and respected rules and that the national regulatory framework provides a sound and reliable set of rules to guide their action. Table discussions also reveal that trustworthiness works in a bi-directional way. If trust in security agencies makes the use of a given SOST more acceptable, *the opposite is also true: the use of a more acceptable SOST (CCTVs or SLT, in this case) helps security agencies to be perceived as more trustworthy.*

Moreover, although all these technologies are considered (more or less) likely to be abused, the absence of information, communication and public scrutiny makes both agencies and technologies less likely to be considered trustworthy, even in the absence of scandals or known abuses. Security agencies that deliver precise information about when, for what purposes and to what extent surveillance technologies are operated would significantly increase their degree of trustworthiness. Finally, especially in Spain and Hungary, the participants pointed out that trustworthiness is a complex concept and that it involves not only the degree of trust citizens may have towards security agencies or their technologies but also the type of socio-political context in which both security agencies and technologies operate. As someone in Hungary suggested, the same type of data, retrieved by the same kind of agencies through the same technology, will be used differently in a totalitarian regime than in a democratic one. In other terms, participants made clear that *the key question is not just how safe is the technology, but also how safe is the political and institutional context in which the technology is implemented.*

Social, Temporal and Spatial Proximity

The literature on risk analysis and public understanding of science on nuclear power plants or similar risky technologies had made clear that proximity to the operational space and time of a new technology makes the latter less likely to be accepted. The famous NIMBY factor (Not In My Back-Yard) has proved a very powerful factor influencing the acceptability of risky technologies, especially in the case of those technologies whose benefits were expected to be for the general public but whose risks

were higher for those who lived and operate close to them. The case of SOSTs, however, was different because some of these technologies at least are meant to provide direct benefits for those who operate them, such as in the case of smartphone location tracking, or for those who live and act under their direct gaze, such as in the case of Smart CCTVs. The statistical analysis, in general, confirmed that SOSTs targeting specific groups or profiles, usually presented as “suspects” or “criminals” are eventually more acceptable than SOSTs (smart CCTVs and SLT) that operate on blanket surveillance (DPI). Whilst confirming this general outcome, the table discussions in the citizen summits show that national exceptions do exist. Due to their specific history, national collective memory of a totalitarian past, participants in Austria and Germany argued with more emphasis than elsewhere that surveillance technologies cannot be considered more acceptable if they only target specific groups. In contrast, regardless of whom these technologies are targeting, the scope of surveillance must always be proved necessary, justified and proportionate. Although not confirmed by the analysis, temporal proximity seems to be discursively common in many citizen summits where a few participants suggested that those SOSTs that are considered to have a greater margin to expand in scope and depth in the future (DPI and SLT) are less acceptable than SOSTs whose aims and scope seems to be more clearly defined (CCTVs).

Perceived Level of Threat

The statistical analysis did not confirm that a more intense perception of security threat would make SOSTs more acceptable. More specifically, two of the three dimensions employed to measure ‘perceived level of threat’, i.e., personal safety and national security have no significant effect on the acceptability of SOSTs, probably because people feel very safe in these countries and because they either do not consider national security as a high priority or because they do not consider that SOSTs are an effective way to improve national security. The remaining dimension, i.e., concerns for online security, does have a positive effect on acceptability, though. In general, thus, the more participants worried about their safety online, the more willing they were to accept SOSTs.

Two more interesting insights proceed from the table discussions. First of all, although it is considered by far the least acceptable technology, the ability of DPI to be used to protect against cyber-crimes provides this SOST with some degree of acceptance if directed at cyber-security. Although they may consider their country safe to different degrees, participants of all countries are seriously concerned about cyber-security and would welcome new security measures specifically targeting cybercrime. Second, it is also interesting to consider that only in Germany and Austria the participants who felt more secure in their daily life and in their country were also less willing to support SOSTs, because their concern to have their privacy eroded increased significantly. The small-scale research examined in a greater depth how citizens assess security. It was found that people interpret security first of all on individual level, as a subjective feeling often expressed by referring to a general absence of fear, worry and concern related to some form of physical, mental or digital attack against them or their loved ones or their property. It is also influenced by existential concerns and social problems. Especially when they are used for untargeted surveillance, SOSTs do not have a direct effect on this subjective feeling of safety. On the contrary, citizens see risks especially in the exaggerated surveillance that endanger often the core of their privacy, which they think should be protected in any case. Moreover, participants in both series of empirical research felt that current levels of security threats do not justify the extensive, untargeted surveillance used for crime prevention (D7.2).

Perceived Intrusiveness

Whilst the statistical analysis has confirmed the validity of perceived intrusiveness in relation to acceptability of SOSTs, it is interesting to consider that the table discussions in all countries, but especially in Norway and Denmark, suggest that SOSTs negatively affecting personal information privacy (DPI) are less acceptable than technologies addressing general privacy (CCTV and SLT). This is perhaps due to the fact that information privacy is considered more intimate than our bodily image in the public space or our movements and localization. The sphere of personal communication, which is considered directly at stake when DPI operates, is perceived as especially sensitive, and so are the data

that can be retrieved through the implementation of surveillance technologies targeting this space and this set of data. This specific factor, along with the lack of transparency and accountability, explains an important part of the higher rejection rate of DPI, compared to other technologies, in all the countries participating.

Perceived Effectiveness

Table discussions in all countries confirmed quite clearly that the effectiveness of a certain SOST is an important factor influencing their acceptability. Clearly, effective technologies, i.e. those that are considered able to attain the objectives they are meant to pursue, enjoy a higher degree of acceptability among participants across the nine European Countries. Whilst this is confirmed by the statistical analysis, the data proceeding from the table discussions suggest that SOSTs increasing personal safety (CCTV and SLT) tend to be more acceptable than SOSTs addressing mostly national security issues.

Substantive Privacy Concerns

With regards to privacy, the statistical analysis suggests that a higher concern for both information and physical privacy makes SOSTs less acceptable. The table discussions across the participating countries confirm the importance of this factor, but they also enrich, as the debates in the Nordic Countries show, our understanding of the relationship between privacy concern and acceptability of SOSTs. Moreover, in several table discussions, the moderators reported a discursive shift from privacy concerns, which were increasingly associated to the old good days but no longer possible to preserve, to data protection concerns, which are mostly articulated in terms of keeping an eye on how security agencies handle our data, and on the quality and precision of these data. This finding was reinforced in the small-scale research when privacy concerns and the question of core of privacy were discussed. A number of citizens regarded personal and contact data a part of their privacy and data protection as an important issue for them (D7.2)

Security-privacy balance and the trade-off Model

In most countries, the majority of participants considered SOSTs as both intrusive and effective, a position that place them in a situation where they could potentially see a trade-off between privacy and security in relation to SOSTs. It is interesting to notice, however, that, considering SOSTs as effective and intrusive does not necessarily lead to a higher willingness to trade privacy and liberty in exchange for more security. In fact, among those who considered SOSTs both as intrusive and effective, not even half were effectively willing to trade more privacy in exchange for increased security. Moreover, as the tables in the following section show, there exist a significant minority, always between 15 and 30 per cent, which consider SOSTs as highly intrusive but hardly effective. This is an interesting result in its own right, for it shows that the dominant framework used to justify security policies and measures negatively affecting citizens' rights and privacy may be largely adopted by the citizens but, first, does not imply more willingness to accept liberty restrictions in the name of enhanced security and, second, it is actively rejected by a quite significant minority. Moreover, table discussions and descriptive statistics suggest that in Germany and Austria, the majority of participants do not think in terms of trade-off as SOSTs are considered as highly intrusive but hardly effective."

This issue was further explored in the small-scale meetings, in which participants were asked to reflect on the trade-off approach. Opinions were strongly divided. Those who accepted the trade-off approach felt that the model is valid, because they thought that surveillance *per se* entails the infringement of privacy. However, even those who embraced the model often thought that safeguards must be put in place for any personal data collected. Others accept sacrificing their privacy in certain circumstances, and accepted surveillance: if it is completed in a transparent manner; when the SOST does not intrude into the core of privacy; in particularly serious situations when human lives are directly endangered; when the SOST is not used for prevention but after the event. They tended to accept surveillance in the short term to solve immediate security problems but regarded that it is the root of the security

problems that should be remedied in the long term solving the societal problems behind a great number of security threats. Others not only insisted on these long-term solutions, but also preferred non-surveillance based alternatives also in the short term. Some others, finally, argued that a society can be secure and at the same time protect citizens' right to privacy, and thought that the development of security technology should take into account both respect for privacy and data protection legislation.

6.4.2 Unexpected emerging factors

The table discussions not only offer valuable information to complement existing knowledge proceeding from the statistical analysis, they also offer interesting insights about the existence of other factors that are likely to affect lay public's acceptability of SOSTs. These factors are briefly described and discussed in this section, and constitute a valuable starting point for future research on the acceptability of surveillance-orientated security technologies as well as of new and emerging technologies in general.

First of all, it seems that there is an impact on acceptability proceeding from the type of crime targeted by the technologies. In general, participants in Spain suggested that when technologies shift attention away from crimes that concern participants (such as financial crimes and corruption) to other crimes that are perceived as less urgent (terrorism) they are considered less acceptable. In other countries like for instance Hungary and Italy, the fear of petty, everyday crime is strong, and people expect from SOSTs to decrease threats related to these types of crimes. The analysis of the data gathered in the small-scale events demonstrated that a great number of participants in all the countries involved in the research, do not feel, or cannot assess national security threats, and consequently often feel that preventive mass surveillance does not improve their personal feeling of security, and does not provide solutions for a significant number of security challenges they face.

Second, whenever technologies are perceived to have a negative impact on atypical, non-conformist behaviours, they tend to be considered as less acceptable. Participants in Germany, and to a certain extent in Italy, expressed concern, for instance, that a massive deployment of SOSTs may have the unwelcome results of discriminating people by their appearances, political or religious world-views or sexual preferences and repressing non-conformist behaviours, which, while they do not represent a threat to society, are a valuable contribution to a richer, more diversified and vibrant society.

Third, the risk of function creep is very relevant when it comes to assess the acceptability of a SOST. Table discussions in Germany, Austria, Hungary and Spain suggest that whenever the risk of function creep is perceived as very high, be it for the technical specificities of the technology or for the context in which these technologies are implemented, the acceptability of such technology is negatively affected.

Fourth, table discussions in Austria, Hungary, Spain and Italy reveal that participants consider the human factor very important and that they do not like to be monitored and interpreted only by mathematical algorithms. If the implementation of SOSTs is considered to rely excessively on mathematical algorithms such as DPI, and/or to produce a loss of the human factor, in the sense of replacing human operators, these SOST are considered less acceptable.

Fifth, the involvement of private, business-oriented, actors and operators in security operations and technologies is a delicate issue when it comes to assess acceptability of SOSTs. In general all participants across countries expressed concerns about the involvement of private actors or about public-private partnerships in security operations. Table discussions in Spain and in Hungary explicitly disclosed that the involvement of private, business-orientated actors in the operation, implementation and storage of data for security purposes reduces acceptability of the technologies involved.

Sixth, the way a technology is designed and the way its framework of implementation operates are also very relevant factors which are likely to affect lay public's acceptability of SOSTs. In general, table discussion in Hungary and Spain suggest that if a security strategy based on SOSTs provides citizens with the possibility to opt out or to exert control over the data retrieved and stored, this is likely to positively affect the acceptability of the SOSTs involved. Also in the small-scale events, the large majority of participants (93 per cent) argued that they should be able to control their own personal data and information collected through the use of SOSTs.

Seventh, it is important to consider that the presence of some direct benefits for technology users increase the acceptability of the SOSTs. This is, for instance, the case of smartphone location tracking, which is used by a variety of apps to provide services of GPS road, or outdoors, navigation and services location, apart from being potentially employed for security purposes by security agencies. The convenience of smartphone location tracking for commercial, leisure or even private safety features makes these SOSTs more acceptable, even in the face of the acknowledged privacy risks.

Finally, the clarity of how a technology works and operates and the clarity of the purposes for which it is operated, also appear to be likely to affect acceptability of SOSTs. Table discussions in UK suggested that the complexity of the way a technology works and operates negatively affect acceptability. Table discussions in Switzerland suggested that when the purpose for which a technology is implemented and operates is clear, acceptability is higher. Technologies and security measures that are considered to have unclear and/or unrestricted purposes, such as DPI and SLT, are, in general, less acceptable than technologies and measures considered to have more clear and delimited purposes.

Are more likely to be considered acceptable, SOSTs which...

- ✓ ...target crimes which are within the citizens' priorities;
- ✓ ...empower citizens and make them feel in control;
- ✓ ...are employed with a clear, delimited purpose in mind.
- ✓ ...provide direct, personal services and benefits to their users

Are less likely to be considered acceptable, SOSTs which...

- × ...promote intolerance and segregation;
- × ...entail high function creep risks;
- × ...undermine the role of humans;
- × ...involve private sector or foreign national security agencies (DPI).

Table 17. New and Emerging factors likely to influence SOSTs' acceptability

6.5 Criteria

In the previous chapters, and especially in chapter four and five, we have made an important distinction between factors and criteria likely to influence acceptability of SOSTs. In this chapter, which addresses the empirical results of the project in relation to this specific issue, we would like to start from this distinction. Whereas **factor** can be defined as something that helps produce or influence a result, or as one of the things that cause something to happen, a criterion is something that is used as a reason for making a judgment or decision or a standard on which a judgment or decision may be based.

This conceptual distinction is not merely theoretical, it has consequences with respect to how we can actually identify and study them. Factors can be assessed through both quantitative and qualitative methods, and the very research design of the citizen summits was developed to allow an in-depth study of factors from both a quantitative and a qualitative point of view. However, the research design was also structured in such a way that the criteria adopted and employed by the participants to assess the acceptability of SOSTs could also be observed and analysed. Criteria, in fact, are elements that are used by people to make decisions or standards on which judgement can be made; they can only emerge in table discussions and articulated debates about controversial issues and topics. Along with the idea of getting a more dynamic and articulated understanding of the factors affecting public acceptability of SOSTs, this is the other main reason leading the consortium SURPRISE to complement a survey-based

methodology with table discussions and recommendations rounds in the citizen summit: criteria can only be assessed through a qualitative analysis of these debates and discussions.

In the following section, these criteria – which are often a conglomerate of different arguments, standards or principles employed by the participants in the discursive dynamics of the table discussions – have been collected and made consistent and stable for a better understanding of under which circumstances participants consider the implementation of SOSTs more acceptable. In case there is not reference to any specific country, it means that the criterion has been explicitly discussed and adopted by participants in all the involved.

6.5.1 Criteria under which SOSTs are more likely to be considered acceptable

1) International legal framework

Also regulatory challenges regarding national and international laws were raised: “It is not clear who is in charge and responsible administrative authority for international surveillance. How is this regulated?” Discussants here identified a need for national actions to limit surveillance but also for international regulations in order to reduce disparity between different countries and impact of SOSTs beyond different legal borders. (Austria National Report p. 33)

“The need for new and international legal frameworks was seen as important, and even more – an oversight body that could intervene if someone broke the law when using deep packet inspection in an illegal way.” (Norway National Report p.23)

Given the transnational, and often global, nature of both security threats and the security strategies and measures implemented to counter these threats, the national fragmentation of legislation and of data protection authorities is perceived as an obstacle to both security strategies and data protection rights and principles. People across countries suggest that an international legislation and oversight regulatory international body, such as a European Data protection authority, would make the implementation of SOSTs more acceptable. A clear, unified and transnationally operating, legal framework, enforced by a single, accountable authority, has often presented as a much-needed condition for the operation of SOSTs.

SOSTs are more acceptable, thus, if operating within a European regulatory framework and under the control of a European regulatory body.

2) Transparency, information and accountability

“In fact, some participants even suggested the creation and implementation of a law of transparency that could regulate in a clear and accessible way the retrieval, storage and use of personal information: “We need a law of transparency, as much as we have a law on data protection” (Spanish national report p. 43).

SOSTs are operated in a situation where information, transparency and responsibility are perceived as lacking or missing. The small-scale meetings not only confirmed this finding but also suggested that those who believe they knew quite a lot about these topics have a superficial and often partially incorrect knowledge (D7.2). The participants consider that a necessary criterion to be adopted when SOSTs are to be introduced is to ensure that detailed and accessible information about operation modes, operators, rules, domains and purposes is provided to the public beforehand. Information campaign are also required in order to increase citizens' knowledge of data protection legislations and about the overall security accountability chain, so that it becomes clear whose responsibility is to be addressed when things go wrong.

SOSTs are more acceptable if operating in a context where transparency about the procedures, information about both data protection rights and principles and about the purposes and the scopes of security actions as well as accountability of security operators is ensured at all times.

3) Public-private separation

Generally speaking, private actors were not considered as acceptable institutions to be entrusted the responsibility of enacting security measures and/or operate security technologies, let alone monitor and control the “controllers”. In contrast, it was explicitly suggested by all the groups that only a public body, independent from political control, should enact these tasks and operation (Spanish National Report p. 49)

Participants are especially worried that profit seeking actors, like industry and business actors, who take advantage of SOSTs to gather data about individuals for marketing purposes or profit generating activities, may share these data to security agencies without their previous knowledge. As a result, they are especially concerned about their rights and privacy when private actors are involved in the implementation and operation of SOSTs. In principle, they suggest that SOSTs’ operation must be confined, whenever possible, to public authorities only. When private actors are involved, the requirements of transparency, information and accountability need to be even stricter in order to avoid function creep, commercial abuses and unauthorized profits.

SOSTs are more acceptable if operated only by public authorities and only for public benefits. The participation of private actors in security operations, such as when security agencies acquire banking data or Facebook data or when security functions are outsourced to private operators, therefore, must be strictly regulated.

4) Cost-effectiveness

*Citizens made clear to want more evaluation (and according information) of purpose, appropriateness, costs, impacts of SOSTs and surveillance practices in accordance with **commensurability**. Some participants mentioned data retention and that surveillance measures are mostly paid by taxpayers respectively the citizens themselves (Austrian National Report, p.33).*

“I have no problems with smart CCTV but the use of it, the running costs, the legitimacy and the effectiveness of it needs to be carefully monitored. And the watchers made accountable. (UK National Report, p. 20)

Participants considered that most of these technologies are developed, implemented and operated by public institutions on public money. They insisted on the need for thorough cost-effectiveness analysis of the prospective SOSTs before they are fully developed and introduced. Different criteria have been suggested to produce such evaluation, for instance, cost-effectiveness compared to the prospected results (UK), or to other technological alternatives or to non-technological ones (Spain, Germany, and Austria).

SOSTs are more acceptable if their benefits largely outweigh their costs, especially in comparison to other non-technological, less intrusive, alternatives.

5) Data control and information

“Active information obligation for data collectors (public and private), means the citizen is not required to make a demand but rather that who collects data should be obliged to inform the concerned person; what is stored, how long and why at all! E.g. also in form of a yearly report of the data collecting entity, where it is publicly declared for which purpose and how much data is collected” (German National Report p.53).

One of the main sources of concerns for participants across the participating countries was the shared feeling of being submitted to surveillance practices without being informed or consulted. They considered that surveillance devices and/or practices should never be imposed on people without their knowledge and, whenever possible, permission. Although they acknowledge that, in some cases, informing citizens about the installation and operation of SOSTs would jeopardize their outcomes, participants made it clear that they would consider SOSTs more acceptable if they were informed about when, where and for what purposes is this SOST being operated. They would, thus, welcome a system of surveillance that, whenever possible, notifies citizens if they are under surveillance and/or in case data about them has been recorded and stored. As a result, participants strongly encouraged the introduction of an opt-in frame, i.e. the possibility to pro-actively choose whether to accept surveillance.

Even when the opt-in frame is not possible, they would especially appreciate to be notified when they are under surveillance and for what purposes.

SOSTs are more acceptable when their operation can be regulated through an opt-in approach. Whenever this is not possible, their operation need to be communicated to targeted individuals.

6) Data access, management and protection

"These concerns surface the need for effective data protection approaches and reinforce the need for citizens to be reassured in this regard, as the following comments from participants show: "The problem I have with CCTV and DPI is who has access to all my information, where is it stored and how long for? Who accounts for it all?" (UK National Report p. 18)

One of the most interesting aspects of the table discussions was that participants did recognise that sometimes the privacy of suspect individuals need to be affected in order to increase security. However, they argued that this is not the case with data protection rights and principles. Participants claimed access to their own stored and recorded data at all times. If it is indeed necessary to retrieve data about individuals, these must not only be notified, they must also be provided with the right to access and modify their data as well as the right to be 'forgotten'. Especially in the Spanish debate, participants not only claimed the possibility to control what is monitored and for what purposes, they also wanted to be able to choose what to keep private and what could be made public.

SOSTs are more acceptable if they allow monitored individuals to access, modify and remove their own data.

7) Nature, scope and context of data retrieved

"At some tables the participants expressed that they found location as less sensitive type of data than for example the content of their communication, which can be accessed through deep packet inspection". Norway national report p. 28

Participants in various countries, but especially in Austria and Germany, suggested that some type of data such as those related to location or bodily appearance are considered less sensitive than other type of data, such as those related to personal communication. They also clarified that data retrieved in public spaces, such as public buildings and streets, are less sensitive than data gathered in more private spaces, such as private houses or common private spaces, like clubs or associations. In general, security actions should always target less sensitive data in less sensitive spaces, whenever possible. In Germany and Austria it could even be detected that participants would prefer measures that prevent mass surveillance, make identification processes more difficult and target only already identified suspects in order to ensure that the general population remains as unaffected as possible by governmental surveillance. Therefore, the nature and context of data retrieval for security purposes emerges as a crucial criterion employed by the participants to decide if and when SOSTs are acceptable. Moreover, the scope of data gathering is also crucial; the participants insisted that access to these data is acceptable only when the selection criteria to decide whom to monitor and for what purposes are explicitly communicated and respected

SOSTs are more acceptable if they target less sensitive data and spaces, whenever possible, according to criteria and purposes known to the public.

8) Nature, scope and purposes of surveillance activities

"In some cases, participants worried about DPI leading to personal information about them being accessible to third party companies which might use it in other ways or for other purposes. In particular, there were also worries about the involvement of profit making businesses in the implementation of security involving SOSTs, with one participant commenting that "No security services should be outsourced to private (profitmaking) companies" (Postcard 54)" (UK National Report).

Along with the previous criterion, the nature, scope and purposes of SOSTs are also a relevant criterion that participants have adopted when discussing the acceptability of the security technologies at stake. In general, all participants agreed that blanket surveillance couldn't be considered acceptable. German participants, for instance, not only considered that the wider the surveillance, the less effective the technology, but also argued that the wider the surveillance, the less trustworthy the institution using SOSTs for this purpose. Clearly, the security priorities addressed by the SOSTs may change according to local sensitivity and priorities: while it should not be used to enhance national security but to increase personal safety in Germany and in Austria, in Hungary and Spain they only make sense (if effective, which is controversial) for national security. Regardless of the main purposes and priorities, though, all participants agreed that surveillance technologies should be deployed only after reasonable evidence is gathered to suggest that surveillance is effectively necessary.

SOSTs are more acceptable if they not operate blanket surveillance. After reasonable evidence is gathered, they should only address specific targets, in specific times and spaces and for specific purposes. Whilst their purposes may change, these changes need to be explicitly discussed and publicly approved.

9) Non-technological alternatives and security measures not based on surveillance

"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". (Hungary National Report p.36)

"A clear estimation of the actual need to use these technologies. Realistic evaluation of the threat situation and of the real risks, and appropriately discreet use of security technologies. Alternatives should be sought and in the security sector greater value should be placed on the human factor (investigating authorities) than on the technology." (Swiss national report, p. 48)

"Italian citizens claimed that alternative security approaches were desirable, especially for crime prevention. Alternative measures were described in very general terms as measures aimed at reducing social inequalities or other root causes of insecurity, and as mechanisms that do not target citizens and their personal data. Suggestions included: i) addressing societal injustice and unease, taking care of the environment, investing in harmonious cohabitation, rather than targeting criminals; ii) protecting critical infrastructure at the source, addressing culturally-sensitive issues, such as tax evasion; iii) investing in neighbourhood patrols, or CCTV cameras [...]. Italian National Report p. 39

Participants in various countries have expressed concern that current security measures based on the implementation of SOSTs are simply targeting and repressing criminals and their activities without addressing the social, cultural and economic causes of crime and terrorism. Moreover, they also acknowledged the importance of non-technological alternatives and the potential role to be played by security measures that are not based on surveillance. They have also appreciated the importance of the human factor in security operations and strategies and considered that security technologies should not replace human operators but rather help and complement them. As a result, they would assess more favourably SOSTs that complement human operators and that work as part of a broader and more complex strategy that is not ultimately repressive but aims at tackling the social and economic sources of crime and deviance. Such strategies, not only should include actions to restore trust in political systems and institutions, they should also shift the focus to address especially social inequalities. The point is not to choose between technology and human operators or between root actions to address poverty and inequality and repressive surveillance technologies. The point, as they frame it, is to combine technology and social action to reduce the factors that encourage crime whilst ensuring an efficient, crime preventing security strategy that respect human rights and privacy.

SOSTs are more acceptable if they work and operate in combination with non-technological measures and social strategies addressing the social and economic causes of insecurity. SOSTs are not alternatives but complementary to human resources and social policies.

10) Privacy-by-Design

“Also, citizens’ request of being in control of the personal data processed by SOSTs seems to support the idea of privacy by design⁴⁵² currently proposed in policy circles.” (Italian National Report p.41)

“The concept of “privacy by design” was mentioned by one participant, and she hoped that future technology developers would use their knowledge to increase privacy, instead of increasing surveillance.” (Norway national report, p.23)

SOSTs should be further developed not only in order to increase their surveillance capacity but also in order to protect privacy to a much greater extent. These developments should include improvements to prevent misuse and false information. Several participants, both in the large-scale and the small-scale events, considered that incorporating technical devices, protocols or options to protect citizens’ privacy in the design might be insufficient to solve all the privacy issues; it was nonetheless a good strategy to tackle at least some of them. They encouraged, therefore, the development of new SOSTs with a Privacy-by-Design protocol.

SOSTs are more acceptable if they incorporate Privacy-by-Design protocols and mechanisms.

⁴⁵² Cavoukian, Ann. 2011. Privacy by Design in Law, Policy and Practice. A White Paper for Regulators, Decision-makers and Policy-makers. Toronto: Information and Privacy Commissioner, Ontario.

7 Conclusion

Over the past ten years, in the face of global terrorism, nuclear proliferation, and transnational organized crime, new approaches to safeguard national and personal security have emerged. In fact, security is a highly contested concept whose definitions change in scope and depth as we write. While during the 1990s the focus was on *human* security, which emphasised the role of integrated, global system of international intervention to complement the effort of so called “failed states” in securing their citizens, since 2011 the war on terrorism has encouraged a re-evaluation of *homeland* security in tackling new global threats. As a result of the spatial and temporal unpredictability of criminal actions and of their global repercussions, a safer society is often pursued through the implementation of security policies that increasingly rely on the deployment of SOST and interconnected data exchange systems in order to transform unknown threats into predictable events. Security threats, thus, have been increasingly framed in such a way that (a) technology makes always sense as a solution, and (b) surveillance is the only and inevitable way to increase security levels. The rise of security in the policy agenda, both in economic and political terms, accompanied by the rapid expansion of the conceptual scope and relevance of security issues, principles and values, are intertwined phenomena that need to be addressed in order to understand the proliferation of surveillance-orientated devices meant to address security problems.

These new approaches to security are characterized by a number of novel principles and characteristics, which no doubt have crucial implications on the relation between security, technology and democracy. The security agenda is expanding, incorporating new social policy domains previously free from the security concerns and rules: migration, organized crime, social integration, environmental management, energy policy and even Internet navigation have become integral parts of security policy. This expansion is not merely to be understood in terms of extension: the incorporation of these policy domains into security policy is also a way of securitizing them, which means removing them from the ordinary political debate and subjecting them to the urgency, the pressure and the rules of security issues. When a social problem becomes an issue of security policy, it is removed from ordinary political debate and ceases to be addressed along traditional democratic means. Expansion and securitization are also subjecting these policy issues to a new approach, which is fundamentally based on threat anticipation and pre-emptive action. Pre-emption implies action before a crime has actually been committed, and yet, according to the European Union Charter of Rights, everyone is innocent not only before he/she commits a crime but actually until the contrary is proved in court. Maybe the risk of terrorist attack being perpetrated may justify a suspension of this basic civil right, but a suspension this remains nonetheless.

This is, in a way, a security paradox that lies at the heart of the new concept of security and is further aggravated by the new emphasis on risk assessment and risk management. The attempt to prevent a security threat from materializing needs the deployment of a powerful and ever-expanding intelligence service being able to gather massive amounts of information in order to assess the risk and manage its possible manifestation. In this perspective, all citizens can be subjected to surveillance and be assigned a security label on the basis of the level of risk they pose to the system. Needless to say, these tasks cannot be performed, at least in the terms in which they have been conceived, without the massive deployment of surveillance-orientated security technologies. A higher emphasis on surveillance technology often implies a lower emphasis on the social and economic determinants of crime and restricts focus only to those aspects of security that can actually be addressed by a technology. Thanks to surveillance studies, we are today aware of social sorting, ethnic discrimination and self-censorship usually associated with SOSTs.

Although this was not an inevitable outcome, these technologies have often introduced surveillance as a routine practice, with the unwelcome result of a significant restriction of individual privacy. With privacy curbed down, all the democratic and civil rights that rely on the preservation of the anonymity, confidentiality and intimacy of human behaviour and actions have been negatively affected. Freedom of expression, press, association, movement and political action cannot be fully enjoyed in the absence of a sufficient level of privacy. Precisely as a result of this gradual shift towards a surveillance society, the

implementation of new surveillance-orientated security technologies has been framed, and proposed to the public, in terms of a trade-off between security and liberty. When adopted, the trade-off always implies a reduction of civil liberties in exchange for (allegedly) more security.

Against this background, the introduction of new technologies to foster security is increasingly perceived as a socially problematic and scientifically uncertain option. In fact, several SOSTs are subjecting ordinary citizens to such a level of monitoring and control that some authors speak of a *surveillance society*. Whilst privacy and liberty are being reduced in the name of security, people are forced to trade their rights in exchange for allegedly more security.

Citizens are often asked to renounce part of their liberty and civil rights in exchange for an increased level of security. Citizens cannot be free, it is often repeated, unless they are safe. Yet, they cannot be safe unless they are free or they would no longer be citizens. This is why it is problematic to keep thinking of liberty and security as in opposition to each other. Security and liberty are not mutually exclusive but rather mutually constitutive. As a consequence, security policies need to be radically reconsidered and this process of reconsideration, as odd as it may seem, needs to start from the very subjects that have been bearing so far the costs and the implications of security policies based on SOSTs, pre-emption and risk assessment: the citizens. There is need to allow them to express their views, which are more complex and sophisticated than what we are used to think. There is need, moreover, to change the questions to involve them in novel ways, as they are, ultimately, the subjects and the sovereign of political actions.

A variety of perceptions and opinions studies have been realized in Europe to understand *to what extent and under what conditions*, European citizens are willing to trade part of their privacy/liberty in exchange for increased security. However, like the security policy approaches from which they stem, most of these perception and opinion studies, have also been inspired by a trade-off approach and, thus, tend to take it for granted. Yet, alternative approaches do exist and are strongly influenced by demographic, institutional and cultural factors, which imply that the acceptance of SOSTs is context-dependent. For instance, if trust in institutions depends on the type of technology in use, trust in technology also depends on citizens' confidence in the institutions using the technology.

Public assessment of privacy and security issues associated with the introduction of new SOSTs not only is more complex than the trade-off assumes, it is also largely affected by a variety of factors, which relate to how these technologies address social priorities and to the social and institutional context of implementation. Therefore, security technologies need to be assessed not only on the basis of technical effectiveness, but also on the basis of how, when, where, and by whom these technologies are going to be implemented. As a consequence, it becomes necessary to explore not only citizens' opinions and knowledge about security, privacy, technology and institutions, but also the actual social, economic and political context in which these technologies, and possible alternatives, are likely to be implemented.

The SurPRISE project aims precisely at casting new light not only on whether citizens do actually employ a trade-off approach to assess the introduction of new security technologies, but also on the main factors behind over-acceptance and over-rejection of SOSTs. The variety of different practices, sensitivities, debates and arguments existing and operating in the European countries increases the complexity of the factors and criteria that are likely to have an impact in the way European citizens frame the acceptability of surveillance-orientated security technologies. On the one hand, it seems difficult, therefore, to identify single universally valid factors capable of explaining the different levels of acceptability that each and very SOST may enjoy in each European country. On the other hand, however, institutional, social and cultural factors emerge as crucial elements in the complex process leading European citizens to decide when, where, for what purposes and to what extent a surveillance-orientated security technology is acceptable. Our results, in many ways, endorse the critiques made by the contextual approaches towards the deficit model in the studies on the public assessment of new technologies and, at the same time, seem to support also the claims of the socio-cultural approaches in risk analysis.

Despite this variety, thus, it has been possible to identify a list of factors and criteria that seem to be relevant in most of the countries under study and relevant to the study of the acceptability of the majority of the technologies at stake. More specifically, the report provides insights about how (a)

individual characteristics (e.g. citizenship status, ethnicity, income, age, education, etc.), (b) elements of the institutional context, (c) social and cultural factors, and (d) the specific features of the technology under study (novelty, intrusiveness, safeness, etc.), affect the probability of considering a security measure acceptable. On the basis of these outcomes, it elaborates a new model of the relations between surveillance, security and privacy.

This model stands out today as the most exhaustive and complex model trying to explain a wide variety of factors potentially affecting the acceptability of surveillance-orientated security technologies (SOSTs). The research design employed in the citizen summits has allowed the SURPRISE project team to collect a sophisticated, robust and extensive dataset on public acceptability of SOSTs, which includes both quantitative and qualitative data. The combined analysis of these data has not only allowed us to obtain very important results in the quest for the factors which determine the acceptability of SOSTs, it has also permitted the identification of the most important criteria the participants in this study adopt to take decisions about the acceptability of SOSTs.

In this final chapter, we would like to summarise these findings and discuss them together in order to highlight the importance of the information provided for policy makers, security operators, security industry and citizens alike. First of all, we would like to emphasise the importance of the factors that have been found to strongly correlate with the acceptability of SOSTs. In line with the results that proceed from both the contextual approaches to public engagement in science and the socio-cultural approach to risk analysis, the outcomes of our study show that **institutional trustworthiness is a key factor** determining the acceptability of SOSTs. This has crucial implications for policy makers, because it shows that, besides what citizens may think or know about security technologies, the degree of trust that security agencies and political institutions enjoy is a crucial element that citizens do take into account when assessing the acceptability of security technologies. According to our results, it is equally important to consider that **the perceived level of threat does not significantly affect the acceptability of SOSTs**. An increased perception of insecurity does not make SOSTs more acceptable, nor citizens more willing to renounce to their privacy and rights. A third, very interesting result is that **social proximity**, a factor that has been developed as part of this study drawing from the already known spatial and temporal proximity, **has a very significant impact on the acceptability of SOSTs**. Security technologies that have no specific target but operate blanket surveillance are considered significantly less acceptable than security technologies carefully focusing on specific targets.

As we expected, also considering the work of Sanquist,⁴⁵³ **both effectiveness and intrusiveness emerge as quite significant in relation to the acceptability of SOSTs**. Technologies that are perceived as effective are more likely to be considered acceptable, and those that are perceived as intrusive are less likely to be perceived as acceptable. Much of the security technology discourse, however, insists that security technologies need to be intrusive to be effective. In our analysis we found out that the relation between effectiveness and intrusiveness, on the one hand, and acceptability, on the other hand, is quite more complex than this. We found out, for instance, that perceived effectiveness of SOSTs seems to positively influence substantive privacy concerns, **which suggests that participants consider more effective the SOSTs that have a low impact on privacy**. Or, to put it differently: the more a technology is considered intrusive, the less it is considered effective. Blanket surveillance, thus, not only is considered unacceptable, it is also considered not effective. This result questions the general idea that SOSTs need to be intrusive to be effective, and, consequently, radically questions the trade-off approach. It also suggests to technology developers that a privacy-friendly design is a crucial element when it comes to assess not only the acceptability of a new security technology but also its effectiveness.

In this study, moreover, we did quantify the amount of citizens effectively seeing SOSTs as privacy infringing and security enhancing at the same time, we found out that, although in many countries the majority of participants may envision a trade-off between security and privacy when SOSTs are implemented, they were not more willing to accept SOSTs or to trade their privacy for more security. Even when participants see a potential trade-off between security and privacy, thus, they remain critical

⁴⁵³ Sanquist, Thomas F, Heidi Mahy, and Frederic Morris. 2008. "An exploratory risk perception study of attitudes toward homeland security systems." *Risk analysis* 28 (4):1125-1133.

of the persistent reduction of civil liberties and privacy, and suggest that this process should be limited or stopped altogether. Consistently with these results, we found out that the trade-off approach does not generally influence acceptability, except in the case of very controversial SOSTs, like DPI, where the participants adopting the trade-off were found slightly more willing to accept DPI. Finally, we suggest in this study that the quantification of the trade-off approach in empirical terms may be used as a way to measure and quantify the actual acceptance of SOSTs. The larger is the number of people who consider SOSTs are effective and not intrusive; the more likely are these SOSTs to be socially accepted and legitimate. It should be the aim of policy makers, security operators and industry actors to develop technologies the score as high as possible in this novel measurement system.

Some more results need to be mentioned here. First of all, a complex scenario surrounding privacy emerges. People are extremely concerned about their online safety and their information privacy (i.e. the dimension we called Reserve), which signal concerns associated to data collection, data errors, unauthorised secondary use of data or data sharing. Concerns associated to physical privacy, in its three dimensions – i.e., Intimacy, Anonymity and Solitude – also play an important role in shaping SOSTs acceptability. Finally, we found out that age is positively correlated with acceptability; a result that radically questions the belief that the digital natives generation, due to their familiarity with ICTs and SOSTs, would be less concerned about privacy.

Some of the most interesting results of this study proceed also from a number of unexpected factors that have emerged from the qualitative analysis and were not measured in the quantitative analysis. Apart from confirming the importance and the validity of combining quantitative and qualitative methods, these unexpected factors help casting lights on neglected issues, and complete the picture, paving the way for future studies on the subject. Factors like the type of crime targeted, the risk of function creep, the clarity of the operational functions of SOST or the personal convenience of the technology emerge as very relevant when citizens assess the acceptability of SOSTs. Moreover, whilst people do not like to be judged or interpreted by mathematical algorithms, they also express concern about SOSTs having a negative impact on atypical, non-conformist behaviours, which they value as positive and necessary in the society. By the same token, while they express concern about public-private partnerships in security operations, citizens clearly suggested that acceptable technologies should primarily address the types of crime they consider a priority, such as crime streets and political corruption and financial crimes.

Last but not least, our study has identified ten criteria, more or less generally shared by the participants in the citizen summits and used to take explicit decision on the acceptability of SOSTs. According to the participants involved, SOSTs are more acceptable when they operate under an international legislative framework, monitored by a data protection authority with sufficient powers at the European level. They are more acceptable, moreover, when operated by transparent, accountable public agencies that inform citizens about their purposes and functions. They are more acceptable if they are cost-effective and allow citizens to access and control the data they retrieve and store. Their acceptability, moreover, increases if SOSTs target the least sensitive data, only in public spaces, whenever possible and are specifically orientated towards suspects and criminal activities. Their use is more tolerated if SOSTs are employed only after significant evidences have been collected and only after judicial authorities grant permission. Finally, SOSTs are more acceptable if they incorporate Privacy-by-Design mechanisms and principles and do not replace human intervention. Rather, to be more acceptable, they need to be employed to complement and support human operations, as part of a broader, socially informed, security strategy that addresses also the social and economic causes of crime and violence by reducing social inequality and economic marginalisation.

8 Bibliography

- Acquisti, A. and J. Grossklags (2007), "What can behavioral economics teach us about privacy?", in Alessandro Acquisti, Sabrina De Capitani di Vimercati (Ed.), *Digital Privacy: Theory, Technologies and Practices*, pp. 363–377. Auerbach Publications (Taylor and Francis Group).
- Acquisti, A., L. John, and G. Loewenstein (2009), "What is privacy worth?", in *Workshop on Information Systems Economics (WISE 2009)*.
- Acquisti, A. (2010) "Background Paper #3: The Economics of Personal Data and the Economics of Privacy", The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines, OECD Conference Centre, available at: <http://www.oecd.org/sti/interneteconomy/46968784.pdf>
- Adams, G., Cornu, C. James, A. and Schmitt, B. (2001) *Between cooperation and competition: the transatlantic defence market*. Western European Union: Institute for Security Studies.
- Akter, S.K., D'Ambra, J. and Ray, P. (2011) "Trustworthiness In health Information Services: An Assessment Of A Hierarchical Model With Mediating And Moderating Effects Using Partial Least Squares", *Journal of the American Society for Information Science and Technology* 62(1): 100-116.
- Alhakami, A.S. and Slovic, P. (1994) A psychological study of the inverse relationship between perceived risk and perceived benefit. *Risk Analysis* 14(6): 1085-96.
- Alkire, S. (2003) "A Conceptual Framework for Human Security," Working Paper CRISE 02 Jul 2009 <http://www.crise.ox.ac.uk/pubs/workingpaper2.pdf>
- Allum, N. et al. (2008) "Science knowledge and attitudes across cultures: a meta-analysis", *Public Understanding of Science* 17: 35-54.
- Altman, I. (1975) *The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding*, Monterey, CA: Brooks/Cole Publishing, p.24.
- Amoore, L. (2006) "Biometric Borders: Governing Mobilities in the War on Terror," *Political Geography* 25(3): 336–51.
- Amoore L. and De Goede, M. (eds.) (2008) *Risk and the War on Terror*. New York: Routledge.
- Anders, J. and Holst, M. (2008) *D 5.8 Synthesis Report - Interview Meetings on Security Technology and Privacy*, PRISE Project
- Andrejevic, M. (2002) "The work of watching one another: Lateral surveillance, risk, and governance," *Surveillance & Society* 2(4).
- Aradau, C., and R. Van Munster. 2007. "Governing terrorism through risk: Taking precautions, (un) knowing the future." *European Journal of International Relations* 13(1):89-115.
- Avgerou, C.; Ganzaroli, A.; Poulymenakou, A. and Reinhard, N. (2009) "Interpreting the Trustworthiness of Government Mediated by Information and Communication Technology: Lessons from Electronic Voting in Brazil" *Information Technology for Development* 15 (2): 133 – 148.
- Axworthy, L. (2001) "Human security and global governance: putting people first," *Global governance* 7:19.
- Baldwin, D.A. (1997) "The concept of security." *Review of International Studies* 23(1): 5-26.
- Barnett, J. et al. (2007): "Belief in public efficacy, trust and attitudes toward modern genetic science," *Risk Analysis* 27 (4): 921-933.
- Barry, A., Osborne, T. and Rose, N. (eds.) (1996) *Foucault and political reason: liberalism, neo-liberalism and rationalities of government*. London: UCL Press.
- Bechmann, G. (1995) "Riesgo y desarrollo científico técnico. Sobre la importancia social de la investigación y valoración del riesgo" *Cuadernos de Sección Ciencias Sociales y Económicas* 2:59-98.
- Beck, U. (1992) *Risk Society: Towards a New Modernity*. London: Sage.
- Beck, U. (2002) "The Terrorist Threat: World Risk Society Revisited" *Theory, Culture and Society* 19(4): 39-55
- Beck, U. (2006) *Cosmopolitan Vision*. Cambridge: Polity Press

- Beck, U. and Lau, C. (2005) "Second Modernity as a research agenda: theoretical and empirical explorations in the meta-change of modern society," *British Journal of Sociology*, 56(4): 525-557.
- Beck U., Bonss, W. and Lau, C. (2003) "The Theory of Reflexive Modernization – Problematic, Hypotheses and Research Programme" *Theory, Culture and Society* 20(2): 1-33
- Bélanger, F., Hiller, J. and Smith, WJ (2002) "Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes", *Journal of Strategic Information Systems*, 11(3/4): 245-270.
- Benner, M., and Löfgren, H. (2007) "The Bio-economy and the Competition State: Transcending the Dichotomy between Coordinated and Liberal Market Economies" *New Political Science* 29(1): 77-95.
- Bennett, C.J. (1995) *The Political Economy of Privacy: A Review of the Literature*, Hackensack, NJ: Center for Social and Legal Research.
- Bennett, Colin J. (2011) "Review of Nissenbaum's Privacy in Context: Policy and the Integrity of Social Life", *Surveillance & Society* 8(4): 541-543.
- Bickerstaff, K.; Simmons, P. Pidgeon, N. (2006) *Public perceptions of risk, science and governance: main findings of a qualitative study of six risk cases*. Understanding risk working paper. Available at www.psych.cf.ac.uk
- Bigo, D. (2000) "Internal and external securitisations in Europe," *International Relations Theory and European Integration: Power, Security and Community*:154.
- Birch, K. (2006) "The neoliberal underpinnings of the bioeconomy: The ideological discourses and practices of economic competitiveness," *Genomics, Society and Policy* 2 (3): 1-15.
- Biscop, S. (2004) *The European security strategy: implementing a distinctive approach to security*: Centre d'etudes de Defense.
- Biscop, S. (2005) *The European Security Strategy: A global agenda for positive power*. Ashgate Publishing Company.
- Boholm, A. (1996) "Risk perception and social anthropology: a critique of cultural theory," *Ethnos* 61(1): 64-84
- Bord, R.J. and O'Connor, R.E. (1992) "Determinants of risk perceptions of a hazardous waste site", *Risk Analysis* 12: 411-416
- Bovet, A. (2012) *Gènes dans la démocratie. Le génie génétique dans l'espace public suisse (1992-2005)*. Lausanne; Éditions Antipodes.
- Bowyer, K.W. (2004) "Face Recognition Technology: Security versus Privacy," *IEEE Technology and Society Magazine* 23(1): 9–19.
- Brehmer, B. (1987) "The Psychology of Risk", in Singleton, W.T. and Howden, J. (eds) *Risk and Decisions*, New York: Wiley. pp.25–39,
- Bronfman, N. C. and Vázquez, E.L. (2011). "A Cross-Cultural Study of Perceived Benefit Versus Risk as Mediators in the Trust-Acceptance Relationship", *Risk Analysis: An International Journal* 31(12): 1919-1934.
- Brooks, D.J. (2009). "What is security: Definition through knowledge categorization." *Security Journal* 23(3): 225-39.
- Brown, J.L. and Ping, Y. (2003) "Consumer perception of risk associated with eating genetically engineered soybeans is less in the presence of a perceived consumer benefit," *Journal of the American Dietetic Association* 103(2): 208-214.
- Burchell, G., Gordon, C. and Miller, P. (eds) (1991) *The Foucault Effect: Studies in Governmentality*. Chicago: University of Chicago Press
- Burkard Schmitt et al. (2004) "Research for a Secure Europe " Luxembourg: Office for Official Publications of the European Communities, p. 12.
- Burningham, K. and Thrush, D. (2004) "Pollution concerns in context: a comparison of local perception of risks associated with living close to a road and a chemical factory", *Journal of Risk Research* 7: 213-232.

- Burns, T. W., O'Connor, D.J. and Stocklmayer, S.M. (2003) "Science Communication: A Contemporary Definition," *Public Understanding of Science* 12: 183-202.
- Buzan, B. (1984) "Peace, power, and security: contending concepts in the study of International Relations," *Journal of Peace Research* 21(2):109-25.
- Buzan, B. (1991) *People, states and fear: An agenda for international security studies in the post-cold war era*. Boulder, Colorado: Rienner.
- Buzan, B., Wæver, O. and de Wilde, J. (1998) *Security: a new framework for analysis*. Boulder: Lynne Rienner.
- Campesi, G. (2009) *Genealogia della pubblica sicurezza. Teoria e storia del moderno dispositivo poliziesco*. Verona: Ombre Corte.
- Callon, M. et al. (2009) *Acting in an Uncertain World. An Essay on Technical Democracy*, Cambridge, Carnevale, D. G. (1995) *Trustworthy Government : Leadership and Management Strategies for Building Trust and High Performance* (1st ed.), San Francisco: Jossey-Bass Publishers, p. 11.
- Carolan, M. (2006) "Science, expertise and democratization of decision-making process," *Society and Nature Resources*, 19: 661-668.
- Chellappa, R. K. and Sin, R. G. (2005) "Personalization Versus Privacy: An Empirical Examination of the Online Consumer's Dilemma," *Information Technology and Management* (6):181-202.
- Clarke, R. (1988) "Information technology and dataveillance" *Communications of the ACM* 31(5): 498-512
- Coker, C. (2002) *Globalization and Insecurity in the Twenty-First Century: NATO and the Management of Risks*. Oxford: Oxford University Press.
- Coker, C. (2004) "NATO and the unbearable lightness of being," *RUSI Journal* 149(3):18-23
- Connor, M. and Siegrist M. (2010) "Factors Influencing People's Acceptance of Gene Technology: The Role of Knowledge, Health Expectations, Naturalness, and Social Trust", *Science Communication* 32: 514-538.
- Cook, K. S., Hardin, R. and Levi, M. (2005) *Co-operation Without Trust?* New York: Russell Sage Foundation.
- Cooper, M. (2008) "The inequality of security: Winners and losers in the risk society," *Human Relations* 61(9): 1229-1258
- Côté-Boucher, K. (2008) "The Diffuse Border: Intelligence-Sharing, Control and Confinement along Canada's Smart Border," *Surveillance and Society* 5(2): 142-65.
- Council of Europe (1950) "Convention for the Protection of Human Rights and Fundamental Freedoms - as amended by Protocols No. 11 and No. 14",
- Council of the European Union "Report on the implementation of the European Security Strategy – Providing Security in a Changing World", CAB66, 17/04/2008.
- Council of the European Union "Draft Internal Security Strategy for the European Union: Towards a European Security Model" (Brussels, DG H, 7120/10), p. 20.
- Cousens, E.M., Kumar, C. and Wermester, K. (2001) *Peacebuilding as politics: cultivating peace in fragile societies*: Lynne Rienner Pub.
- Covello, V. T. (1983) "The perception of technological risks: a literature review," *Technological Forecasting and Social Change* 23: 285-297
- Cowan, R. and Foray, D. (1995) "Quandaries in the economics of dual technologies and spillovers from military to civilian research and development," *Research Policy* 24(6): 851-68.
- Critchley, C. R. (2008): "Public opinion and trust in scientists: the role of the research context, and the perceived motivation of stem cell researchers," *Public Understanding of Science* 17: 309-327.
- CSC Leading Edge Forum (2011) "Data rEvolution Report".
- Cvetkovich, G. and Löfstedt, R (eds) (1999) *Social trust and the management of risk*. London:Earthscan.
- Cvetkovich, G. (1999) "The attribution of Social Trust" in Cvetkovich, G. and Löfstedt, R. (eds) *Social Trust and Management of Risk* London: Earthscan.

- Davis, D.W. and Silver, B.D. (2004) "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America," *American Journal of Political Science* 48(1): 28–46.
- Davies, S. (1997) "Re-engineering the right to privacy : how privacy has been transformed from a right to a commodity", in Agre and Rotenberg (ed) *Technology and Privacy : the new landscape*, MIT Press,
- Dawson, K. and Ziv, D. (2012) "A Conversation On The Role Of Big Data In Marketing And Customer Service", in MediaPost Blogs: CRM, on the 25th of April 2012
- Degli Esposti, Sara (2014) "A Roadmap for developing acceptable surveillance-based security measures". Proceedings of the 9TH Security Research conference »FUTURE SECURITY«, organised by the Institutes of Fraunhofer Group for Defense and Security VVS in Berlin, September 16–18, 2014, pp. 71-80.
- De Goede, M. (2012) "The SWIFT affair and the global politics of European security" *JCMS: Journal of Common Market Studies*.
- De Marchi, B. (2003) "Public Participation and risk governance," *Science and Public Policy* 30: 171-176.
- Dean, M. (1999) *Governmentality: Power and Rule in Modern Society*. London: Sage
- Dietz, T., Scott Frey, R. and Rosa, E. (1996) "Risk, Technology, and Society".in *Handbook of Environmental Sociology*. Westport, Greenwood Press.
- Doty, R. M., Peterson, B. E. and Winter, D.G. (1991) "Threat and authoritarianism in the United States, 1978-1987," *Journal of Personality and Social Psychology* 61(4): 629.
- Douglas, M. (1966) *Purity and Danger, An Analysis of Conceptions of Pollution and Taboo*. London:Routledge.
- Douglas, M. (1970) *Natural Symbols, Explorations in Cosmology*. London: Penguin.
- Douglas, M. (1985) *Risk Acceptability According to the Social Sciences*. New York: Russel Sage Fondation
- Douglas, M. (1992) *Risk and Blame: Essays in Cultural Theory*. London: Routledge
- Douglas, M. and Wildavsky, A. B. (1982). *Risk and Culture: An essay on the selection of technical and environmental dangers*. Berkeley: University of California Press.
- Dourish, P. and Anderson, K. (2006) "Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena," *Human–Computer Interaction* 21(3): 319–42.
- Duffield, M. and Waddell, N. (2006) "Securing Humans in a Dangerous World," *International Politics*, 43(1): 1-23.
- Durant, R. F. and Legge J. S. (2005) "Public Opinion, Risk Perceptions, and Genetically Modified Food Regulatory Policy" *European Union Politics* 6(2):181-200
- Earle, T.C. and Cvetkovich, G.T. (1995) *Social Trust: Toward a Cosmopolitan Society*. Westport, CT: Praeger
- Eastlick, M. A., Lotz, S. L. and Warrington, P. (2006) "Understanding Online B-to-C Relationships: An Integrated Model of Privacy Concerns, Trust, and Commitment," *Journal of Business Research* 59(8): 877-886
- Englewood Cliffs: Prentice Hall. Smith, V.K. (1986) "A Conceptual Overview of the Foundations of Benefit-Cost Analysis", in Bentkover, J.D. Covello, V.T. and Mumpower, J. (eds) *Benefits Assessment: The State of the Art*, Dordrecht: Reidel. pp. 13–34.
- Eriksson, J. and G. Giacomello, G. (2006) "The information revolution, security, and international relations: (IR) relevant theory?" *International political science review* 27(3): 221-44.
- Eriksson, J. and Rhinard, M. (2009) "The Internal-External Security Nexus Notes on an Emerging Research Agenda," *Cooperation and Conflict* 44(3): 243-67.
- European Commission (1996) "The challenges facing the European Defense-Industry, A contribution for Action at European Level", Brussels: COM(96), 10 1996.
- European Commission (1997) "Implementing a European Union Strategy on Defence-related Industry", Brussels: COM(97), 583, 1997
- European Commission "Communication on Conflict Prevention" Brussels: COM (2001), 211, 2001.

- European Commission (2003) "Toward an EU Defence Equipment Policy", Brussels: COM(2003), 113, 2003.
- European Commission (2003) "A Secure Europe in a Better World – European Security Strategy", Brussels: COM (2003).
- European Commission (2004): "Research for a secure Europe: Report of the Group of Personalities in the Field of Security Research," Luxembourg Office for Official Publication of the European Communities.
- European Commission (2007) *Public engagement in science*. European Research Area.
- European Commission "Action Plan for an innovative and competitive Security Industry" COM (2012) 417 final
- European Commission (2007) *Specific Program on 'Prevention, Preparedness and Consequence Management of Terrorism and other Security related risks'*. Brussels 12 February 2007, Doc. 2007/124/EC.
- Evans, G. and Durant, J. (1995) "The relationship between knowledge and attitudes in the public understanding of science in Britain," *Public Understanding of Science* 4(1): 57-74.
- Evans, R., Kotchetkova, I. and Susanne, L. (2009) "Just around the Corner: Rethorics of Progress and Promise in Genetic Research", *Public Understanding of Science* 18(1):43-59.
- Felt, U., and Wynne, B. (2007) "Taking European knowledge society seriously," *Luxembourg: DG for Research. EUR 22*: 700.
- Ferraro, K. A. (1996) "Women's fear of victimization: Shadow of sexual assault?" *Social Forces*, 75: 667–690.
- Ferretti, M.P. and Pavone, V. (2009): "What do civil society organisations expect from participation in science? Lessons from Germany and Spain on the issue of GMOs" *Science and Public Policy* 36(4).
- Festinger, L. (1957) *A Theory of Cognitive Dissonance*. Stanford: Stanford University Press.
- Fischhoff, B. (1995) "Risk perception and communication unplugged: twenty years of process,," *Risk Analysis* 15(2): 137-145.
- Fischhoff, G., Goitein, B. and Shapiro, Z. (1982) "The Experienced Utility of Expected Utility Approaches", in Feather, N.T. ed. *Expectations and Actions: Expectancy-Value Models in Psychology*, Hillsdale: Lawrence Erlbaum. p. 315–40,
- Fischhoff, B., Lichtenstein, S., Slovic, P., Derby, S. L. and Keeney, R. L. (1981) *Acceptable Risk*. Cambridge: Cambridge University Press
- Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S. and Combs, B. (1978). "How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits," *Policy Sciences* 9: 127-152.
- Flynn, J., Burns, W. Mertz, C.M. Slovic, P. (1992) "Trust as a Determinant of Opposition to a High-level Radioactive Waste Repository: Analysis of a Structural Model" *Risk Analysis* 12: 417-429.
- Flynn, J., Slovic, P. Mertz, C.M. (1994) "Gender, Race, and Perception of Environmental Health Risks" *Risk Analysis* 14: 1101-1108
- Foucault, M. (1991) "Governmentality," in G. Burchell, C. Gordon and P. Miller (eds.), *The Foucault Effect: Studies in Governmentality*. London: Harvester Wheatsheaf. pp. 87-104.
- Freudenburg, W. R. (1989) "Perceived risk, real risk: social science and the art of probabilistic risk assessment," *Science* 242: 9-44
- Freunderberg, W.R: (1993) "Risk and Recreancy: Weber, the Division of Labor, and the Rationality of Risk Perceptions", *Social Forces* 71: 909-932
- Frewer L.J, Howard, C. Hedderley, D. Shepherd, R (1996) "What determines trust and information about Food-Related Risk? Underlying Psychological Constructs," *Risk Analysis* 16: 473-486.
- Frewer L.J., Howard, C. and Shepherd, R. (1997). "Public concerns in the United Kingdom about General and Specific Applications of Genetic Engineering: Risk, Benefit and Ethics," *Science, Technology and Human Values* 22(8).

- Friedewald, M. and Bellanova, R. (2012) *Deliverable 1.1. Smart Surveillance – State of the Art*. SAPIENT Project. Available in www.sapientproject.eu.
- Fritzsche, A. (1986) *Wie sicher leben wir?* Köln;
- Frost, M. (1996) *Ethics in international relations: a constitutive theory*: Cambridge University Press.
- Fukuyama, F. (1989) "The end of history." *Globalization and the Challenges of a New Century*:161-80.
- Gad, C. and Lauritsen, P. (2009) "Situated surveillance: an ethnographic study of fisheries inspection in Denmark". *Science & Society*, 7(1): 49-57.
- Gallie, W.B. (1955) "Essentially contested concepts." Pp. 167-98 in *Proceedings of the aristotelian society*: JSTOR.
- Gallup (2002) *Terrorism in the United States*, Poll Topics and Trends
- Gaskell, G., Allum, N., Wagner, W., Kronberger, N., Torgersen, H., Hampel, J. and Bardes, J. (2004) "GM Foods and the Misperception of Risk Perception," *Risk Analysis* 24(1): 185–94
- Gaskell, G., Eyck, T. et al. (2005) "Imagining nanotechnology: cultural support for technological innovation in Europe and the United States," *Public Understanding of Science* 14: 81-90.
- Gaspar, D. (2005) "Securing humanity: Situating 'human security' as concept and discourse," *Journal of Human Development* 6(2): 221-45
- Gottweiss, H. (2002) "Gene therapy and the public: a matter of trust," *Gene Therapy* 9(11): 667-669.
- Goven, J. (2006) "Processes of Inclusion, Cultures of Calculation, Structures of Power". *Science, Technology and Human Values* 3(5): 565-599.
- Gross, A. G. (1994): "The roles of rhetoric in the public understanding of science", *Public Understanding of Science* 3 (1): 3-23.
- Haggerty, K.D. (2010) *Surveillance and democracy*. Cavendish Pub Limited
- Haggerty, K.D. and Ericson, R.V. (2000) "The Surveillant Assemblage" *British Journal of Sociology* 51(4): 605-622.
- Halpern-Felsher, B. L., & Millstein, S. G. (2002) "The effects of terrorism on teens' perceptions of dying: the new world is riskier than ever", *Journal of Adolescent Health*, 30, 308-311.
- Haq, M. (1995) *Reflections on human development*: USA: Oxford University Press.
- Harbor, B. (1990) "Arms conversion and military-civilian technological synergy," *Science and Public Policy* 17(3): 194-200.
- Hardin, R. (2002) *Trust and Trustworthiness* New York: Russell Sage Foundation, p.135.
- Hayes, B., Rowlands, M. and Buxton, N. (2009) *Neoconopticon: The EU security-industrial complex*. Transnational Institute.
- Hazard B. and Seidel G. (1993) "Informationsbedingte und psychosoziale Ursachen für die Angst vor Gesundheitsschäden durch Radon" in: Auran K., Hazard B and Tretter F. (eds.) *Umweltbelastungen und Ökologie*. Opladen: Westdeutscher Verlag, pp. 113-132.
- Heng, Y. (2006) "The 'Transformation of War' Debate through the Looking Glass of Ulrich Beck's World Risk Society" *International Relations* 20(1): 69-91.
- Hoban, T., Woodrum, E. and Czaja, R.(1999) "Public opposition to genetic engineering" *Rural Sociology* 57: 476-493
- Hoos, I. (1980) "Risk Assessment in Social Perspective" in *Perceptions of Risk*. Measurements. Washington, DC: NCRP
- Huddy, L., Feldman, S., Capelos, T. and Provost, C. (2002) "The consequences of Terrorism: Disentangling the effects of personal and national threat." *Political Psychology* 23(3): 485-509.
- Hunter, S. and Leyden, K., (1995) "NIMBY: Explaining opposition to hazardous waste facilities," *Police Studies. Journal* 23 (4), 601–619.
- Irwin A, Simmons P and Walker G (1999) "Faulty environments and risk reasoning: the local understanding of industrial hazards", *Environment and Planning* 31: 1311-1326.

- Jackson, N.J. (2006) "International organizations, security dichotomies and the trafficking of persons and narcotics in post-Soviet Central Asia: a critique of the securitization framework." *Security Dialogue* 37(3): 299-317.
- Jain A. K., Ross, A. and Uludag, U. (2005) "Biometric Template Security: Challenges and Solutions" available at <http://biometrics.cse.msu.edu>, last accessed June 2008.
- Jasanoff, S (2003) "Technology of humility: citizen participation in governing science," *Minerva* 41:223–24.
- Jasanoff, S. (2004) *States of Knowledge: The Co-Production of Science and the Social Order*. London: Routledge.
- Jasanoff, S. (2005) *Designs on nature: Science and Democracy in Europe and the United States*. Princeton, NJ: Princeton University Press.
- Jeanne M. Hauch (1994), "Protecting Private Facts in France: The Warren & Brandeis Tort is Alive and Well and Flourishing in Paris", 68 *Tulane Law Review* 1219 (May).
- Johnson, E. J., and Tversky, A. (1983) "Affect, generalization and the perception of risk," *Journal of Personality and Social Psychology* 45: 20–31.
- Joss, S. and Bellucci, S. (eds) (2002) *Participatory Technology Assessment. European perspectives*. London: Centre for the Study of Democracy,
- Just, R.E., Health, D.L. and Schmitz, A. (1982) *Applied Welfare Economics and Public Policy*, Englewood Cliffs: Prentice Hall.
- Kahneman, D. and Tversky, A. (1974) "Judgment under uncertainty. Heuristics and biases", *Science* 185: 1124–31.
- Kahneman, D. and Tversky, A. (1979) "Prospect theory: an analysis of decision under risk," *Econometrica* 47(2): 263-91.
- Kasperson, R. E., Renn, O., Slovic, P., Brown, H.S., Emel, J., Goble, R., Kasperson, J.X. and Ratick, S. (1988) "The social amplification of risk: a conceptual framework," *Risk Analysis* 8 (2): 177-187
- Katz, C. L., Pellegrino, L., Pandey, A., Ng, A., and DeLisi, L. E. (2002) "Research on psychiatric outcomes and interventions subsequent to disasters: a review of the literature", *Psychiatry Research*, 110, 201-217.
- Kaul, I. (1994) "Human Development Report 1994," *American Journal of Economics and Sociology* 54(1):56-565. UI
- Kessler, O. and Daase, C. (2008) "From Insecurity to Uncertainty: Risk and the Paradox of Security Politics" *Alternatives: Global, Local, Political* (April/June).
- King, G. and Murray, C.J.L. (2001) "Rethinking human security." *Political Science Quarterly*: 585-610.
- Knights, D., Noble, F., Vurdubakis, T. and Willmott, H. (2001) "Chasing Shadows: Control, Virtuality and the Production of Trust," *Organization Studies* 22(2): 311–36.
- Knudsen, O.F. (2001) "Post-Copenhagen security studies: desecuritizing securitization," *Security Dialogue* 32(3): 355-68.
- Kolluru, R. V. and Broks., D.G. (1995) "Integrated Risk Assessment and Strategic Management" in *Risk Assessment and Management Handbook. For Environmental, Health, and Safety Professionals*. New York: McGraw-Hill.
- Kronberger, N., Holtz, P. and Wolfgang Wagner, W (2012) "Consequences of media information uptake and deliberation: focus groups, symbolic coping with synthetic biology." *Public Understanding of Science* 21(2):174-87.
- Kurath, M. and Gisler, P. (2009) "Informing, involving or engaging: Science communication in the ages of atom, bio- and nanotechnology", *Public Understanding of Science* 18 (5): 559- 573.
- Lauritsen, P. (2011) *Big Brother 2.0*. Information Forlag
- Leaning, J. and Arie, S. (2000) *Human security: a framework for assessment in conflict and transition*. Washington: United States Agency for International Development/Complex Emergency Response and Transition Initiative.

- Lee, J.K., and Rao, H.R. (2007) "Perceived risks, counter-beliefs, and intentions to use anti-/counter-terrorism websites: An exploratory study of government-citizens online interactions in a turbulent environment," *Decision Support Systems* 43(4): 1431-49.
- Leonard W. Labaree, ed. (1963) *The Papers of Benjamin Franklin*, v. 6, p. 242
- Levidow, L. and Marris, C. (2001) "Science and Governance in Europe: lessons from the case of agbiotech," *Science and Public Policy* 28(5): 345-60.
- Levi, M. and Wall, D. (2004) "Technologies, Security, and Privacy in the Post 9/11 European Information Society." *Journal of Law and Society* 31(2): 194-220
- Liberatore, A. (2007) "Balancing security and democracy, and the role of expertise: Biometrics politics in the European Union" *European Journal of Criminal Policy* 13: 109-137.
- Lichtenstein, S., Slovic, P., Fischhoff, B., Layman, M., and Combs, B. (1978). Judged frequency of lethal events. *Journal of Experimental Psychology: Human Learning and Memory* 4: 551-578.
- Lodge, J. (2005) "e-Justice, Security and Biometrics: The EU's Proximity Paradox," *European Journal of Crime, Criminal Law and Criminal Justice* 13(4): 533-64
- Lodge, J. (2007) "Freedom, Security and Justice: The Thin End of the Wedge for Biometrics?" *Annali Istituto Superiore Sanità* 43(1): 20-6.
- Lopes, L. L. (1983) "Some thoughts on the psychological concept of risk," *Journal of Experimental Psychology: Human Perception and Performance* 9: 137-144
- Lowrance, W. W. (1976) *Of Acceptable Risk: Science and the Determination of Safety*. Los Altos: William Kaufman;
- Luce, R. D. and Weber. (1986) "An axiomatic theory of conjoint, expected risk," *Journal of Mathematical Psychology* 30: 188-205.
- Luhmann, N. (1989) *Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität* Enke, Stuttgart
- Lupton, D. (1999) *Risk*. London: Routledge
- Lutterbeck, D. (2005) "Blurring the dividing line: The convergence of internal and external security in Western Europe," *European Security* 14(2): 231-53.
- Lyon, D. (2002). *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London and New York: Routledge
- Lyon, D. ed. (2006) *Theorizing Surveillance: the Panopticon and Beyond*. Cullompton, Devon (UK): Willan Publishing.
- Lyon, D. (2007) "Surveillance Security and Social Sorting: Emerging Research Priorities," *International Criminal Justice Review* 17(3): 161-70
- Maki, K. (2011) "Neoliberal Deviants and Surveillance: Welfare Recipients under the watchful eye of Ontario Works," *Surveillance & Society*, 9(1/2): 47-63.
- Malhotra, N. K., Kim, S. S. and Agarwal, J. (2004) "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model," *Information Systems Research* 15(4): 336-355.
- Manners, I. (2002) "European [security] Union: from existential threat to ontological security." *Roskilde University Publications*.
- Manners, I. (2006) "Normative Power Europe Reconsidered: Beyond the Crossroads," *Journal of European Public Policy* 13(2): 182-99.
- Margulis, S.T. (1977) "Conceptions of privacy: Current status and next steps", *Journal of Social Issues*, 33 (3): 5-21, p. 10.
- Margulis, S.T. (2003). "On the Status and Contribution of Westin's and Altman's Theories of Privacy" *Journal of Social Issues* 59(2): 411-429.
- Marshall, NJ (1974) "Dimensions of privacy preferences", *Multivariate Behavior Research*, 9(3), 255-272.
- Marshall, R.D., Bryant, R.A., Amsel, L, Suh, E.J., Cook, J.M. and Neria, Y. (2007) "The psychology of ongoing threat relative risk appraisal, the September 11 attacks, and terrorism-related fears." *American Psychologist; American Psychologist* 62(4):304.

- Matheny, A. and Williams, B. (1985) "Knowledge vs NIMBY: Assessing Florida's Strategy for Siting Hazardous Waste Disposal Facilities", *Policy Studies. Journal*. 14 (1), 70–80.
- Mayer, R. C., Davis, J. H. and Schoorman, F. D. (1995) "An Integrative Model of Organizational Trust" *Academy of Management Review*, 20: 709-734.
- Mazur, A. (1987). "Does public perception of risk explain the social response to potential hazard?" *Quarterly Journal of Ideology* 11: 5-41
- McCahill, M. (2012) Surveillance, Crime and the Media in Ball, K, Haggerty, K. and Lyon, D. (eds.) *The Routledge Handbook of surveillance Studies*. London: Routledge.
- McKinsey Global Institute (2011) "Big data: The next frontier for innovation, competition, and productivity", by James Manyika, Michael Chui, Brad Brown, Jacques Bughin, Richard Dobbs, Charles Roxburgh, Angela Hung Byers, published in May 2011
- Michael, James (1994) *Privacy and Human Rights*, UNESCO
- Milberg, S. J., Smith, H. J., and Burke, S. J. (2000) "Information Privacy: Corporate Management and National Regulation," *Organization Science* (11:1), pp. 35-57.
- Miller, S. (2001) "Public understanding of science at the crossroads", *Public Understanding of Science* 10:115-120
- Moffatt S, Bush J, Dunn C, Howel D, and Prince H (1999) Public awareness of air quality and respiratory health and the impact of health advice. Newcastle: University of Newcastle.
- Moffatt S, Hoeldke B, Pless-Mulloli T (2004) "Local environmental concerns among communities in North-East England and South Hessen Germany: the influence of proximity to industry", *Journal of Risk Research* 6: 125-144
- Monahan, T., ed. (2006) *Surveillance and Security: Technological Politics and Power in Everyday Life*. New York: Routledge.
- Morgenthau, H.J. (1993) *op.cit.* Waltz, K.N. (1979) *Theory of international politics*. New York: McGraw-Hill.
- Muller, B.J. (2008) "Securing the Political Imagination: Popular Culture, the Security Dispositif and the Biometric State," *Security Dialogue* 39(2–3): 199–220.
- Mythen, G. (2004) *Ulrich Beck: A Critical Introduction to the Risk Society*. London: Pluto Press
- Mythen, G. and Walklate, S. (2006) *Beyond the 'Risk Society': Critical Reflections on Risk and Human Security*. London: McGraw-Hill.
- NATO (1999) "The Transformation of the Alliance" in *Strategic Concept*, pp. 33-58.
- Nesserini, F. and Bucchi, M. (2011) "Which indicators for the new public engagement activities? An exploratory study of European research institutions," *Public Understanding of Science* 20(1): 64-79.
- Niehoff, B. P., and Moorman, R. H. (1993) "Justice as a Mediator of the Relationship between Methods of Monitoring and Organizational Citizenship Behavior" *Academy of Management Journal*, 36: 527-556.
- Nissenbaum, H. (2004) "Privacy as Contextual Integrity," *Washington Law Review* 79,(February): 119-158.
- Nissenbaum, H. (2010) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Palo Alto, CA: Stanford University Press, p. 127.
- Nowotny, H. (2003) "Dilemma of expertise" *Science and Public Policy* 30(3): 151-156.
- Nowotny, H., Scott, P. and Gibbons, M. (2003) "Introduction; Mode 2 Revisited: The New Production of Knowledge" *Minerva* 41(3): 179-194.
- OECD (2004) "The Security Economy", Paris: OECD Press
- O'Malley, P. (2004) *Risk, Uncertainty and Government*. London: Glasshouse Press.
- O'Malley, P. (2009) Governmentality and Risk, in J. Zinn ed., "Social Theories of risk and uncertainty", working paper, available at <http://www.papers.ssrn.com>
- Paris, R. (2001) "Human security: paradigm shift or hot air?" *International Security* 26(2): 87-102
- Pavlou, P. A., Liang, H. and Xue, Y. (2007) "Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective," *MIS Quarterly* 31(1): 105-136

- Pavone, V. (2007) "From intergovernmental to global: UNESCO, as response to globalization," *The Review of International Organizations* 2(1):77-95
- Pavone, V., Osuna, C. and Degli Esposti, S. (2010) "Invertir en ciencia y tecnología en tiempos de austeridad económica: ¿Qué opinan los ciudadanos?", *Percepción Social de la Ciencia y la Tecnología 2010*, FECYT, available at: <http://www.fecyt.es/fecyt/detalle.do?elegidaSiguiente=&elegidaNivel3=;SalaPrensa;publicaciones;estudiosinformes&elegidaNivel2=;SalaPrensa;publicaciones&elegidaNivel1=;SalaPrensa&tc=publicaciones&id=PSC2010>
- Pavone, V., Goven, J. and Guarino, R. (2011) "From risk assessment to in-context trajectory evaluation-GMOs and their social implications," *Environmental Sciences Europe* 23(1):3-13.
- Pavone, V. and S. Degli Esposti (2012) "Public assessment of new surveillance-orientated security technologies: Beyond the trade-off between privacy and security " *Public Understanding of Science* 21(July): 556-572.
- Peck, J. and Tickell, A. (2002) "Neoliberalizing Space," *Antipode* 34(3).
- Pedersen, D.M. (1997) "Psychological Functions of Privacy" *Journal of Environmental Psychology* 17(2): 147-156
- Pedersen, D.M. (1999) "Model for types of privacy by privacy functions", *Journal of Environmental Psychology* 19(4): 397-405
- Perrow, C. (1984). *Normal Accidents: Living with High Risk Technologies*. New York: Basic Books. Short, J.F. and Clarke, L. (1992) "Social Organization and Risk", in Short, J.F. and Clarke, L. (eds) *Organizations, Uncertainties, and Risk*, Boulder: Westview. pp. 309–21.
- Pidgeon, N. F., Lorenzoni I., and Poortinga W. (2008): "Climate change or nuclear power-No thanks! A quantitative study of public perceptions and risk framing in Britain", *Global Environmental Change* 18: 69-85.
- Plough, A. and Krinsky, S. (1987) "The Emergence of Risk Communication Studies: Social and Political Context," *Science, Technology, and Human Values* 12(3 and 4): 4-10.
- Pol, E., Moreno, E., Guàrdia, J. and Iñiguez, L., (2002) Identity, quality of life and sustainability in an urban suburb of Barcelona: adjustment to City-Identity- Sustainability network structural model. *Environmental Behaviour*. 34 (1), 67–80.
- Pol, E., Di Masso, A. Castrechini, A. Bonet, M.R. and Vidal, T. (2006) "Psychological parameters to understand and manage the NIMBY effect", *Revue Européenne de Psychologie Appliquée* 56: 43-51.
- Porcedda, M.G., M. Vermeulen et al. (2013). Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy. Deliverable 3.2, SurPRISE Project. Florence, European University Institute.
- Posner, R. A. (1978) "The right of privacy", *Georgia Law Review* 12(3): 393–422. Posner, R. A. (1981, May) "The economics of privacy", *The American Economic Review* 71(2): 405–409.
- Qin, W. and Brown, J.L. (2008) "Factors explaining male/female differences in attitudes and purchase intention toward genetically engineered salmon," *Journal of Consumer Behaviour* 7(2): 127-45.
- Rachel, L. Finn, Wright, D. and Friedewald, M. (2013) "Seven Types of Privacy" in Gutwirth, S.; Leenes, R.; de Hert, P.; Pouillet, Y. (eds.) *European Data Protection: Coming of Age*, Chapter 1, Dordrecht: Springer. DOI 10.1007/978-94-007-5170-5_1
- Rasmussen, M.V. (2001) "Reflexive Security: NATO and International Risk Society," *Millennium: Journal of International Studies* 30(2): 285–309.
- Rasmussen, M.V. (2006) *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century*. Cambridge: Cambridge University Press.
- Rayner, S. (1987) "Risk and Relativism in Science for Policy" B.B. Johnson and, B.B. and Covello, V.T. (eds) *The Social and Cultural Construction of Risk*. Dordrecht: Reidel.p23.
- Rayner, S. (1992) "Cultural theory and risk analysis" in Krinsky, S. and Golding, D. (eds.) *Social Theories of Risk*. Westport: Praeger.

- Razzouk, N. Y., Seitz, V. et al. (2008). "Consumer concerns regarding RFID privacy: an empirical study ", *Journal of Global Business & Technology*, 4(1): 69-78.
- Reiss, A. (1992) "The Institutionalization of Risk" in: Short, J.F. and Clarke, L. (eds) *Organizations, Uncertainties, and Risk*, Boulder: Westview. p. 299–308,
- Renn, O. (1998) "Three decades of risk research: accomplishments and new challenges," *Journal of Risk Research* 1(1): 49-71.
- Renn, O. (1991) "Risikowahrnehmung und Risikobewertung: Soziale Perzeption und gesellschaftliche Konflikte," in Chakraberty, S., Yadigarolu, G. (eds.) *Ganzheitliche Risikobetrachtung*, Köln: 1–62.
- Renn, O. (1992) "Concepts of Risk: A Classification" in Krimskie and Golding (eds.) *Social Theories of Risk*. Westport: Preager."
- Renn, O. (2010) "Public acceptance of energy technologies." Available at: <http://elib.uni-stuttgart.de/opus/volltexte/2010/5451/pdf/ren88.pdf>
- Renn O., Kasperson R.E. and Slovic P. (1992) "The social amplification of risk: theoretical foundations and empirical applications," *J.Soc.Iss.* 48(4): 137-160.
- Renn, O., Webler, T. et al. (1995). *Fairness and competence in Citizen Participation*, London: Kluwer.
- Resnick, M. L. and Montania, R. (2003) "Perceptions of Customer Service, Information Privacy, and Product Quality From Semiotic Design Features in an Online Web Store," *International Journal of Human-Computer Interaction* 16(2): 211-234
- Rieker, P. (2006) "From Common Defence to Comprehensive Security: Towards the Europeanization of French Foreign and Security Policy?" *Security Dialogue* 37(4):509-28.
- Riley, T.B. (2007) "Security vs. Privacy: A Comparative Analysis of Canada, the United Kingdom, and the United States," *Journal of Business and Public Policy* 1(2): 1–21.
- Roger, C. (1997) "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", Original of 15 August 1997, latest revs. 16 September 1999, 8 December 2005, 7 August 2006, available at: <http://www.rogerclarke.com/DV/Intro.html>
- Ross, L.D. (1977) *The Intuitive Psychologist and His Shortcomings: Distortions in the Attribution Process*, in: Berkowitz, L. (ed.) *Advances in Experimental Social Psychology* Vol.10, pp. 173-220, New York: Random House.
- Rowe, G. (1977) *An Anatomy of Risk*. New York.
- Salter, B. and Faulkner, A. (2011) "State strategies of governance in biomedical innovation: Aligning conceptual approaches for understanding rising powers in the global context", *Globalization and Health* 7(11).
- Sanquist, Thomas F, Heidi Mahy, and Frederic Morris (2008) "An exploratory risk perception study of attitudes toward homeland security systems." *Risk analysis: An International Journal* 28 (4):1125-1133.
- Santiso, C. (2002) "Promoting democratic governance and preventing the recurrence of conflict: the role of the United Nations development program in post-conflict peace-building." *Journal of Latin American Studies*
- Sattler, D. N., Kaiser, C. F., and Hittner, J. B. (2000) "Disaster preparedness: Relationships among prior experience, personal characteristics, and distress", *Journal of Applied Social Psychology*, 30: 1396–1420.
- Schmidt, M. (2004) *Investigating risk perception: a short introduction*. Available at: www.markusschmidt.eu/pdf/intro_risk_perception_Schmidt.pdf
- Schwartz, B. (1968) "The Social Psychology of Privacy", *American Journal of Sociology* 73(6): 741-752.
- Searle, R.H., Den Hartog, D.N., Weibel, A., Gillespie, N., Six, F., Hatzakis, R. and Skinner, D. (2011) Trust in the Employer: The Role of High Involvement Work *International Journal of Human Resource Management* 22(5), pp 1069 – 1092.
- Shareder-Frechette, K. S. (1991). *Risk and Rationality*. Berkley: University of California Press.

- Shearing, C. and Johnston, L. (2005) "Justice in the risk society" *The Australian and New Zealand Journal of Criminology* 38(1): 25-38.
- Scheinin M. et al. (2009). Terrorism and the Pull of 'Balancing' in the name of security. Law and Security, Facing The Dilemmas. EUI Working papers Series, Law Department, 2009/1, pp.- 55-64.
- Short, J. F. (1984) "The social fabric of risk: toward the social transformation of risk analysis," *American Sociological Review* 49: 711-725
- Siegrist, M. (2008) "Factors influencing public acceptance of innovative food technologies and products." *Trends in Food Science & Technology* 19: 603-608.
- Siegrist, M and Cvetkovich, G. (2000) "Perception of Hazards:The Role of Social Trust and Knowledge", *Risk Analysis* 20: 713-720.
- Simmel, G. (1957), *Brücke Und Tür*, Stuttgart: K. F. Koehler, p. 1.
- Sjöberg, L. (1999) "Perceived competence and motivation in industry and government in risk perception." in Cvetkovich and Löfstedt (eds). *Social trust and the Management of risk* London: Earthscan. pp. 89-99.
- Sjöberg L. (2000) "Factors in Risk Perception", *Risk Analysis* 20(1): 1-11
- Sjöberg, L. (2004) "The Perceived Risk of Terrorism" *Working Paper Series in Business Administration* 2002(11).
- Slovic, P. (1987) "Perception of Risk," *Science* 236: 280-285
- Slovic, P. (2000) *The Perception of Risk*. Earthscan.
- Slovic, P., Fischhoff, B. and Lichtenstein, S. (1985) "Rating the risks: The structure of expert and lay perceptions" in: Covello, V. T., Mumpower, J. L., Stallen, P. J. M. und Uppuluri, V. R. R. (eds.) *Environmental impact assessment, technology assessment, and risk analysis*. Berlin, Heidelberg, New York: Springer, pp. 131–156
- Slovic P., Fischhoff B. and Lichtenstein S. (1986) "The psychometric study of risk perceptions" in Covello V.T., Menkes J and Mumpower J. (eds.) *Risk evaluation and management*. New York, London: Plenum Press, pp. 3-24.
- Smith, D. A. and Uchida, C. D. (1988) "The social organization of self-help: A study of defensive weapon ownership". *American Sociological Review*, 53, 94–102.
- Smith, H Jeff, Milberg, Sandra J, and Sandra J Burke (1996) "Information Privacy: Measuring Individuals' Concerns about Organizational Practices", *MIS Quarterly* 20(2): 167-196.
- Smith, H. J., Dinev, T. et al. (2011) "Information Privacy Research: An Interdisciplinary Review", *MIS Quarterly* 35(4): 980-927.
- Smith, M. L. (2011) "Limitations to Building Institutional Trustworthiness through E-Government: A Comparative Study of Two E-Services in Chile", *Journal of Information Technology* 26: 78-93
- Smith, V.K. (1986) "A Conceptual Overview of the Foundations of Benefit-Cost Analysis", in Bentkover, J.D. Covello, V.T. and Mumpower, J. (eds) *Benefits Assessment: The State of the Art*, Dordrecht: Reidel. pp. 13–34.
- Sorensen, T.C. (1990) "Rethinking national security." *Foreign Affairs*:1-18.
- Spence A. et al., (2010) "Public Perceptions of Energy Choices: The Influence of Beliefs About Climate Change and the Environment", *Energy and the Environment* 21 (5): 385-407.
- Spence, K. (2005) "World Risk Society and War Against Terror," *Political Studies* 53(2): 284-302
- Stallings, R. A. (1987) Organizational Change and the Sociology of Disaster. Dynes, R et al (eds) *Sociology of Disasters*
- Stewart, K. A., and Segars, A. H. (2002) "An Empirical Examination of the Concern for Information Privacy Instrument," *Information Systems Research* (13:1), pp. 36-49.
- Stone, EF, Gardner, DG, Gueutal, HG, and McClure, S (1983) "A Field Experiment Comparing Information-Privacy Values, Beliefs, and Attitudes Across Several Types of Organizations," *Journal of Applied Psychology* 68(3): 459-468.

- Strange, S. (1996) *The retreat of the state: The diffusion of power in the world economy*: Cambridge University Press.
- Strickland, L.S. and Hunt, L.E. (2005) "Technology, Security, and Individual Privacy: New Tools, New Threats, and the New Public Perceptions," *Journal of the American Society for Information Science and Technology* 56(3): 221–34.
- Stritzel, H. (2007) "Towards a theory of securitization: Copenhagen and beyond," *European Journal of International Relations* 13(3): 357–83.
- Sunshine, J., and Tyler, T. R. (2003) "The role of procedural justice and legitimacy in shaping public support for policing" *Law & Society Review*, 37(3): 513–548
- Surveillance Studies Network (2006) "Report on Surveillance society, 2006", available at Surveillance Studies Network (2006), Report on Surveillance society, 2006 available at www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_public_discussion_document_06.pdf. See also Lodge, J. (2005) "e-Justice, Security and Biometrics: The EU's Proximity Paradox," *European Journal of Crime, Criminal Law and Criminal Justice* 13(4): 533–64.
- Sustein, C.R. (2007) *Worst-case scenarios*. Harvard University Press.
- Swedlow, B. (2011) "Cultural Coproduction of Four States of Knowledge," *Science, Technology & Human Values*
- Tansey, J. and O'Riordan, T. (1999). "Cultural theory and risk: a review." *Health, Risk and Society* 1(1): 71–90.
- Taureck, R. (2006) "Securitization theory and securitization studies," *Journal of International Relations and Development* 9(1): 53–61.
- Thaler, R. H. (1983) "Illusions and mirages in public policy", *Public Interest* 73: 60–74.
- Thompson, M. (1982) "A three dimensional model" in Douglas, M. (ed) *Essays in the Sociology of Perception*. London: Routledge
- Todt, O. et al. (2010) "Practical Values and Uncertainty in Regulatory Decision-making," *Social Epistemology* 24(4): 349–362.
- Tsoukala, A. (2006) "Democracy in the Light of Security: British and French Political Discourses on Domestic Counter-terrorism Policies," *Political Studies* 54(3): 607–27.
- Ul-Haq, M. (1995) *Reflections on human development*: USA: Oxford University Press.
- United Nations (1948) "The Universal Declaration of Human Rights", available at:
- Valverde, M. and Mopas, M.S. (2004) "Insecurity and the Dream of Targeted Governance" in Wendy Larner and William Walters (eds.) *Global Governmentality*. New York: Routledge, pp. 233–250
- Varian, H. R. (1996) "Economic Aspects of Personal Privacy", Technical report, University of California, Berkeley.
- Venkatesh, V. Morris et al. (2003) "User Acceptance of information technology: Toward a unified view" *MIS Quarterly*, 27 (3) 425–478
- Volio, F. (1981) "Legal personality, privacy and the family" in Henkin (ed) *The International Bill of Rights*, New York: Columbia University Press.
- Wæver, O. (2007) "Securitization and desecuritization," *International Security*, 66
- Wallerstein, I. (1979) *The capitalist world-economy*: Cambridge University Press.
- Walt, S.M. (1998) "International relations: one world, many theories." *Foreign Policy* :29–46.
- Waltz, K.N. (1979) *Theory of international politics*. New York: McGraw-Hill.
- Warren, S. Brandeis, L. (1890), "The Right to Privacy", *Harvard Law Review* 4: 193.
- Webb, M. (2007) *Illusions of Security: Global Surveillance and Democracy in the Post-9/11 World*. San Francisco, CA: City Lights Books
- Weiss, C. (2005) "Science, technology and international relations." *Technology in Society* 27(3): 295–313.
- Westin, A.F. (1967) *Privacy and Freedom*, New York: Atheneum, p.7.

- Whitley, R. (1987) "Taking Firms Seriously as Economic Actors: Towards a Sociology of Firm Behaviour., *Organization Studies* (Walter de Gruyter GmbH & Co. KG.), 8: 125-147, p. 133.
- Wiegman, O, Gutteling, J M, Boer, H (1991) "Verification of information through direct experiences with an industrial hazard", *Basic and Applied Social Psychology*, 12: 325-339.
- Wilsdon, J. and Willis, R. (2004) *See-through science: Why public engagement needs to move upstream*. London: Demos.
- Williams, M.C. (2003) "Words, Images, Enemies: Securitization and International Politics", *International Studies Quarterly* 47(4): 511-531
- Williams, M. J. (2008) "(In)Security Studies, Reflexive Modernization and the Risk Society" *Cooperation and Conflict* 43: 57-79
- Wisdom, J. (2007) "Public engagement of science across the European Research Area" *Public engagement of science*.
- Wolfers, A. (1952) "' National Security" as an Ambiguous Symbol," *Political Science Quarterly*: 481-502.
- Woodhouse, J (2010) *CCTV and its effectiveness in tackling crime*. Department of Home Affairs Standard Note SN/HA/5624
- Wynne, B. (1975) "The rhetoric of consensus politics: a critical review of technology assessment," *Research Policy* 4(2): 108-58.
- Wynne, B. (1984) "Public Perceptions of Risk" in Aurrey, J. (ed) *The Urban Transportation of Irradiated Fuel*. London: Macmillan.
- Wynne, B. (1992) "Misunderstood misunderstanding: social identities and public uptake of science," *Public Understanding of Science* 1(3):281-304
- Wynne, B. (2006) "Public Engagement as a Means of Restoring Public Trust in Science: Hitting the Notes, but Missing the Music?" *Community Genetics* 9(3): 211–20.
- Wynne, B. (2008) "Elephants in the Rooms Where Publics Encounter 'Science'? A Response to Darrin Durant, 'Accounting for Expertise: Wynne and the Autonomy of the Lay Public'," *Public Understanding of Science* 17(1): 21–33.
- Zinn, O. (2006) "Recent Developments in Sociology of Risk and Uncertainty" *Forum Qualitative Research* 7(1).
- Zinn, J. O. (2010) "Risk as a Discourse: Interdisciplinary Perspectives." *Critical Approaches to Discourse Analysis across Disciplines* 4(2): 106-124.
- Zureik, E. and Salter, M.B. (2005) *Global Surveillance and Policy: Borders, Security, Identity*. Cullompton: Willan Publishing.
- Zureik, E. and Hindle, K. (2004) "Governance, Security and Technology: The Case of Biometrics," *Studies in Political Economy* 73(Spring/Summer): 113–38.

9 List of Figures

Figure 1. Relationship between physical and information privacy	66
Figure 2. Model of Trust and Acceptance (Siegrist 2000).....	91
Figure 3. Theoretical Model	97
Figure 4. Map of Citizen Summits	100
Figure 5. Citizen summit key elements	101
Figure 6. Surprise postcards and recommendation forms	102
Figure 7. Factors expected to exert an influence on SOSTs Acceptability	104
Figure 8. : Frequency distribution (%): Acceptability of SOST in general	105
Figure 9. Frequency distribution (%): Items measuring Perceived Level of Threat	106
Figure 10. Frequency distribution (%): Technology supporters	107
Figure 11. Frequency distribution (%): Technology detractors	107
Figure 12. Frequency distribution (%): Information Privacy Concerns scale.....	109
Figure 13. Frequency distribution (%): Acceptability of specific SOSTs.....	110
Figure 14. Frequency distribution (%): Active avoidance of sCCTV/DPI/SLT	111
Figure 15. Frequency distribution (%): Resistance to specific SOSTs.....	112
Figure 16. Frequency distribution (%): Familiarity – Habituation	113
Figure 17. Frequency distribution (%): Familiarity.....	114
Figure 18. Frequency distribution (%): Perceived Effectiveness.....	115
Figure 19. Frequency distribution (%): Perceived Effectiveness – Accuracy	115
Figure 20. Frequency distribution (%): Perceived Effectiveness – Perceived security	116
Figure 21. Frequency distribution (%): Perceived Effectiveness – Validity	117
Figure 22. Frequency distribution (%): Perceived Intrusiveness.....	117
Figure 23. Frequency distribution (%): Perceived Intrusiveness – Risk of embarrassment.....	118
Figure 24. Frequency distribution (%): Perceived Intrusiveness – Intrusiveness.....	119
Figure 25. Frequency distribution (%): Perceived Intrusiveness – Risk of human rights infringement (I).....	120
Figure 26. Frequency distribution (%): Perceived Intrusiveness – Risk of human rights infringement (II)	120
Figure 27. Frequency distribution (%): Temporal proximity	121
Figure 28. Frequency distribution (%): Spatial proximity.....	122
Figure 29. Frequency distribution (%): Social proximity.....	122
Figure 30. Frequency distribution (%): Substantive Privacy Concerns. – Anonymity.....	123
Figure 31. Frequency distribution (%): Substantive Privacy Concerns. – Intimacy	124
Figure 32. Frequency distribution (%): Substantive Privacy Concerns – Solitude	125
Figure 33. Frequency distribution (%): Institutional trustworthiness	126
Figure 34. Frequency distribution (%): Institutional trustworthiness – Ability.....	126
Figure 35. Frequency distribution (%): Institutional trustworthiness – Benevolence.....	127
Figure 36. Frequency distribution (%): Institutional trustworthiness – Integrity	128
Figure 37. Frequency distribution (%): Regulation	129
Figure 38. Frequency distribution (%): Risk-Benefit balance – sCCTV (N=1093)	129
Figure 39. Frequency distribution (%): Risk-Benefit balance – DPI (N=1100)	130
Figure 40. Frequency distribution (%): Risk-Benefit balance – SLT (N=1065)	130

Figure 41. Graph showing all not-rejected hypotheses according to SEM results..... 133

10 List of Tables

Table 1.	Criteria for the development of more acceptable surveillance-orientated security technologies.....	ix
Table 2.	Risk analysis approaches	52
Table 3.	Psychological aspects attenuating or amplifying risk perception	55
Table 4.	Comparison of Westin's and Pedersen's privacy states	60
Table 5.	Comparison of Westin's and Pedersen's privacy functions	61
Table 6.	Taxonomy of privacy types.....	66
Table 7.	Relationships among privacy dimensions, functions and fundamental rights	69
Table 8.	Factors identified in previous studies.....	77
Table 9.	Factors that increase or hinder familiarity with certain risks.....	82
Table 10.	Correlation between acceptability and each attribute of the security system	84
Table 11.	Interpretation of SOSTs in relation to privacy and security	88
Table 12.	Overlaps between physical and information privacy: some examples.....	93
Table 13.	SOSTs assigned to group of countries.....	100
Table 14.	Total participants answered questions on each specific SOST and countries.....	101
Table 15.	Programme of a typical Surprise Citizen Summit.....	103
Table 16.	List of tested propositions	141
Table 17.	New and Emerging factors likely to influence SOSTs' acceptability.....	146
Table 18.	SEM model: Comparison between GLS, ML and ADF estimates.....	176
Table 19.	SEM – Generalised Least Squares (GLS) estimates	177
Table 20.	SEM – Maximum Likelihood (ML) Estimates.....	178
Table 21.	Quantile Regression: Other factors influencing Acceptability – Perceived Threat and General Attitudes toward Security Measures.....	179
Table 22.	Median Regression: Other factors influencing Acceptability – Regulation and the fact of considering a specific SOST as effective and not intrusive	180
Table 23.	Median Regression: Other factors influencing Acceptability – Regulation and the fact of considering a specific SOST as effective and intrusive	181
Table 24.	Median Regression: Other factors influencing Acceptability – Regulation and the fact of considering a specific SOST as not effective and highly intrusive	182
Table 25.	List of variables.....	183

11 List of Abbreviations

Abbreviation	Definition
BSE	Bovine spongiform encephalopathy
CCTV	Closed circuit television
CFIP	Concern for Information Privacy
CPR	Civil Registration System (Det Centrale Personregister)
DPI	Deep Package Inspection
EC	European Commission
EKINT	Eötvös Károly Institute
ESS	European Security Strategy
EU	European Union
EURODAC	European Conference on Design Automation
ESDP	European Security and Defence Policy
GDR	German Democratic Republic
GMC	Genetically modified crops
GMOs	Genetically modified organisms
GOP	Grand Old Party
HCLU	Hungarian Civil Liberties Union
ICT	Information and communications technology
IPR	Intellectual property rights
ISO	International Organization for Standardization
ISSP	International Social Survey Program
IT	Information Technology
NATO	North Atlantic Treaty Organization
NGO	Non Governmental Organisation
NIMBY	"not in my backyard"
OECD	Organisation for Economic Co-operation and Development
PCP	Pre-commercial procurement
PES	Public Engagement with Science
RFID	Radio-frequency identification
SLT	Smartphone Location Tracking
SOST	Surveillance-oriented security technology
STS	Science and Technology Studies
SVS	Salient ethical values
UNDP	United Nations Development Programme
WMD	Weapon of mass destruction

12 Annex

12.1 Statistical techniques applied in testing the hypotheses

12.1.1 Structural equation modelling (SEM)

Due to its characteristics, the statistical technique known as structural equation modelling (SEM) was chosen to test the effect of the independent variables and of the covariates on the dependent variable (i.e., SOST Acceptability), as well as the interaction effects between independent variables and covariates.

Structural equation modelling (SEM)⁴⁵⁴ is a powerful way for analysing covariance structures, though it does not represent a device for rigorous testing of causal theories.⁴⁵⁵ SEM is a confirmatory method whose most important and common sources of mis-specifications are produced by omitted variables and poor measurement.

Rather than building a latent variables model, we found it more convenient to summarise the information contained in each observed variable measuring a specific construct into an unweighted component, and then use these components to test the hypotheses. Standardised variables, which are those that are both centred on zero and are scaled so that they have a standard deviation of 1,⁴⁵⁶ were used to estimate these components and to facilitate the interpretation of results. The components perfectly reflect the scales presented in the previous section. Exploratory factor analysis and reliability tests were also performed before constructing the SEM model in order to ensure our measures were valid.

SEM is considered a large-sample technique.⁴⁵⁷ We can think about minimum sample size in terms of the ratio of cases (N) to the number of model parameters that require statistical estimates (q). An ideal sample size-to-parameters ratio would be 20:1.⁴⁵⁸ Such a sample should always guarantee stability in the model estimation. Less ideal would be an N:q ratio of 10:1, which for the example just given for q = 10 would be a minimal sample size of 10 × 10, or N = 100.⁴⁵⁹ Considerations related to normality and other distributional characteristics of the data, the estimation method chosen to fit the model, or the linearity of the relationships between variables, are all elements that contribute to determine an acceptable minimum sample size for using SEM. Information on the sample size of each analysis is reported in the tables of results.

In the tables presented in the following pages, the same model was tested for each SOST – i.e., smart CCTV (sCCTV), deep packet inspection (DPI) and smartphone location tracking (SLT). Three alternative estimation methods (i.e., the maximum likelihood, the generalised least squares method and the asymptotic distribution free method) were also used to check the stability of results for variables not perfectly normally distributed.

⁴⁵⁴ For additional references please visit: <http://www.ssicentral.com/lisrel/references.html>

⁴⁵⁵ Muthen, Bengt O. 1987. "Response to Freedman's Critique of Path Analysis: Improve Credibility by Better Methodological Training." *Journal of Educational Statistics* 12 (2):178-184. doi: 10.2307/1164895.

⁴⁵⁶ For more information please visit: <http://www.jeremydawson.co.uk/slopes.htm>

⁴⁵⁷ Kline, Rex B. 2011. *Principles and Practice of Structural Equation Modeling*. Edited by Todd D Little. Third Ed. ed, Methodology in the Social Sciences. New York: The Guilford Press.

⁴⁵⁸ Jackson, Dennis L. 2003. "Revisiting Sample Size and Number of Parameter Estimates: Some Support for the N:q Hypothesis." *Structural Equation Modeling: A Multidisciplinary Journal* 10 (1):128-141. doi: 10.1207/S15328007SEM1001_6.

⁴⁵⁹ Kline 2001: p. 12.

The maximum likelihood (ML) estimation method is a normal theory full-information method⁴⁶⁰ for continuous variables, which assumes multivariate normality for the population distribution of the endogenous variables. If the joint distribution of the variables is not distributed normally, ML can produce biased estimates. For this reason, we have also used the Generalised Least Squares (GLS) and the Asymptotic Distribution Free (ADF) large sample methods. As the GLS fit function is asymptotically equivalent to the ML fit function, we expect to find equivalent results in large enough samples.⁴⁶¹ Analyses were performed by using IBM SPSS AMOS 22.⁴⁶²

12.1.2 Quantile Regression

Quantile regression is a semi-parametric statistical method, which can be used to estimate the functional relationships between a set of covariates and the dependent variable for all portions of its probability distribution. This technique helps the researcher consider the impact of a covariate on the entire distribution of the dependent variable and not merely on its conditional mean.

Quantile regression represents a very good alternative to ordinary least square regression in the presence of skewed dependent variables or non-normally distributed errors. It is also invariant to monotonic transformations of the regressors, and it is more robust to outliers than least squares regression. Although it avoids assumptions about the parametric distribution of the error process, the quantile regression estimator is asymptotically normally distributed.

Despite its computation requiring linear programming methods to minimize the sum of absolute squared errors, an optimal solution can always be identified after a finite number of iterations.

When the 0.5th quantile, which is the median, is chosen, quantile regression becomes known as median regression. In this case, the conditional median function $Qq(y|x)$ is used to assess the relationship between the independent and dependent variables, exactly in the same way as the conditional mean function is used in linear regression. For this reason, interpretation of the results resembles the interpretation of the results of a traditional linear regression. Quantile regression results are particularly useful when extremes are important.

In this study, we are especially interested in understanding how various factors can exercise the same or a different influence on people who are highly supportive of the adoption of surveillance-based security measures and people who are highly sceptical about their implementation. For this reason the 0.25th quantile and the 0.75th quantile regression were used in testing the effects of the Level of Perceived Threat and of the General Attitudes toward Security Technology over Acceptability of SOSTs in general. Median regression was used to assess the effects of the Security-Privacy Balance variables on Acceptability of specific SOSTs.

In running these analyses the authors used Stata 12.

⁴⁶⁰ "When all statistical requirements are met and the model is correctly specified, ML estimates in large samples are asymptotically unbiased, efficient, and consistent. In this sense, ML estimation has an advantage under these ideal conditions over partial-information methods [such as two-stage least squares (TSLS) method] that analyse only a single equation at a time." Kline 2011: p. 155.

⁴⁶¹ Browne, M. W. (1982). Covariance structures. In D. M. Hawkins (Ed.), *Topics in applied multivariate analysis* (pp. 72-141). Cambridge, UK: Cambridge University. Browne, M. W. (1984). Asymptotically distribution-free methods for the analysis of covariance structures. *British Journal of Mathematical and Statistical Psychology*, 37, 1-21. Jöreskog, K. G. (1967). Some contributions to maximum likelihood factor analysis. *Psychometrika*, 32(4), 443-482. Muthén, B., & Kaplan, D. (1985). A comparison of methodologies for the factor analysis of non-normal Likert variables. *British Journal of Mathematical and Statistical Psychology*, 38, 171-189. Muthén, B., & Kaplan, D. (1992). A comparison of some methodologies for the factor analysis of non-normal Likert variables: A note on the size of the model. *British Journal of Mathematical and Statistical Psychology*, 45, 19-30. Yung, Y.-F., & Bentler, P. M. (1994). Bootstrap-corrected ADF test statistics in covariance structure analysis. *British Journal of Mathematical and Statistical Psychology*, 47, 63-84.

⁴⁶² The results presented have been tested using SPSS Amos 22 and Stata 12. Initial versions of the SEM model were tested by using Mplus 7.2. The authors wish to thank Dr Chris Stride for his help in using Mplus and for all his advices.

12.2 Tables of results

P	DV	IV	Sign			sCCTV			DPI			SLT		
			(GLS)	(ML)	(ADF)	(GLS)	(ML)	(ADF)	(GLS)	(ML)	(ADF)	(GLS)	(ML)	(ADF)
P1	Acceptability	Age	P	P	*	***	***	*	R	R	R	*	*	R
P2		Education	P	P	R	R	R	R	R	R	R	*	R	R
P3		Effectiveness	P	P	***	***	***	***	***	***	***	***	***	***
P4		SOST Understanding	N	N	R	R	R	R	R	R	R	R	R	R
P5		Intrusiveness	N	N	***	***	***	***	***	***	***	***	***	***
P6		Gender	P	P	*	R	R	*	R	R	R	*	R	R
P7		Social Proximity	P	P	***	***	***	***	***	***	***	***	***	***
P8		Substantive Privacy Concerns	N	N	*	***	***	*	***	***	***	***	***	***
P9		Spatial Proximity	N	N	***	***	***	***	***	***	***	***	***	***
P10		Temporal Proximity	N	N	R	R	R	R	R	R	R	R	R	R
P11		Institutional Trustworthiness	P	P	***	***	***	***	***	***	***	***	***	***
P12		Interaction between Age and Trustworthiness	N	N	***	***	***	***	***	***	***	***	***	***
P13	Effectiveness	Age			*	***	***	*	R	R	R	*	*	*
P14		Education			R	R	R	R	R	R	R	R	R	R
P15		Intrusiveness	N	N	***	***	***	***	***	***	***	***	***	***
P16		Gender	P	P	R	R	R	R	R	R	R	R	R	R
P17		Social Proximity	P	P	***	***	***	***	***	***	***	***	***	***
P18		Substantive Privacy Concerns	P	P	R	R	R	R	R	R	R	R	R	R
P19		Institutional Trustworthiness	P	P	***	***	***	***	***	***	***	***	***	***
P20		Interaction between Age and Trustworthiness	P	P	*	R	R	*	R	R	R	*	*	R
P21	Intrusiveness	Age			*	R	R	*	R	R	R	R	R	R
P22		Education			R	R	R	R	R	R	R	R	R	R
P23		SOST Understanding	P	P	*	***	***	*	R	R	R	R	R	R
P24		Gender	N	N	R	R	R	R	R	R	R	R	R	R
P25		Social Proximity	N	N	***	***	***	***	***	***	***	***	***	***
P26		Substantive Privacy Concerns	P	P	***	***	***	***	***	***	***	***	***	***
P27		Spatial Proximity	P	P	***	***	***	***	R	R	R	R	R	R
P28		Temporal Proximity	P	P	***	***	***	***	***	***	***	***	***	***
P29		Institutional Trustworthiness	N	N	***	***	***	***	***	***	***	***	***	***
P30	Substantive Privacy Concerns	Age			*	***	***	*	R	R	R	*	*	*
P31		Effectiveness			***	***	***	***	*	*	*	***	***	***
P32		SOST Understanding	N	N	***	***	***	***	R	R	R	R	R	R
P33		Gender	P	P	R	R	R	R	R	R	R	R	R	R
P34		Spatial Proximity	P	P	***	***	***	***	***	***	***	***	***	***
P35		Temporal Proximity	P	P	***	***	***	***	***	***	***	***	***	***
No of observations			1198	.88	.97	.93	.87	.96	.90	.91	.98	.93	.93	.93
CFI			1144	.91	.90	.90	.90	.90	.90	.90	.90	.90	.90	.90

Significance level Alpha = *** 0,001; ** 0,01; * 0,05.⁴⁶³

Table 18. SEM model: Comparison between GLS, ML and ADF estimates

⁴⁶³ "The significance level of a statistical hypothesis test is a fixed probability of wrongly rejecting the null hypothesis H0, if it is in fact true. It is the probability of a type I error and is set by the investigator in relation to the consequences of such an error. That is, we want to make the significance level as small as possible in order to protect the null hypothesis and to prevent, as far as possible, the investigator from inadvertently making false claims. The significance level is usually denoted by alpha Significance Level = P(type I error) = alpha." The Statistics Glossary, originally developed by Valerie J. Easton and John McColl. Available at: <http://www.stats.gla.ac.uk/glossary/?q=node/456>

	DV	IV	Sign	sCCTV			DPI			SLT					
				Est.	S.E.	P	Sig.	Est.	S.E.	P	Sig.	Est.	S.E.	P	Sig.
P1	Acceptance	↔ Age	P	0.050	0.019	0.008	***	0.019	0.022	0.374	R	0.047	0.021	0.027	*
P2		↔ Education		0.013	0.019	0.482	R	0.032	0.022	0.143	R	0.046	0.021	0.029	*
P3		↔ Effectiveness	P	0.357	0.028	0.000	***	0.258	0.030	0.000	***	0.281	0.029	0.000	***
P4		↔ SOST Understanding		-0.021	0.018	0.244	R	-0.016	0.022	0.467	R	0.017	0.022	0.440	R
P5		↔ Intrusiveness	N	-0.134	0.029	0.000	***	-0.162	0.030	0.000	***	-0.180	0.029	0.000	***
P6		↔ Gender		0.031	0.018	0.086	R	-0.011	0.021	0.620	R	0.043	0.021	0.038	*
P7		↔ Social Proximity	P	0.181	0.023	0.000	***	0.150	0.026	0.000	***	0.139	0.026	0.000	***
P8		↔ Substantive Privacy Concerns	N	-0.114	0.028	0.000	**	-0.167	0.031	0.000	***	-0.111	0.029	0.000	**
P9		↔ Spatial Proximity		-0.013	0.019	0.482	R	0.004	0.024	0.878	R	0.023	0.023	0.317	R
P10		↔ Temporal Proximity	N	-0.075	0.026	0.004	**	-0.034	0.028	0.225	R	-0.072	0.027	0.008	**
P11		↔ Institutional Trustworthiness	P	0.164	0.024	0.000	***	0.132	0.030	0.000	***	0.215	0.027	0.000	***
P12	↔ Interaction between Age and Trustworthiness		-0.060	0.020	0.002	**	0.003	0.023	0.882	R	-0.031	0.022	0.156	R	
P13	Effectiveness	↔ Age		0.031	0.021	0.138	R	-0.052	0.022	0.018	*	-0.014	0.023	0.530	R
P14		↔ Education		0.009	0.021	0.660	R	0.020	0.022	0.357	R	0.009	0.023	0.710	R
P15		↔ Intrusiveness	N	-0.387	0.025	0.000	***	-0.348	0.026	0.000	***	-0.220	0.027	0.000	***
P16		↔ Gender		0.012	0.020	0.537	R	0.026	0.021	0.218	R	0.021	0.023	0.342	R
P17	↔ Social Proximity	P	0.292	0.024	0.000	***	0.232	0.025	0.000	***	0.287	0.026	0.000	***	
P18	↔ Substantive Privacy Concerns		0.028	0.022	0.202	R	0.096	0.024	0.000	***	0.028	0.025	0.264	R	
P19	↔ Institutional Trustworthiness	P	0.249	0.025	0.000	***	0.252	0.028	0.000	***	0.306	0.027	0.000	***	
P20	↔ Interaction between Age and Trustworthiness	P	0.055	0.022	0.012	*	-0.008	0.023	0.744	R	0.024	0.024	0.307	**	
P21	Intrusiveness	↔ Age		0.034	0.020	0.080	R	0.030	0.022	0.187	R	-0.001	0.022	0.947	R
P22		↔ Education		-0.028	0.020	0.155	R	0.034	0.022	0.128	R	0.011	0.023	0.627	R
P23		↔ SOST Understanding	P	0.045	0.019	0.019	*	0.050	0.023	0.031	**	-0.006	0.023	0.799	R
P24		↔ Gender		-0.035	0.019	0.065	R	-0.012	0.022	0.589	R	0.027	0.022	0.211	R
P25		↔ Social Proximity	N	-0.185	0.022	0.000	***	-0.081	0.026	0.002	**	-0.017	0.026	0.498	R
P26		↔ Substantive Privacy Concerns	P	0.301	0.028	0.000	***	0.244	0.032	0.000	***	0.333	0.029	0.000	***
P27		↔ Spatial Proximity		0.057	0.020	0.004	**	-0.014	0.025	0.566	R	-0.020	0.024	0.406	R
P28		↔ Temporal Proximity	P	0.348	0.026	0.000	***	0.287	0.028	0.000	***	0.295	0.027	0.000	***
P29		↔ Institutional Trustworthiness	N	-0.106	0.024	0.000	***	-0.189	0.029	0.000	***	-0.187	0.026	0.000	***
P30		↔ Age		-0.053	0.024	0.023	**	-0.023	0.025	0.347	R	0.006	0.025	0.812	R
P31		↔ Effectiveness	N	-0.148	0.029	0.000	***	-0.073	0.030	0.014	*	-0.172	0.029	0.000	***
P32		↔ SOST Understanding		0.018	0.023	0.445	R	0.004	0.025	0.872	R	0.040	0.025	0.111	R
P33		↔ Gender		-0.005	0.023	0.835	R	0.028	0.024	0.250	R	-0.016	0.025	0.513	R
P34		↔ Spatial Proximity	P	0.061	0.024	0.009	**	0.078	0.027	0.004	**	0.013	0.026	0.614	R
P35		↔ Temporal Proximity	P	0.465	0.026	0.000	***	0.388	0.026	0.000	***	0.435	0.025	0.000	***
N				1198				1202				1144			
RMSEA				0.094				0.092				0.077			
CFI				0.883				0.869				0.914			
CMIN/DF				11.523				11.098				7.79			
Stability Index				0.067				0.034				0.054			

Significance level Alpha = *** 0,001; ** 0,01; * 0,05.

Table 19. SEM – Generalised Least Squares (GLS) estimates

		sCCTV	(ML) DPI	SLT	Sign	sCCTV Est.	sCCTV S.E.	P	DPI Est.	DPI S.E.	P	SLT Est.	SLT S.E.	P
P1	Acceptance	***	R	R	*	0.083	0.019	0.000	0.028	0.023	0.232	0.051	0.021	0.018
P2	↔ Age	R	R	R		0.014	0.018	0.461	-0.009	0.023	0.705	0.039	0.022	0.077
P3	↔ Education	***	***	***	P	0.375	0.029	0.000	0.354	0.034	0.000	0.326	0.03	0.000
P4	↔ Effectiveness	R	R	R		-0.01	0.019	0.594	-0.041	0.024	0.086	0.017	0.022	0.432
P5	↔ SOST Understanding	***	***	***	N	-0.304	0.038	0.000	-0.195	0.038	0.000	-0.229	0.04	0.000
P6	↔ Intrusiveness	R	R	R		0.028	0.018	0.125	-0.004	0.022	0.871	0.039	0.021	0.063
P7	↔ Gender	***	***	***	P	0.147	0.024	0.000	0.098	0.028	0.000	0.122	0.026	0.000
P8	↔ Social Proximity	**	***	**	N	-0.088	0.032	0.006	-0.195	0.034	0.000	-0.102	0.035	0.003
P9	↔ Substantive Privacy Concerns	R	R	R		0.026	0.02	0.188	-0.011	0.026	0.663	0.03	0.024	0.213
P10	↔ Spatial Proximity	R	R	R		0.004	0.028	0.895	0.047	0.031	0.135	-0.052	0.029	0.068
P11	↔ Temporal Proximity	***	***	***	P	0.083	0.024	0.000	0.17	0.031	0.000	0.2	0.028	0.000
P12	↔ Institutional Trustworthiness	**	R	R		-0.065	0.021	0.002	-0.03	0.025	0.222	-0.043	0.023	0.06
P13	↔ Age and Trustworthiness	R	R	R		0.041	0.022	0.07	-0.046	0.024	0.058	-0.008	0.026	0.743
P14	↔ Effectiveness	R	R	R		-0.012	0.022	0.595	-0.003	0.024	0.911	-0.015	0.027	0.585
P15	↔ Education	***	***	***	N	-0.354	0.028	0.000	-0.309	0.028	0.000	-0.228	0.032	0.000
P16	↔ Intrusiveness	R	R	R		0.033	0.022	0.136	0.033	0.023	0.155	0.041	0.025	0.104
P17	↔ Gender	***	***	***	P	0.308	0.027	0.000	0.254	0.028	0.000	0.282	0.031	0.000
P18	↔ Social Proximity	R	R	R		0.039	0.024	0.104	0.11	0.026	0.000	0.039	0.029	0.171
P19	↔ Substantive Privacy Concerns	***	***	***	P	0.257	0.028	0.000	0.307	0.029	0.000	0.315	0.033	0.000
P20	↔ Institutional Trustworthiness	R	R	R		0.046	0.025	0.066	0.039	0.026	0.132	0.077	0.028	0.006
P21	Intrusiveness	R	R	R		0.029	0.019	0.135	0.015	0.024	0.522	0.027	0.022	0.221
P22	↔ Age	R	R	R		-0.001	0.019	0.971	0.029	0.024	0.218	0.026	0.023	0.254
P23	↔ Education	***	***	***	P	0.069	0.019	0.000	0.072	0.024	0.003	-0.013	0.023	0.557
P24	↔ SOST Understanding	R	R	R		-0.033	0.019	0.077	0.004	0.023	0.868	0.028	0.022	0.191
P25	↔ Gender	***	***	***	N	-0.181	0.022	***	-0.087	0.028	0.002	-0.017	0.026	0.501
P26	↔ Social Proximity	***	***	***	P	0.388	0.028	***	0.396	0.03	0.000	0.444	0.028	0.000
P27	↔ Substantive Privacy Concerns	**	*	R	P	0.064	0.02	0.002	-0.054	0.026	0.04	0.025	0.024	0.311
P28	↔ Spatial Proximity	***	***	***	P	0.357	0.027	***	0.357	0.03	0.000	0.309	0.027	0.000
P29	↔ Temporal Proximity	***	***	***	N	-0.112	0.023	***	-0.105	0.029	0.000	-0.211	0.026	0.000
P30	↔ Institutional Trustworthiness	**	R	R		-0.078	0.026	0.002	-0.012	0.028	0.676	0.021	0.027	0.435
P31	↔ Age	***	*	***	N	-0.166	0.032	***	-0.097	0.037	0.01	-0.195	0.033	0.000
P32	↔ Effectiveness	R	R	R		-0.039	0.025	0.127	-0.021	0.029	0.467	0.055	0.028	0.049
P33	↔ SOST Understanding	R	R	R		-0.022	0.025	0.393	0.037	0.028	0.192	-0.017	0.027	0.535
P34	↔ Gender	***	***	***	P	0.093	0.026	***	0.083	0.032	0.009	0.056	0.029	0.052
P35	↔ Spatial Proximity	***	***	***	P	0.588	0.028	***	0.525	0.031	0.000	0.513	0.028	0.000
P35	↔ Temporal Proximity	***	***	***	P	0.588	0.028	***	0.525	0.031	0.000	0.513	0.028	0.000
N														
1198														
1202														
1144														
NPAR														
94														
94														
20:1														
15:1														
10:1														
Ideal Sample Size														
1880														
RMSEA														
0.10														
0.10														
CFI														
0.970														
CMIN/DF														
13.1														
8.7														
Stability Index														
0.081														
0.052														
0.073														

Significance level Alpha = *** 0,001; ** 0,01; * 0,05. The model is non-recursive.

Table 20. SEM – Maximum Likelihood (ML) Estimates

	25% quantile regression			75% quantile regression			25% quantile regression			75% quantile regression			25% quantile regression			75% quantile regression		
	ACC_PRE		ACC_POS	ACC_PRE		ACC_POS	ACC_PRE		ACC_POS	ACC_PRE		ACC_POS	ACC_PRE		ACC_POS	ACC_PRE		ACC_POS
	Sign	Sig	Sign	Sign	Sig	Sign	Sign	Sig	Sign	Sign	Sig	Sign	Sign	Sig	Sign	Sign	Sig	P
P1																		
AGE																		
P36																		
EDQUAL																		
P37																		
EARNING																		
P38																		
THR1																		
P39		*																
THR2																		
P40		**																
THR3																		
P41		***																
TEC1																		
P42																		
TEC2																		
P43		***																
TEC3																		
P44		***																
TEC4																		
P45																		
TEC5																		
Austria																		
Germany																		
Denmark																		
Hungary																		
Italy																		
Norway																		
Spain																		
UK																		
Switzerland																		
Constant																		
No. obs.																		
R ²																		

^ Variable omitted because of collinearity.

Significance level Alpha = *** 0,001; ** 0,01; * 0,05.

Table 21. Quantile Regression: Other factors influencing Acceptability – Perceived Threat and General Attitudes toward Security Measures

	DV: ACC_CTV						DV: ACC_DPI						DV: ACC_SLT					
	Sig.	Est.	Std. Err.	P			Sig.	Est.	Std. Err.	P			Sig.	Sign	Est.	Std. Err.	P	
P1	**	0,042	0,016	0,009		AGE		-0,011	0,019	0,580		AGE			0,031	0,018	0,091	
P46		0,030	0,047	0,519		SEX		0,046	0,057	0,421		SEX			-0,006	0,054	0,908	
P36		-0,014	0,017	0,418		EDQUAL		-0,013	0,021	0,518		EDQUAL			0,006	0,019	0,747	
P47		0,083	0,058	0,150		REG_CCT		-0,121	0,076	0,111		REG_SLT			0,018	0,061	0,761	
P48	***	0,234	0,063	0,000		TO_CDUM1	**	0,293	0,117	0,013		TO_SDUM1	**	P	0,170	0,069	0,014	
P3	***	0,371	0,057	0,000		PEF_DPI1	***	0,454	0,063	0,000		PEF_SLT1	***	P	0,377	0,057	0,000	
P5	***	-0,219	0,063	0,001		PIN_DPI1	***	-0,277	0,074	0,000		PIN_SLT1	***	N	-0,255	0,066	0,000	
P11	***	0,123	0,022	0,000		TRU_DPI1	***	0,145	0,026	0,000		TRU_SLT1	***	P	0,181	0,026	0,000	
P8	***	-0,167	0,022	0,000		SPC_DPI2	***	-0,231	0,029	0,000		SPC_SLT2	***	N	-0,181	0,026	0,000	
P7	***	0,119	0,018	0,000		SOCX_DPI	***	0,121	0,023	0,000		SOCX_SLT	***	P	0,090	0,022	0,000	
AUSTRIA		0,001	0,087	0,988		ITALY	**	-0,371	0,122	0,002		DENMARK	***	P	0,552	0,103	0,000	
GERMANY	***	-0,639	0,093	0,000		SPAIN	**	-0,315	0,124	0,011		NORWAY	***	P	0,501	0,114	0,000	
HUNGARY		-0,010	0,091	0,916		AUSTRIA	**	-0,328	0,123	0,008		HUNGARY	***	P	0,427	0,098	0,000	
SPAIN		0,084	0,098	0,390		UK		-0,094	0,109	0,387		ITALY	***	P	0,353	0,097	0,000	
UK	***	0,281	0,087	0,001		SWITZERLAND	**	-0,331	0,110	0,003		SWITZERLAND	***	P	0,410	0,090	0,000	
Constant		3,328	0,194	0,000		Constant		3,788	0,241	0,000		Constant			2,766	0,210	0,000	
No obs.		755					681						680					
Pseudo R		0,454					0,336						0,375					
		Var. Denmark omitted because of collinearity					Var. Norway omitted because of collinearity					Var. Germany omitted because of collinearity						

Significance level Alpha = *** 0,001; ** 0,01; * 0,05.

Table 22. Median Regression: Other factors influencing Acceptability – Regulation and the fact of considering a specific SOST as effective and not intrusive

Significance level Alpha = *** 0,001; ** 0,01; * 0,05.

Key factors affecting public acceptance and acceptability of SOSTs

[illegible]

Significance level Alpha = *** 0,001; ** 0,01; * 0,05.

Table 24. Median Regression: Other factors influencing Acceptability – Regulation and the fact of considering a specific SOST as not effective and highly intrusive

VAR NAME	VAR LABEL	VAR VALUES
AGE	Age (years)	6 options (from 18 to over 70 years old)
SEX	Gender	2 options (Male; Female)
ETHNIC	Belonging to a minority ethnic group	2 option (Yes; No)
CHN	Children at home aged 16 or under	2 option (Yes; No)
AREA	Area of living	3 options (Metropolitan; Urban; Rural)
EDQUAL	Education	6 options (from Primary to University Postgraduate)
EMPSTAT	Employment status	6 options (Employed; Self-employed; Unemployed; Stay-at-home parent or carer; Student; Retired)
OCC	Occupation	9 categories (from "Manager, legislator or senior official" to "Elementary worker")
EARNINGS	Earnings compared to the average of your country	5 options (from "A lot less than the average" to "A lot more than the average")
CITIZEN	Citizenship status	6 options (Citizen; Citizen of another European country; ...)
THR1	I generally feel safe in my daily life	5 options (from "Strongly disagree" to "Strongly agree")
THR2	I worry about security when I am online	5 options (from "Strongly disagree" to "Strongly agree")
THR3	I feel that this country is a safe place in which to live	5 options (from "Strongly disagree" to "Strongly agree")
EVAL1	I have gained new insight by participating in the citizen summit	5 options (from "Strongly disagree" to "Strongly agree")
EVAL2	I believe the citizen summit has generated valuable knowledge for the politicians	5 options (from "Strongly disagree" to "Strongly agree")
IPC1	I am concerned that too much information is collected about me	5 options (from "Strongly disagree" to "Strongly agree")
IPC2	I am concerned information held about me may be inaccurate	5 options (from "Strongly disagree" to "Strongly agree")
IPC3	I am concerned that my personal information may be shared without my permission	5 options (from "Strongly disagree" to "Strongly agree")
IPC4	I am concerned that my personal information may be used against me	5 options (from "Strongly disagree" to "Strongly agree")
TEC1	The use of surveillance-oriented security technologies improves national security	5 options (from "Strongly disagree" to "Strongly agree")
TEC2	Surveillance-oriented security technologies are only used to show that something is being done to fight crime	5 options (from "Strongly disagree" to "Strongly agree")
TEC3	If you have done nothing wrong you do not have to worry about surveillance-oriented security technologies	5 options (from "Strongly disagree" to "Strongly agree")
TEC4	If surveillance-oriented security technology is available national governments might as well make use of it	5 options (from "Strongly disagree" to "Strongly agree")
TEC5	Once surveillance-oriented security technologies are in place they are likely to be abused	5 options (from "Strongly disagree" to "Strongly agree")

FAM_CCT1	In the area where you live, how often do you see CCTV cameras	5 options (from "Never" to "All of the time")
FAM_CCT2	I understand what smart CCTV is	5 options (from "Strongly disagree" to "Strongly agree")
PEF_CCT1	I believe that Smart CCTV improves national security	5 options (from "Strongly disagree" to "Strongly agree")
PEF_CCT2	In my opinion, Smart CCTV is an effective national security tool	5 options (from "Strongly disagree" to "Strongly agree")
PEF_CCT3	I feel more secure when smart CCTV is in operation	5 options (from "Strongly disagree" to "Strongly agree")
PEF_CCT4	Smart CCTV is an appropriate way to address national security threats	5 options (from "Strongly disagree" to "Strongly agree")
PIN_CCT1	I believe that Smart CCTV is intrusive	2 option (Yes; No)
PIN_CCT2	I feel that smart CCTV is forced upon me without my permission	5 options (from "Strongly disagree" to "Strongly agree")
PIN_CCT3	The idea of smart CCTV makes me feel uncomfortable	5 options (from "Strongly disagree" to "Strongly agree")
PIN_CCT4	Smart CCTV worries me because it could violate my fundamental human rights	5 options (from "Strongly disagree" to "Strongly agree")
PIN_CCT5	Smart CCTV worries me because it could violate everyone's fundamental human rights	5 options (from "Strongly disagree" to "Strongly agree")
SPC_CCT1	Smart CCTV worries me because it could result in my behaviour being misinterpreted	5 options (from "Strongly disagree" to "Strongly agree")
SPC_CCT2	Smart CCTV worries me because it could reveal sensitive information about me	5 options (from "Strongly disagree" to "Strongly agree")
SPC_CCT3	Smart CCTV worries me because it could let strangers know where I am	5 options (from "Strongly disagree" to "Strongly agree")
ACC_CCT1	Overall I support the adoption of Smart CCTV as a national security measure	5 options (from "Strongly disagree" to "Strongly agree")
ACC_CCT2	Active avoidance of smart CCTV	5 options
ACC_CCT3	Challenging the use of smart CCTV for security purposes	5 options
TRU_CCT1	Security agencies which use Smart CCTV are trustworthy	5 options (from "Strongly disagree" to "Strongly agree")
TRU_CCT2	Security agencies which use Smart CCTV are competent at what they do	5 options (from "Strongly disagree" to "Strongly agree")
TRU_CCT3	Security agencies which use Smart CCTV are concerned about the welfare of citizens as well as national security	5 options (from "Strongly disagree" to "Strongly agree")
TRU_CCT4	Security agencies which use Smart CCTV do not abuse their power	5 options (from "Strongly disagree" to "Strongly agree")
TOF_CCT1	I think that the level of intrusiveness is acceptable given the benefits smart CCTV offers	2 option (Yes; No)
TOF_CCT2	Risk-benefit balance of CCTV (Trade-off)	4 options ("useful, not intrusive"; "useful, highly intrusive"; "not useful, not intrusive"; "not useful, highly intrusive")
TO_CDUM1	Trade-Off: CCTV - Dummy var cat 1 (useful, not intrusive)	2 option (Yes; No)
TO_CDUM2	Trade-Off: CCTV - Dummy var cat 2 (useful, highly intrusive)	2 option (Yes; No)
TO_CDUM3	Trade-Off: CCTV - Dummy var cat 3 (not useful, not intrusive)	2 option (Yes; No)
TO_CDUM4	Trade-Off: CCTV - Dummy var cat 4 (not useful, highly intrusive)	2 option (Yes; No)
REG_CCT	Laws and regulations ensure that smart CCTV is not misused	2 option (Yes; No)
SOCC_CCT	Smart CCTV does not bother me as long as it only targets criminals	5 options (from "Strongly disagree" to "Strongly agree")

TPRX_CCT	I worry about how the use of smart CCTV could develop in the future	5 options (from "Strongly disagree" to "Strongly agree")
SPRX_CCT	Smart CCTV only bothers me if it is used in the areas where I live and work	5 options (from "Strongly disagree" to "Strongly agree")
FAM_DPI1	How often do you use the internet	5 options (from "Never" to "All of the time")
FAM_DPI2	I understand what DPI is	5 options (from "Strongly disagree" to "Strongly agree")
PEF_DPI1	I believe that DPI improves national security	2 option (Yes; No)
PEF_DPI2	In my opinion, DPI is an effective national security tool	5 options (from "Strongly disagree" to "Strongly agree")
PEF_DPI3	When I am online, I feel more secure because DPI is used	5 options (from "Strongly disagree" to "Strongly agree")
PEF_DPI4	DPI is an appropriate way to address national security threats	5 options (from "Strongly disagree" to "Strongly agree")
PIN_DPI1	I believe that DPI is intrusive	5 options (from "Strongly disagree" to "Strongly agree")
PIN_DPI2	I feel DPI is forced upon me without my permission	5 options (from "Strongly disagree" to "Strongly agree")
PIN_DPI3	The idea of DPI makes me feel uncomfortable	5 options (from "Strongly disagree" to "Strongly agree")
PIN_DPI4	DPI worries me because it could violate my fundamental human rights	5 options (from "Strongly disagree" to "Strongly agree")
PIN_DPI5	DPI worries me because it could violate everyone's fundamental human rights	5 options (from "Strongly disagree" to "Strongly agree")
SPC_DPI1	DPI worries me because it could result in my behaviour being misinterpreted	5 options (from "Strongly disagree" to "Strongly agree")
SPC_DPI2	DPI worries me because it could reveal sensitive information about me	5 options (from "Strongly disagree" to "Strongly agree")
SPC_DPI3	DPI worries me because it could let strangers know where I am	5 options (from "Strongly disagree" to "Strongly agree")
ACC_DPI1	Overall I support the adoption of Deep Packet Inspection as a national security measure	5 options (from "Strongly disagree" to "Strongly agree")
ACC_DPI2	Active avoidance of DPI	5 options
ACC_DPI3	Challenging the use of DPI for security purposes	5 options
TRU_DPI1	Security agencies which use DPI are trustworthy	5 options (from "Strongly disagree" to "Strongly agree")
TRU_DPI2	Security agencies which use DPI are competent at what they do	5 options (from "Strongly disagree" to "Strongly agree")
TRU_DPI3	Security agencies which use DPI are concerned about the welfare of citizens as well as national security	5 options (from "Strongly disagree" to "Strongly agree")
TRU_DPI4	Security agencies which use DPI do not abuse their power	5 options (from "Strongly disagree" to "Strongly agree")
TOF_DPI1	I think that the level of intrusiveness is acceptable given the benefits DPI offers	2 option (Yes; No)
TOF_DPI2	Risk-benefit balance (Trade-off) of DPI	4 options ("useful, not intrusive"; "useful, highly intrusive"; "not useful, not intrusive"; "not useful, highly intrusive")
TO_DDUM1	Trade-Off: DPI - Dummy var cat 1 (useful, not intrusive)	2 option (Yes; No)
TO_DDUM2	Trade-Off: DPI - Dummy var cat 2 (useful, highly intrusive)	2 option (Yes; No)
TO_DDUM3	Trade-Off: DPI - Dummy var cat 3 (not useful, not intrusive)	2 option (Yes; No)
TO_DDUM4	Trade-Off: DPI - Dummy var cat 4 (not useful, highly intrusive)	2 option (Yes; No)

	smartphone location tracking offers	
TOF_SLT2	Risk-benefit balance (Trade-off) of Smartphone Location Tracking	4 options ("useful, not intrusive"; "useful, highly intrusive"; "not useful, not intrusive"; "not useful, highly intrusive")
TO_SDUM1	Trade-Off: SLT - Dummy var cat 1 (useful, not intrusive)	2 option (Yes; No)
TO_SDUM2	Trade-Off: SLT - Dummy var cat 2 (useful, highly intrusive)	2 option (Yes; No)
TO_SDUM3	Trade-Off: SLT - Dummy var cat 3 (not useful, not intrusive)	2 option (Yes; No)
TO_SDUM4	Trade-Off: SLT - Dummy var cat 4 (not useful, highly intrusive)	2 option (Yes; No)
REG_SLT	Laws and regulations ensure that smartphone location tracking is not misused	2 option (Yes; No)
SOCX_SLT	Smartphone location tracking does not bother me as long as it only targets criminals	5 options (from "Strongly disagree" to "Strongly agree")
TPRX_SLT	I worry about how the use of smartphone location tracking could develop in the future	5 options (from "Strongly disagree" to "Strongly agree")
SPRX_SLT	Smartphone location tracking only bothers me if it is used to track my own smartphone	5 options (from "Strongly disagree" to "Strongly agree")
KNOW_PRE	Pre-SurPRISE SumMIT: what is your knowledge of surveillance-oriented security technologies	4 options (I knew little to nothing; "I had some knowledge"; "I knew a good amount"; "I was very knowledgeable")
ACC_PRE	Pre-SurPRISE SumMIT: surveillance-oriented security technologies should be routinely implemented to improve national security	5 options (from "Strongly disagree" to "Strongly agree")
OPCL_PRE	Pre-SurPRISE SumMIT: the use of surveillance-oriented security technologies is eroding privacy in general	5 options (from "Strongly disagree" to "Strongly agree")
OPC2_PRE	Pre-SurPRISE SumMIT: the use of surveillance-oriented security technologies is eroding my privacy	5 options (from "Strongly disagree" to "Strongly agree")
ALT_PRE	Pre-SurPRISE SumMIT: Alternative approaches to security (not surveillance-oriented security) should be given higher priority	5 options (from "Strongly disagree" to "Strongly agree")
KNOW_POS	Post-SurPRISE SumMIT: how would you rate your knowledge of security technologies	5 options (from "Strongly disagree" to "Strongly agree")
ACC_POS	Post-SurPRISE SumMIT: surveillance-oriented security technologies should be routinely implemented to improve national security	4 options (I knew little to nothing; "I had some knowledge"; "I knew a good amount"; "I was very knowledgeable")
OPCL_POS	Post-SurPRISE SumMIT: use of surveillance-oriented security technologies is eroding privacy in general	5 options (from "Strongly disagree" to "Strongly agree")
OPC2_POS	Post-SurPRISE SumMIT: use of surveillance-oriented security technologies is eroding my privacy	5 options (from "Strongly disagree" to "Strongly agree")
ALT_POS	Post-SurPRISE SumMIT: Alternative approaches to security which do not involve surveillance oriented security technologies should be given higher priority	5 options (from "Strongly disagree" to "Strongly agree")
CHASOST	Has this experience changed your attitudes regarding security oriented surveillance technology	3 options ("Yes, they are now more negative"; "No, they are the same as before the meeting"; "Yes, they are now more positive")
CTYDUM1	Country Dummy for cat 1 Austria	2 option (Yes; No)
CTYDUM2	Country Dummy for cat 2 Denmark	2 option (Yes; No)
CTYDUM3	Country Dummy for cat 3 Germany	2 option (Yes; No)

CTYDUM4	Country Dummy for cat 4 Hungary	2 option (Yes; No)
CTYDUM5	Country Dummy for cat 5 Italy	2 option (Yes; No)
CTYDUM6	Country Dummy for cat 6 Norway	2 option (Yes; No)
CTYDUM7	Country Dummy for cat 7 Spain	2 option (Yes; No)
CTYDUM8	Country Dummy for cat 8 UK	2 option (Yes; No)
CTYDUM9	Country Dummy for cat 9 Switzerland	2 option (Yes; No)

Table 25. List of variables