"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 2.3 – Major security challenges, responses and their impact on privacy – selected security-oriented surveillance technologies

Lead Beneficiary: ITA/OeAW

Author(s): Stefan Strauß (ITA), Johann Čas (ITA)

Due Date: February 2013

Submission Date: June 2013

Dissemination Level: Public

Version: 1

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

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

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

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

Table of Contents

List of Abbreviations

Abbreviation	Meaning
AFSJ	Area of Freedom, Security and Justice
APIS	Advanced Passenger Information System
CCTV	Closed-Circuit Televison
CEPS	Centre for European Policy Studies
CIS	Customs Information System
DPA	Data Protection Authority
DPI	Deep Packet Inspection
DR	Data Retention
ECHR	European Convention on Human Rights
EDPS	European Data Protection Supervisor
ESRAB	European Security Research Advisory Board
ESRIF	European Security Research and Innovation Forum
GPS	Global Positioning System
ICT	Information and Communication Technology
ILP	Intelligence Led Policing
ISP	Internet Service Provider
MEMS	Micro-Electronic Mechanical Systems
NFC	Near-Field-Communication
NGO	Non-Governmental Organization
OECD	Organisation for Economic Co-operation and Development
PNR	Passenger Name Records
RFID	Radio Frequency Identification
SIS	Schengen Information System
SOST	Security-Oriented Surveillance Technology
UAV	Unmanned Aerial Vehicle
UDHR	Universal Declaration of Human Rights
VIS	Visa Information System

Executive Summary

This deliverable presents the final selection of surveillance-oriented security technologies (SOSTs) that build the foundation for the further exploration of the interrelations between privacy, security and surveillance within the SurPRISE project; in particular in the participatory setting to gather citizens' assessments of this interplay.

The SOSTs presented in this document are the outcome of a stepwise analysis where different criteria in combination with different types and dimensions of privacy were used as a heuristic. This report does not provide an in-depth analysis of surveillance-oriented security technologies or practices but describes the selection process along a set of factors ranging from major policy challenges to the interplay between privacy, security and surveillance. As a starting point, the deliverable gives a broad overview on the transformation of the security discourse with a particular focus on European security policy and related strategic objectives as well as major policy challenges on security and privacy, including citizens' perceptions and privacy concerns. The report is to be understood as a sort of bridging document between work package 2 (framing the assessment) and 3 (exploring the challenges) as the selection process and the final set of SOSTs presented is based on information of both WPs. Thus, this document also addresses the political security discourse and the frames of security and its privacy implications while a detailed analysis of these aspects and the socio-cultural factors is part of Deliverable 2.2. In order to sketch the complex interplay between security, surveillance and privacy, an overview on major legal norms is included, while an exploration of the legal aspects and regulatory frameworks is carried out in Deliverable 3.2. Based on these crossover aspects, the selection process and the major criteria are described that lead to the final selection of SOSTs. While this document gives a quick overview on these SOSTs, Deliverable 3.1 gives deeper insights into the current state of the art of surveillance-oriented security technologies.

The structure of the document is as follows:

After a brief introduction, in order to come to an informed selection of SOSTs that mirror the complex interplay between security, privacy and surveillance, section 2 deals with the general role and conceptualization of security and its change over time where important developments in the security discourse are enlightened. Subsequently, the paradigm shift and the transformation of contemporary security strategies and policies are discussed, referring to the theory of securitization to describe the changed framing of security. Section 3 sheds light on major policy challenges for privacy and security. It outlines the main foci and strategic objectives in the European security discourse and shows some insights into experts' assessments of global risks and the view of EU citizens on security issues as well as privacy concerns and related challenges. Section 4 deals with the question how security, privacy and surveillance are interrelated and what are the different types and dimensions of privacy. These build an important guideline for the selection process which is described in section 5, where the final selection of SOSTs is explained. Section 6 provides some concluding remarks.

The changing focus of security is visible in the transformation from traditional state-centered to human security. While the traditional security concept, protecting the state from threats, human security put the individual and the protection of his or her integrity in the center. This changing role of security had some impact on security strategies and policy-making but to some extent developed a momentum on its own. The increasing demand for a holistic security approach aiming at finding accordant strategies to deal with complex security challenges on a global scale strained human security and partially lead to a mixture of different security domains.

While the human security concept found its way into contemporary security policy there was a larger paradigm shift which is strongly related to the process of securitization. This shift is also visible in European security strategies and policy processes. In particular in the Area of Freedom, Security and Justice the role of security changed in way that surveillance-oriented measures also in relation to threat prevention gained higher importance. Increases in the processing of personal data by law enforcement

agencies, growing amounts of databases and information systems and intensified cooperation of national and international security authorities mirror this transformation.

The paradigm shift in contemporary security policy is outlined in relation to the theory of securitization which describes the practice of framing security in the political process. This is of particular interest as the securitization perspective reveals some of the mechanisms in the security discourse that can lead to unintended dynamics where the necessary focus of security measures on specific threats becomes blurry. This can reinforce the security-privacy trade-off which, together with the increasing role of security technology, then becomes further condensed. As a consequence, security measures and SOSTs as their means are endangered to lose sight of their primary security objectives and to become self-referential at the high cost of straining privacy protection.

Related to the changing role of security is a paradigm shift in European security policy which entailed a changed framing of security and privacy. While the security challenges and related responses addressed by security policies are without any doubt important issues for a secure society, there seems to be a sort of imbalance between the strategic security foci set by legal authorities compared to the assessments of experts and the concerns of citizens and the lay public. To some extent, these different perspectives refer to a disparity between security challenges and measures, also as regards different assessments of policy makers, experts and citizens. While experts point out the risks of economic and societal issues that to some extent also reflect in the perceptions of citizens, contemporary security policy does not address these issues in the same intensity than fighting crime and terrorism.

The implementation of surveillance-oriented security measures is often following the logic of the privacy-security trade-off in a way that the consideration of privacy is neglected. The entailed surveillance tendencies mostly embody in the employment of technology. At the same time, there are growing privacy concerns of citizens also regarding surveillance and profiling activities. Citizen have the increasing perception that disclosing personal information is hardly avoidable; entailed are growing concerns regarding informational self-determination and perceived lack of control over personal information. This is also visible in the growing number of requests and complaints brought to data protection authorities. A variety of security measures at EU level in particular in the Area of Freedom Security and Justice are assessed as critical as regards privacy and data protection. DPAs thus intensify their efforts to warn of overwhelming surveillance tendencies and a lacking coherence between security and privacy, mainly at the cost of the latter.

The interplay between security, privacy and surveillance is a complex one and legal norms play an important role in this regard also in relation to the privacy-security trade-off. How surveillance-oriented security technologies affect privacy is a further crucial question to reveal this interplay including the different types and dimensions of privacy. A classification in these types together with a process-oriented view to identify activities that affect privacy provided a fruitful heuristic for the selection process of SOSTs in the SurPRISE context. It allows focusing on SOSTs with a certain privacy impact in order to provide a mix of SOSTs that include different privacy types and a variety of privacy affecting activities. In further steps in the project it also contributes to derive alternative approaches and privacy-by-design mechanisms.

Section 5 describes the selection process, the main selection criteria for an informed choice and finally outlines those SOSTs that are elaborated further in the SurPRISE project. The result represents a relevant spectrum of contemporary surveillance-oriented security technologies that can affect different security domains as well as privacy types. As the SOSTs are the main basis for the participation process aiming at grasping citizens' opinions, also criteria such as actuality, diffusion and familiarity played a role for making the final choice of SOSTs. The selection consists of:

- Cyber surveillance
- (Smart) CCTV
- Location tracking
- Biometrics
- Behavioral profiling
- Drones

This set of SOSTs represents technology-related security measures that are already employed or expected to become issues of wider societal concern. With this mix of existing and emerging technological security measures the different degrees of privacy impacts and modes of surveillance are covered. Cyber surveillance represents a conglomerate of different privacy affecting activities and surveillance practices in relation to the widespread diffusion of ICT and digital networks. It is a sort of Meta-SOST as ICT are mostly used also in relation to other SOSTs. Video surveillance is widely known to the lay public and with smart CCTV becoming increasingly relevant it affects several additional privacy types. Mobile phones and mobile computing are among the fastest growing markets and from a privacy perspective, significantly widen the array of location tracking. Biometrics is already relevant for law enforcement and there is a significant increase in the collection and processing of biometric data. The growing amount of data collections fosters different kinds of profiling activities, which also raises citizens' concerns. Profiling is also a form of crossover activity that affects a variety of privacy types. Drones are among the emerging technologies that are about to become employed also in non-military, civil domains and thus can be expected to have deep societal impact.

These SOSTs reflect some of the major issues concerning contemporary security and privacy discourse. The transformation of security policy is to some extent a reasonable development to cope with security challenges in a global networked society. However, the incorporated framing of security as a holistic concept together with further tendencies for prevention intensifies tensions with privacy and reinforces the privacy-security trade-off, which might complicate further combined with extensive deployment of security technologies. In order to overcome this framing, a deeper understanding of citizens' perceptions of these technologies is required. In accordance with this, the selected SOSTs build the basis for the further exploration of the interplay between privacy, security and surveillance. They are a major part of the participation process and its design including a variety of relevant information material, questionnaires etc. to grasp different views and opinions of citizens on these technologies (in work packages 4, 5 and 7).

1 Introduction

Contemporary security policy is often accompanied by the employment of technological means to address a wide range of security challenges. The reasons for this interplay are manifold and not least shaped by societal development that is increasingly driven by technological progress. Security as a multi-facetted concept is part of this transformation and the same time has to cope with changing requirements to protect society from harm. The increasing use of security-oriented surveillance technologies (SOSTs) in many different domains is one result of this process. The implementation of security policy to address SOSTs is mostly grounded on a model that frames privacy and security as a trade-off. Already the term "trade-off" implies that one value has to be upheld at the expense of the other, i.e. that for improving security one has to accept a certain limitation on her privacy. This model entails a sort of "all-or-nothing position" suggesting that privacy and security are contradictory and that one has to choose between these values on the assumption that there would be a permanent conflict between both.

In such a framing it is seductive to neglect the meaning of privacy protection because it is seen as burden to security. This entails lacking consideration of the costs (economic and social) and effects of security measures. The trade-off is accompanied and shaped by the wrong questions: instead of asking the crucial question of how privacy should be protected, it is frequently asked whether privacy should be protected.[1] As a consequence of this framing, the crucial aspect is undermined: that both values are essential to the societies we live in. The challenge is to develop approaches to reconcile both values without loss in either. SurPRISE copes with this challenge by examining also the perceptions of European citizens on different SOSTs as specific examples. One aim is to reconsider the trade-off model and explore its implications as well as the options to overcome the inherent oversimplification of the relations between privacy and security. The project contributes to finding answers to the questions to what extent a complementary approach is feasible and what are the relevant factors for such an approach.

Objectives of this report

Technology plays a significant role in contemporary security policy. Therefore, its use in relation to surveillance and security is a major part of research in the SurPRISE project. As a starting point for the in-depth analysis of the interplay between privacy and security, we selected technology-related security measures that are presented in this document. The aim of this selection is to provide insight into how current security challenges are addressed by technology and to what extent these are affecting different levels of privacy.

The main objective of this report is to identify and select a limited number of SOSTs that are employed to address key challenges in contemporary security policy. According to the general objectives of SurPRISE, these technological means represent surveillance oriented security measures that are related to potential or actual conflict with fundamental rights and values, with a particular focus on privacy. The selected SOSTs are necessarily a small fraction of the multitude of challenges and possible responses within the general scope of the project; nevertheless they are chosen as much as possible to be representative for the scope of SurPRISE. They mainly serve as concrete examples of security areas, issues and measures that demonstrate possible differences among European states. The SOSTs also constitute the basket of suitable cases to be presented and discussed in the participatory activities which are a core element of SurPRISE.

Starting with an overview on the evolution of security policy and the interrelations between privacy, security and surveillance, this document focusses on security-oriented technologies and their privacy implications. To ensure that the selection exemplifies major security and privacy challenges, the analysis includes crucial policy issues in this regard. Based on information provided by WP2 and WP3, factors and criteria from the literature as well as from workshops and discussions conducted in the project, selected SOSTs are presented in this report that build the basis for the further work packages (in particular WP4)

[1] D. Solove (2011): Nothing to hide: the false tradeoff between privacy and security. Yale University Press. New Haven and London.

in SurPRISE and will be used to develop the participatory process (information material, films, etc.) for the citizen summits (that are part of Task 4.4).

2 Security: an evolving concept[2]

Security is a multi-faceted phenomenon with many different meanings. It varies considerably from one scientific discipline to another and in the broader context of public and political debate. Basically, security derives from the Latin "securus", which itself is based on "sine" (without) and "cura" (concern/worry/problem). This means security may be understood as the status of no necessity to be cautious. It can be defined in general terms as the absence of danger – that is a state where the desired status quo is not threatened or disrupted in any unacceptable way. In the course of time security has been loaded with different dimensions. Since the 18th century security has included the protection of individuals, their rights and property. In 1948 the Universal Declaration of Human Rights[3] stated in Article 3 "Everyone has the right to life, liberty and security of person." And in Article 22: "Everyone, as a member of society, has the right to social security and is entitled to realisation, through national effort and international co-operation and in accordance with the organisation and resources of each state, of the economic, social and cultural rights indispensable for his dignity and the free development of his personality."

The manifold character of security embodies two major roles: the security of society and the security of individuals forming a society. In the context of the SurPRISE project security is understood as concept that includes both roles and thus security of society incorporates citizens that constitute society.[4]

2.1 From state security to human security

There is a long tradition of security policy based on Hobbes' contribution to state philosophy[5], which saw security as a responsibility of the sovereign. Traditional state-centred security was the dominating concept reaching a peak during the Cold War. "For forty years, the major world powers entrusted the security of their populace, and to a certain extent of the world, to a balance of power among states. (…) This type of security relied primarily on an anarchistic balance of power (power as the sole controlling mechanism), the military build-up of two superpowers, and on the absolute sovereignty of the nation-state. (…) Security was seen as protection from invading armies; protection was provided by technical and military capabilities; and wars were never to be fought on home soil – rather, proxy wars were used if direct combat were necessary."[6] After World War II, diplomacy and international organisations began to play a more important role; organisations like the United Nations were widely acknowledged for dispute resolution. In Europe, the Council of Europe was founded which gave birth to the European Convention on Human Rights in 1950.

Although security policy was state-centred for a long time, at least there remained a marginal aspect of security for individuals. During the 1990s, a new approach has become more important in the political sphere focusing more on the individual than on the national state. In 1994 the UNDP introduced the new concept of human security in its Human Development Report[7]. This document is generally seen as the first significant attempt at articulating the broad approach to human security as an aspect of international policy. The report describes human security as having two principal aspects: the freedom from chronic threats such as hunger, disease and repression, coupled with the protection from sudden calamities.[8]

---

2 Parts of this section refer to Deliverable 6.2 of the PRISE project: M. Raguse, M. Meints, O. Langfeldt, W. Peissl (2008): "D6.2 - Criteria for privacy enhancing security technologies"p.16 ff.

3 Universal Declaration of Human Rights (UDHR) https://www.un.org/en/documents/udhr/

4 Raguse et al (2008) op. cit.

5 Referring to Thomas Hobbes' major work "The Leviathan" first published in 1651.

6 T. Owen (2004): Challenges and opportunities for defining and measuring human security, in: Human Rights, Human Security and Disarmament, disarmanet forum 2004 Vol 3. 15-24. p.16

7 United Nations – UN (1994): New dimensions of Human Security. Human development report 1994, United Nations Development Programme, New York, Oxford University Press.

8 See T. Owen (2004) op. cit. p.18

The report identifies seven components of human security:

- Economic security threatened by poverty;
- Food security threatened by hunger and famine;
- Health security threatened by injury and disease;
- Environmental security threatened by pollution, environmental degradation and resource depletion;
- Personal security threatened by various forms of violence;
- Political security threatened by political repression;
- Community security threatened by social unrest and instability.[9]

With the human security concept, the individual-centred approach entered into academic and political discussions. The first "broad" approach was influenced by policy in the field of human development (as mentioned above). Further discussions gave rise to other approaches leading to a "narrow" definition of human security that primarily focused on violent threats. The narrow approach towards human security "restricts the parameters of human security to violent threats against the individual. This can come from a vast array of threats, including the drug trade, landmines, ethnic discord, state failure, trafficking in small arms, etc."[10]

In order to be able to measure the level of human security Owen provides a new definition: "Human security is the protection of the vital core of all human lives from critical and pervasive environmental, economic, food, health personal and political threats."[11]

Type of security	Referent object	Responsibility to protect	Possible threats
Traditional security	The state	The integrity of the state	Interstate war Nuclear proliferation Revolution
Human security	The individual	The integrity of the individual	Disease Poverty Natural Disaster Violence Landmines Human rights abuses

Table 1: Traditional and human security (adapted from Owen 2004, 17)

This conceptionalisation of security provides a useful guiding line. As will be described in the following sections, the concept of (human) security further evolved and significantly changed over time with its

[9] UN (1994) op. cit
[10] T. Owen (2004) op. cit. p.19
[11] Ibd

adoption into various political strategies, and to some extent into a strained political issue complicating contemporary security policy.

2.2 Overview on the transformation of security policy (in Europe)

The changing role of security and related discourses have significantly changed within the last two decades. Not least due the Tragedy of 9/11 and the Madrid terrorist attacks of March 11, there is growth in security and surveillance modalities perceivable on a global scale. As Guild et al (2008) point out, in Europe, this shift becomes particularly visible in The Hague Programme and its ideological premise[12]:

> *The security of the European Union and its Member states has acquired a new urgency, especially in the light of the terrorist attacks in the United States on 11 September 2001 and in Madrid on 11 March 2004. The citizens in Europe rightly expect the European Union, while guaranteeing respect for fundamental freedoms and rights, to take a more effective, joint approach to cross-border problems such as illegal migration, trafficking in and smuggling of human beings, terrorism and organized crime, as well as the prevention thereof… . The programme seeks to respond to the challenge and the expectations of our citizens*[13].

Together with the Treaty of Prüm[14], the Hague Programme has significantly changed the normative and political settings of liberty and security in the Union and thus played a central role in altering how security is framed in Europe. This framing differs very much from its predecessor the Tampere Programme, where "shared commitment to freedom on human rights, democratic institutions and the rule of the law" were seen as common values that "have proved necessary for securing peace and developing prosperity in the European Union"[15]; or in other words: a complementary understanding of security in accordance with freedom (or more precisely liberty) and fundamental rights. In contrast, The Hague Programme entailed an expansion, predominance and strengthening of the security dimension over the other rationales of freedom and human rights. As a consequence, this change of strategic focus became part of a number of further policy documents among EU member states such as the currently effective Stockholm Programme[16]. These policies provided a strong political impulse towards common supranational security responses such as 'Provisions on Police and Judicial Cooperation in Criminal Matters' that is also part of the Treaty of the European Union. A significant increase of databases and information systems for law enforcement is a major part of this intensified cooperation. The Area of Freedom, Security and Justice (AFSJ) plays a particular role for European security strategy in this regard. It represents a set of policies focusing on strategic security issues and security related international data transfers. The Stockholm Programme inter alia aims at "greater coherence among external and internal elements of work in the area of freedom, security and justice" such as Europol, Eurojust, etc.[17]; in line with the ongoing reform of EU data protection regulation, in 2012 the European Council brought in a proposal for data protection in law enforcement to regulate data processing for "the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data".[18] Critics argue that while generally welcoming the

---

12 E. Guild, S. Carrera, T. Balzacq (2008): The changing dynamic of security in an enlarged European Union. Research paper No. 12, The changing landscape of European Liberty and Security - www.ceps.eu http://aei.pitt.edu/11457/1/1746.pdf

13 European Commission, Communication on The Hague Programme: Ten priorities for the next five years – The partnership for European renewal in the field of Freedom, Security and Justice, COM(2005) 184 final, Brussels. http://ec.europa.eu/home-affairs/doc_centre/docs/hague_programme_en.pdf

14 Council of the European Union, Prüm Convention Brussels January 7 2005 http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf

15 European Council, Tampere European Council 15 and 16 October 1999 Presidency Conclusions http://www.europarl.europa.eu/summits/tam_en.htm

16 European Council, Communication on Delivering an Area of Freedom, Security and Justice for European citizens - Action Plan implementing The Stockholm Programme. COM(2010) 171 http://www.statewatch.org/news/2010/apr/eu-com-stockholm-programme.pdf

17 Ibd

18 Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,

reform, several rules of the proposal were insufficient and weaken the protection of personal data e.g. as regards data transfer and profiling.[19]

In general, there seems to be a "difficult relationship between EU and intergovernmental processes in the area of security policy, which is primarily manifested in the form of challenges to the EU 'from below' by certain member states", as Guild et al (2008) argue.[20] The mentioned policies and agreements refer to this (at least to some extent) strained relationship. The AFSJ plays an important role in this regard as it reflects the shift in security framing: since its establishment in 1999 (on the basis of the Amsterdam Treaty) its foci changed significantly. Especially the Prüm treaty paved the way for intensified information exchange for law enforcement among the EU member states. It inter alia enabled the use of DNA profiling and fingerprint databases. The agreements of the Prüm treaty thus entailed a variety of critical aspects. According to Guild et al (2008) it "has created a hierarchy and a multilevel game within the EU" and "by focusing on data exchange, the Convention has provoked competition with the 'principle of availability' proposed by the Commission and The Hague Programme. By reverting to an intergovernmental arena, it excludes the European Parliament at a time when its role in democratic scrutiny is critical. (…) [B]y developing new mechanisms of security that operate above or below the EU level (or both), it has dismantled trust and confidence among member states. Finally, by establishing a framework whose rules are not subject to parliamentary oversight, the Prüm Treaty impacts on the EU principle of transparency"[21].

While an in-depth analysis of the EU's security policies is beyond the scope of this report, the highlighted issues refer to the aspects of security policy that are relevant for the further elaboration of SOSTs with an identifiable impact on privacy and other ethical and legal rights in the context of the SurPRISE project.

2.3 Securitization theory and complicated framing of security

As outlined in the previous sections, contemporary security discourses are characterized by several tensions. The role, meanings and conceptualisations of security vary in many respects depending on the specific domains to which they are related. The incremental transformation of security towards a holistic concept spanning across multiple domains fostered the variety of meanings. Since the post Cold War era the framing of security has been extended, at least in national and international affairs. A shift of how security is framed in this regard is e.g. visible in the changing focus of the United Nations on human security. In 2000, Kofi Annan, peace nobel prize winner and former Secretary-General of the United Nations until 2006, highlighted human security as something that "*in its broadest sense, embraces far more than the absence of violent conflict. It encompasses human rights, good governance, access to education and health care and ensuring that each individual has opportunities and choices to fulfil his or her potential. Every step in this direction is also a step towards reducing poverty, achieving economic growth and preventing conflict. Freedom from want, freedom from fear, and the freedom of future generations to inherit a healthy natural environment – these are the interrelated building blocks of human – and therefore national – security.*"[22]

While this already pointed towards a broadened view, it emphasized on reducing insecurities for ensuring human development in line with freedom and health (similar to Owen's definition in the previous section). However, in later policy, this emphasis seems to have changed towards an even wider view on human security as holistic concept. Such a framing where one threat is seen as trigger to further threats is a breeding ground for prevention and pre-emptive state mechanisms assumed as appropriate

---

and the free movement of such data [COM(2012) 10 final, Brussels, 25.1.2012, 2012/0010 (COD)] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF

19 See e.g. EDRI (2012): European Digital Rights (EDRI) EDRi's Position on the Directive https://dpreformlawenforcement.files.wordpress.com/2012/12/edri-position-papers-directive1.pdf

20 E. Guild, S. Carrera, T. Balzacq (2008) op. cit. p. 6

21 Ibd. p. 8

22 Kofi Annan. "Secretary-General Salutes International Workshop on Human Security in Mongolia." Two-Day. Session in Ulaanbaatar, May 8-10, 2000. Press Release SG/SM/7382. Cited from http://www.gdrc.org/sustdev/husec/Definitions.pdf

answer to combat pervasive threats.[23] Human security became used as "an effort to re-conceptualize security in a fundamental manner"; a framework where "(...) mitigating threats to the insecurity of individuals becomes a central goal of policy recommendations and actions."[24]

As a consequence of this integrative security framing, the original concept of human security with the individual as referent object and the responsibility to protect her from harm seems to have lost its focus to some extent. With the paradigm shift in security policy over the last two decades, the role of security and related policy measures is further strained and complicated as security policy shifts towards a comprehensive conceptualization of security that diminish the already blurry distinction between different meanings of security related to different domains. This is visible on a global scale as well as in the European Security Strategy which slightly developed towards a combination of a holistic security concept and multilateral approach, where tackling new threats, extending the zone of security around Europe and strengthening international order are among the strategic objectives[25].

The claim of policy makers to integrate different domains and sectors into a holistic concept of security is ambitious. On the one hand this approach corresponds to globalization and the need to cooperate beyond national borders on a supra- and international level towards common security strategies. On the other hand the conflation of intertwined but different roles and meanings of security in distinct domains complicates the efforts to develop appropriate security strategies to deal with emerging challenges. Buzan et al (1998) identified five distinct but intertwined sectors that play a strong role in the security discourse[26]: the military, political, economic, societal and environmental sector. As each of these sectors follows its own mechanisms and logics, the role, meanings, and measures in the realm of security might deviate significantly in each sector:

"Different forms or logics of security revolve around claims about referent objects and their existential character. For instance, social security is organized around the concept identity, while state security is organized around the concept of sovereignty."[27] Human security distinguishes from these logics and is linked to the concept of human life and dignity. "While state and societal security discourses also concern human life, they serve to prioritize the state or society as the means of protecting human life and dignity, whereas the discourse of humanitarian security attempts to prioritize human life over the interests of states and/or societies".[28] With an integrative view on once different security concepts, these different logics are at the risk of being neglected. What once was in the domain of humanitarian security in relation to crisis management to deal with natural disasters is used in the same policy issue related to terrorism and organized crime. The strive for a comprehensive security concept might complicate an informed distinction of security domains to develop appropriate measures; and together with technological push it might also entail the seductive assumption that in any case security challenges are manageable preferably by technological means.

From a theoretical stance, this paradigm shift in security policy is the effect of what many scholars (cf. Weaver 1995, Buzan et al 1998, Bigo 2000, Balzacq 2005, Watson 2011) termed the process of securitization.[29] Securitization entails the framing of security towards a holistic concept that spans across

---

[23] This is at least visible in a policy document of the UN: "Today, more than ever before, threats are inter-related and a threat to one is a threat to all." p. 14 "Development… is the indispensable foundation of a collective security system that takes prevention seriously." p. 3 The UN Secretary General's High-level Panel on Threats, Challenges and Change. 2004. A More Secure World: Our Shared Responsibility. New York: United Nations Press.

[24] R. Jolly and D. B. Ray (2006): "The Human Security Framework and National Human Development Reports: A Review of Experiences and Current Debates". United Nations Development Programme, National Human Development Report Unit. p. 5

[25] G. Quille (2004): The European Security Strategy: A Framework for EU Security Interests? In: International Peacekeeping, Vol.11, No.3, Autumn 2004, pp.1–16 http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede20040728_ess_/sede20040728_ess_en.pdf

[26] B. Buzan, O. Weaver, J. de Wilde (1998): Security: A New Framework for Analysis. Lynne Rienner: Boulder, 1998.

[27] S. Watson (2011): The 'human' as referent object? Humanitarianism as securitization. In: Security Dialogue 42(1):3-20. DOI:10.1177/0967010610393549 p. 5

[28] Ibd, p. 5

[29] Cf. B. Buzan, O. Weaver, J. de Wilde (1998) op. cit;

a broad scope of different domains has high influence on contemporary security policy. In the theory of securitization, security is conceptualized from a process view that is "marked by the intersubjective establishment of an existential threat with sufficient saliency to have political effects"[30]. In this process, security is not framed as an objective condition but is linked to political discourse where "sustained strategic practice"' aims at "convincing a target audience to accept, based on what it knows about the world, the claim that a specific development is threatening enough to deserve an immediate policy to alleviate it"[31]. Securitization makes security policy an arbitrary subject to politics. It is linked to political rhetoric and thus creates its own dynamics where the informed need for security measures to address threats becomes decoupled from serious considerations/conceptualizations on appropriate responses. This is also visible in the European security strategy which involves a broad spectrum of different security challenges such as poverty, diseases, climate change, energy supply, terrorism and organized crime. However, measures to deal with these challenges the focus seem to lie mainly on the latter two which then embody in further policy. While without any doubt each of these challenges needs to be addressed with appropriate measures, a lacking distinction between different roles of security can complicate the task to develop these measures. Due to its own particular dynamics the process of securitization can lead to what Guild et al (2008) called the "security continuum" addressing the problem of "political structurization or securitization of certain persons and practices as 'threats'" in a rather pragmatic manner. In this pragmatic act of security and the entailed "logic of converging (in)securitization (…) particular thematic policy issues, such as irregular immigration, borders and the integration of immigrants" are framed as 'threats' or insecurities for the EU and its member states"[32]. Especially the linking of security and (im)migration is a prominent example for the dangerous effects of securitization as several scholars point out.[33]

In such a framing, security becomes "a uniquely powerful discourse that moves issues from the realm of the political to the realm above politics, allowing elites to implement emergency measures that violate the normal political rules of the game"[34]. Issues often become presented as existential threats that require particular "measures and justifying actions outside the normal bounds of political procedure"[35].

As securitization is mostly linked to political processes, it reinforces security discourses in a way that communicates security as a dominant issue of societal concern compared to other state functions and duties mainly the protection of fundamental rights such as the right to privacy.

Core problems of securitization are that security and related measures becomes widely equivocal and manipulable, as measures might be introduced for self-serving purposes that undermine sound evaluation of security in relation to other policy objectives. The result can be conflicting interests and lacking public acceptance and increasing resistance against security policy. Inherent is the danger that security becomes self-referential without focus on reducing realistic risks and threats or is misused to justify other political objectives (such as technological push or other political issues). If security becomes reinforced at the cost of seemingly subordinated objectives such as the protection of civil liberties including privacy, this can lead to a further aggravation of the privacy-security trade-off.

D. Bigo (2000): "When two become one: Internal and external securitisations in Europe." In: International Relations Theory and The Politics of European Integration. Power, Security and Community. M. Kelstrup and M. Williams (eds.), London, Routledge, pp. 171-204.

T. Balzacq (2005): The three faces of securitization: Political agency, audience and context. In: European Journal of International Relations 11(2): 171-201.

S. Watson (2011) op. cit.

30 S. Watson (2011) op. cit., p. 3

31 T. Balzacq (2005): The three faces of securitization: Political agency, audience and context. In: European Journal of International Relations 11(2): 171-201. p. 173

32 E. Guild, S. Carrera, T. Balzacq (2008) op. cit. p. 2

33 E.g. G. Karyotis (2011): "*The fallacy of securitizing migration: elite rationality and unintended consequences*". In: G. Lazaridis (ed.): Security, Insecurity and Migration in Europe. Ashgate, Surrey, Great Britain, pp. 13-30. See also M. Ibrahim (2005): "The Securitization of Migration: A Racial Discourse". In: International Migration, Vol. 43 (5), pp. 163-187.

34 B. Buzan, O. Weaver, J. de Wilde (1998) op. cit. p. 23 f.

35 Ibd, p. 24

2.4 The role of technology in security policy

Technology is often seen as sine qua non in security policy "to every security dilemma and 'threat' identified, as being essential to the establishment of the EU as a common AFSJ"[36]. Technological push related to securitization may lead to a situation where the distinction between different levels and impacts of security threats that are manageable by technology further diminishes. To some extent the nature of ICTs seduces policy makers to perceive them as the most-suitable solution and employ them to address security challenges and implement security measures on behalf of security strategy and policy (as outlined above). The variety of technological features and functionalities draw a delusive picture that complex measures could easily become supported or even fully automated and thus would be cost-effective, more efficient and less prone to errors.

The strong role of technology in European security policy is not least visible in the wide array of databases and information systems such as the Schengen Information Systems (SIS) I and II, Eurodac, the Customs Information System (CIS), the Europol system, Eurojust files and the Visa Information System (VIS). In combination to these systems, methods for direct information exchange among law enforcement authorities are applied that include a variety of data such as the results of DNA analysis, criminal records, passport information etc.[37] Thus, these systems are part of a larger increase in information exchange among law enforcement agencies.[38] This trend towards fostering interoperability and synergies also carries forward a variety of risks with function creep among the most compelling ones.[39]

The employment of technology is to some extent the result of an ambitious strive towards systematic approaches to come to a better informed holistic understanding of security. However, security technologies are often introduced "(…) without duly considering that it could engender more insecurity in terms of data protection, fundamental rights and liberty. Also, a certain tension arises between security technology in its various forms (large-scale centralized EU databases, biometrics and so forth) and the rule of law."[40] An extensive focus on technology-based security measures without assessing their appropriateness regarding societal impacts undermines the roots of security: to protect the individual human as part of the state and maintain their role as active citizens without fear or repression.[41] Together with increasing pre-emptive and preventive modes of surveillance, this essential role and the original concept of human security, i.e. to protect the integrity of the individual and her rights, might be undermined further. So instead of primarily protecting individuals and the state from risks and threats, this holds the danger that individual citizens easily become classified as threats to state security. Security governance in such a framing represents governance of failure.[42] In particular this might occur due to an increasing imbalance of power between the individuals and those institutions that set the security agenda without or with insufficiently including the public's and individual's opinion and perceptions into the policy process. The consequence is a lack in checks and balances and in the public's right to scrutinize appropriateness of governmental security measures. Thus, participatory approaches are strongly demanded to overcome the dichotomy between state and individual, and the

---

36 Guild, Carrera, Balzacq (2008) op. cit. p. 3

37 Cf. T. Balzacq (2008): "The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policy", Journal of Common Market Studies, Vol. 46, No. 1, 2008.
Cf. F. Geyer (2008): Taking Stock: Databases and Information Exchange in the Area of Freedom, Security and Justice, CHALLENGE Research Paper No. 9, CEPS, Brussels.

38 The intensified information collection and exchange is a major part in the AFSJ and the according policies such as the Stockholm Programme as mentioned above.

39 P. Hobbing 2006: Security and Information: SIS II and the Interoperability of JHA Databases, Centre for European Policy Studies (CEPS), Brussels.

40 E. Guild, S. Carrera, T. Balzacq (2008) op. cit. p. 4

41 Examples exist even on the contrary with elements of mistrust in security measures where individuals can easily become subject to surveillance and classified as suspicious without a concrete suspicion; such as false positives on the US "no fly list" https://www.schneier.com/blog/archives/2006/10/nofly_list.html or profiling of innocent in DNA databases in the UK http://www.guardian.co.uk/politics/2009/oct/28/dna-database-innocent-profiles

42 Cf. M. Yar (2011) "From the 'Governance of Security' to 'Governance Failure': Refining the Criminological Agenda", Internet Journal of Criminology (Online)

related security-privacy trade-off model. To reduce the risk of privacy infringements of surveillance technology, a particular focus on privacy enhancing design approaches is essential.[43]

With technological push in relation to securitization and the shift towards pre-emptive state mechanisms and thus modes of security and surveillance, the distinction and boundaries between the different sectors and conceptualizations of security become further blurred.

Security technologies are not merely introduced as responses to specific threats but also part of economic and commercial interests.[44] Thus also economic aspects are to be seen in relation to this development. A strong driver of the global growth in security and surveillance modalities is given by new economic mechanisms and markets not least coined by what the OECD termed the security economy[45] and the field of security economics where security is mainly framed by different economic considerations[46]. The set-up of surveillance here is mostly seen as a necessary means to foster security which also stimulates new markets and innovation. This assumption follows a simple formula claiming more surveillance leads to more security and wider use of related technologies creates new markets. As a consequence, the employment of SOSTs is mainly driven by economic objectives that neglect the negative impacts on the economy and society in a wider sense. Civil society organisations like Statewatch thus criticize the strong influence of the industry on European security research programmes.[47] An overwhelming focus on economic aspects is another crucial aspect that reinforces the privacy-security trade-off at the potential high costs of privacy and other fundamental rights.

---

[43] Privacy enhancing design aspects are considered in WP3, E. Schlehan, M. Hansen, J. Sterbik-Lamina J. S. Samaniego (2013): "D3.1. – Report on surveillance technologies and privacy enhancing design".

[44] B. Hayes (2006). Arming Big Brother. The EU's Security Research Programme. TNI Briefing Series. Amsterdam, Transnational Institute.

[45] OECD (2004): "The Security Economy", http://www.oecd.org/futures/16692437.pdf

[46] Cf. H. Engerer (2009): "Security Economics: Definition and Capacity". Economics of Security Working Paper 5, Berlin: Economics of Security. http://www.diw.de/documents/publikationen/73/diw_01.c.94891.de/diw_econsec0005.pdf

[47] B. Hayes (2009). "NeoConOpticon. The EU Security-Industrial Complex." http://www.statewatch.org/analyses/neoconopticon-report.pdf

3 Major policy challenges on security and privacy

The paradigm shift in security policy is visible in the current foci of the European Union as it reflects how the different security domains conflate the process of securitization and are mainly addressed by technological means. This section gives an overview on the major security domains emphasized in European security strategy as well as the citizens' views on the related main challenges. In order to avoid a narrow, single-sided perspective, the scanning of security challenges in this report integrates, on the one hand, the results from other expert bodies, on the other hand, the perception of risks and threats of citizens as expressed in public opinion polls. The second part of this chapter delineates some of the major privacy challenges by outlining important policy issues and concerns by the European Data Protection Supervisor, as well as presenting some of the citizens' attitudes and concerns on privacy.

3.1 Core domains of EU Security strategy

The domains that are in the center of Security Research Funding from the European Commission provide a useful starting point for the identification of major security challenges. At the global level, the Commission highlights the following as crucial ethical and regulatory challenges to science and research policy[48]:

- **Border, Aviation, Port, and Cargo Security** cover technologies for human identification and authentication, passenger and baggage screening, cargo screening and container tracking. Research in this area focuses on conventional *biometric identifiers* (fingerprints, iris scan, face recognition, voice analysis, hand geometry, palm vein, etc.); multiple and *multimodal biometrics*; behavioural biometrics; radio frequency identification (*RFID*) tags; smart cards micro-electronic mechanical systems (MEMS); surveillance and detection technologies, and more.
- **Biological, Radiological, and Chemical Agents Prevention** is an expanding area focused on detection of and protection from intentional attacks (from both state and non-state actors) and natural hazards (e.g., bird flu). Detection tools include a vast array of chemical, biological, and radiation detectors, from conventional "puffer devices" that detect trace amounts of explosives, to technologies such as neutron resonance fluorescence imaging, which can scan large volumes of cargo or luggage down to the atomic level. Protection tools include vaccines, protective clothing, blast absorbing materials, neutralizing agents, and decontamination materials.
- **Data Capture, Storage, Mining and Profiling** focuses on data handling at various levels, the semantic web, mesh networking and grid computing, devices for intercepting communications signals and related information flows, and more. So-called Intelligence Led Policing (ILP) points towards a merging of law enforcement, counterterrorism, and disaster response technologies. Communication across disparate (and formerly totally independent) national and international agencies has become more and more important, as has the involvement of the private sector.
- **Emergency Preparedness and Response Technologies** include vaccine stockpiles, communications systems, control systems for situational awareness, decision support systems for real-time response, and data integration and fusion. Related technologies include Geospatial Web and Location-Based Services, comprising emerging systems of global epidemiological surveillance based on monitoring online communications and the World Wide Web.

While the second category — *biological and chemical agents prevention* — represents an area where innovations mainly come from chemistry, especially analytical chemistry, the other three areas see innovations emerging from several engineering fields, like mechanical engineering, and computer

[48] European Commission (2012). Ethical and Regulatory Challenges to Science and Research Policy at the Global Level. Brussels, Directorate-General for Research and Innovation. http://ec.europa.eu/research/science-society/document_library/pdf_06/ethical-and-regulatory-challenges-042012_en.pdf

science. Some of these technical innovations are briefly presented to offer concrete examples of digital surveillance-oriented security technologies proposed to be used to fight terror and crime.

At the European level, security domains in the European Union[49] that are explicitly funded inter alia include[50]

- **security of citizens** – technology solutions for civil protection, bio-security, protection against crime and terrorism
- **security of infrastructures and utilities** - examining and securing infrastructures in areas such as ICT, transport, energy and services in the financial and administrative areas.
- **intelligent surveillance and border security** - technologies and methods for protecting Europe's border controls
- **restoring security and safety in case of crisis** - technologies and communication, coordination in support of civil, humanitarian and rescue tasks
- **security systems integration, interconnectivity and interoperability** - information gathering for civil security, protection of confidentiality and traceability of transactions
- **security and society** - socio-economic, political and cultural aspects of security, ethics and values, social environment and perceptions of security
- **security research coordination and structuring** - coordination between European and international security research efforts in the areas of civil, security and defence research.

Of particular relevance is also the European security strategy[51] with its more task and action oriented domains. The following five strategic objectives represent responses to the most urgent challenges[52] to EU security:

a) Disrupt international crime networks

b) Prevent terrorism and address radicalisation and recruitment

c) Strengthen security through border management

d) Raise levels of security for citizens and businesses in cyberspace

e) Increase Europe's resilience in crises and disasters

These issues are of utmost concern to any European country. Each of these domains addresses a number of different security threats and challenges to be tackled to ensure a free and secure society. Ensuring human security is essential to guarantee the development of an inclusive, active and participative society, free from fear, uncertainty, and violence. Although the urgency and relevancy of these problems may appear straightforward to many, approaches and strategies to address these matters may differ substantially across regional areas. Thus it is no surprise that also a variety of security measures and technologies have been developed and implemented as a response to these threats.[53] In fact, each threat – which is a challenge from a policy-making point of view, has been addressed and tackled

[49] European Commission April 2013, http://ec.europa.eu/rea/funding_opportunities/security/index_en.htm
[50] Descriptions of all individual projects funded in these areas are collected in the 2011 security research catalogue http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=5405&lang=en&tpa_id=168
[51] European Commission (2010). Communication from the Commission to the European Parliament and the Council - The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. Brussels. http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf
[52] Serious and organised crime, Terrorism, Cybercrime, Security of EU borders and Natural man-made disasters.
[53] Such as an increasing use of biometric technologies, growing amounts of databases and information systems for law enforcement and increasing data exchange.

through a complex bundle of measures, some of them centred on technological tools and others on social policy actions.

3.2 Expert assessment of global risks

Risk assessments carried out by independent expert groups are taken into account as additional information for the identification of security challenges. The Global Risks Report 2013[54] published by the World Economic Forum is based on a survey of 469 experts from industry, government, academia and civil society. This survey takes a much wider approach to identify the most serious threats for future prosperity and security, thus forming an important instrument of information for the objective of SurPRISE to include the wider societal context into the conducted research.

Based on a ten-year outlook, among the 50 prevalent global risks, the ten highest ranked in terms of likelihood and impact are:[55]

- Severe income disparity
- Chronic fiscal imbalances
- Rising greenhouse gas emissions
- Water supply crises
- Mismanagement of population aging
- Cyber attacks
- Failure of climate change adaption
- Pervasive entrenched corruption
- Extreme volatility in energy and agricultural prices
- Persistent extreme weather

These risks also mirror the problematic interplay between economic and ecologic crisis which is pointed out in the report, as both – economic and environmental systems - are strained on a global level. Together, the increasing threats of climate change and the ongoing economic fragility may raise unprecedented challenges to global and national resilience. To deal with these problems requires structural changes and strategic investments but countries might encounter several difficulties to handle both at the same time.

The domains of EU security research incorporate these risks only partially (e.g. regarding resilience and disaster management). While EU security strategies mainly focus on fighting crime and terrorism, these aspects are not among the high ranked risks in the experts' assessment. One exception is cyber security which is mentioned in the Global Risk Report in relation to the increasingly hyperconnected world that fosters challenges for privacy, freedom of expression and other fundamental rights.

3.3 Security challenges from the citizens' view

Historical, cultural and institutional characteristics vary largely inside Europe. Those differences create variability in the type of policy responses and measures chosen in each context to attack even the same security challenges. The perspective and perception of citizens on security challenges are thus of central importance for SurPRISE. National peculiarities in security policies and related measures are part of Deliverable 2.2 and will be further explored in work package 6 in national reports on the countries involved.

In 2011 a Special Eurobarometer survey was devoted to the public perception of internal security. It serves as a starting point for identifying security challenges in the perception of citizens of the European Union. Special Eurobarometer 371[56] on Internal Security from November 2011 has the specific aim to compare the results from open and unprompted answers of European citizens with the security agenda set out in the Communication from the Commission on the EU Internal Security Strategy in Action: Five

[54] World Economic Forum (2013). Global Risks 2013. An Initiative of the Risk Response Network. Geneva. Eighth Edition. http://reports.weforum.org/global-risks-2013/

[55] http://reports.weforum.org/global-risks-2013/section-seven-online-only-content/data-explorer/

[56] European Commission (2011). Special Eurobarometer 371 - INTERNAL SECURITY. Report Number 371.

steps towards a more secure Europe[57]. The EU Internal Security Strategy comprises the following five challenges: Serious and organised crime, Terrorism, Cybercrime, Security of EU borders and Natural man-made disasters.

All of the five challenges listed in the EU security strategy are included in the top ranking perceived challenges of the citizens as shown in the figures below.

What do you think are the most important challenges to the security of (NATIONALITY) citizens at the moment?

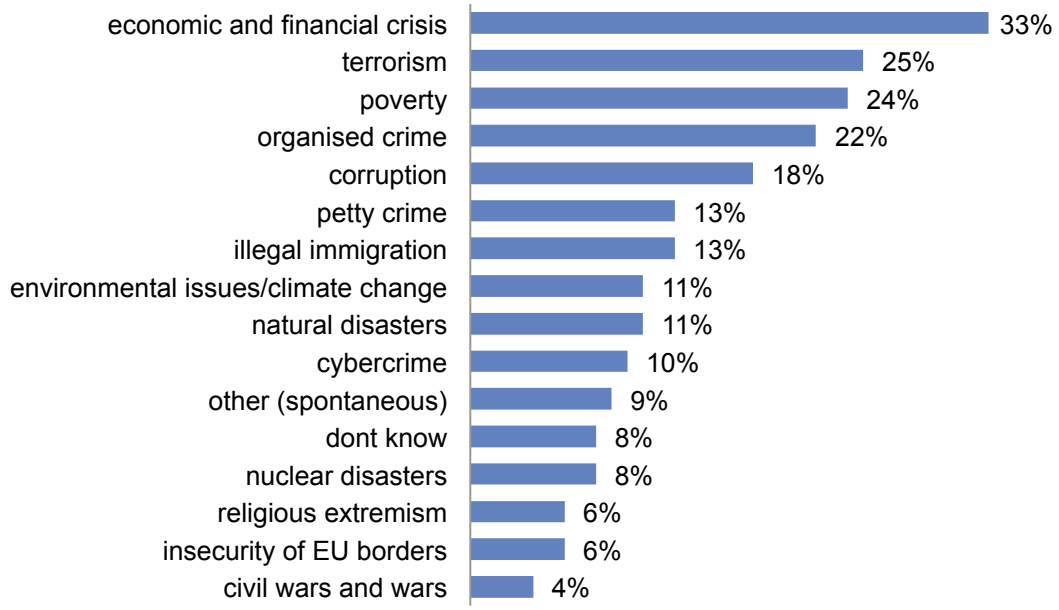

Figure 1: Europeans' views on challenges to national security

[57] European Commission (2010). Communication from the Commission to the European Parliament and the Council - The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. Brussels. Op. cit.

What do you think are the most important challenges to the security of EU citizens at the moment?

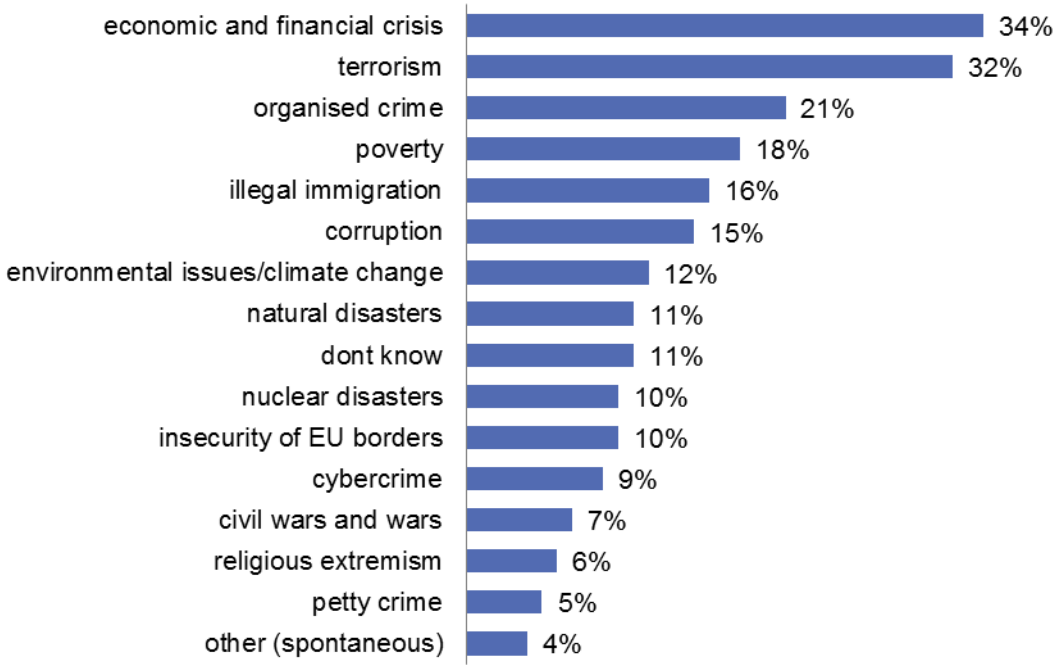

Figure 2:Europeans' views on challenges to EU security

The challenges regarded as most relevant for national and EU security by the citizens are, however, not among the priority challenges included in this Communication from the Commission. The economic and financial crisis is rated first from both, the national and the EU perspective, and also poverty and corruption belong to the most important challenges. Issues about the environment and climate change are together 22% and play an increasing role in EU member states. Notable differences in the viewpoints are that from an EU perspective illegal immigration, which can be linked to border security, is slightly gaining in importance and moving from the seventh to fifth position, whereas petty crime is losing relevance, shifting from the sixth to the 14th position.

The dominance of economic challenges, in line with the experts' assessment in the Global Risk Report 2012, is confirmed by data from open surveys, which provide data over longer periods of time. The graphs below show an overview of the ten most important issues from the EU citizens' point of view in 2003, 2008 and 2012.[58]

[58] The chart is based on the responses to the question "What do you think are the two most important issues facing (OUR COUNTRY) at the moment? (MAX. 2 ANSWERS POSSIBLE)" from the Eurobarometer Trends question database. The presented issues are the ten highest ranked based on their average percentage value during the whole period from 2003 to 2012.

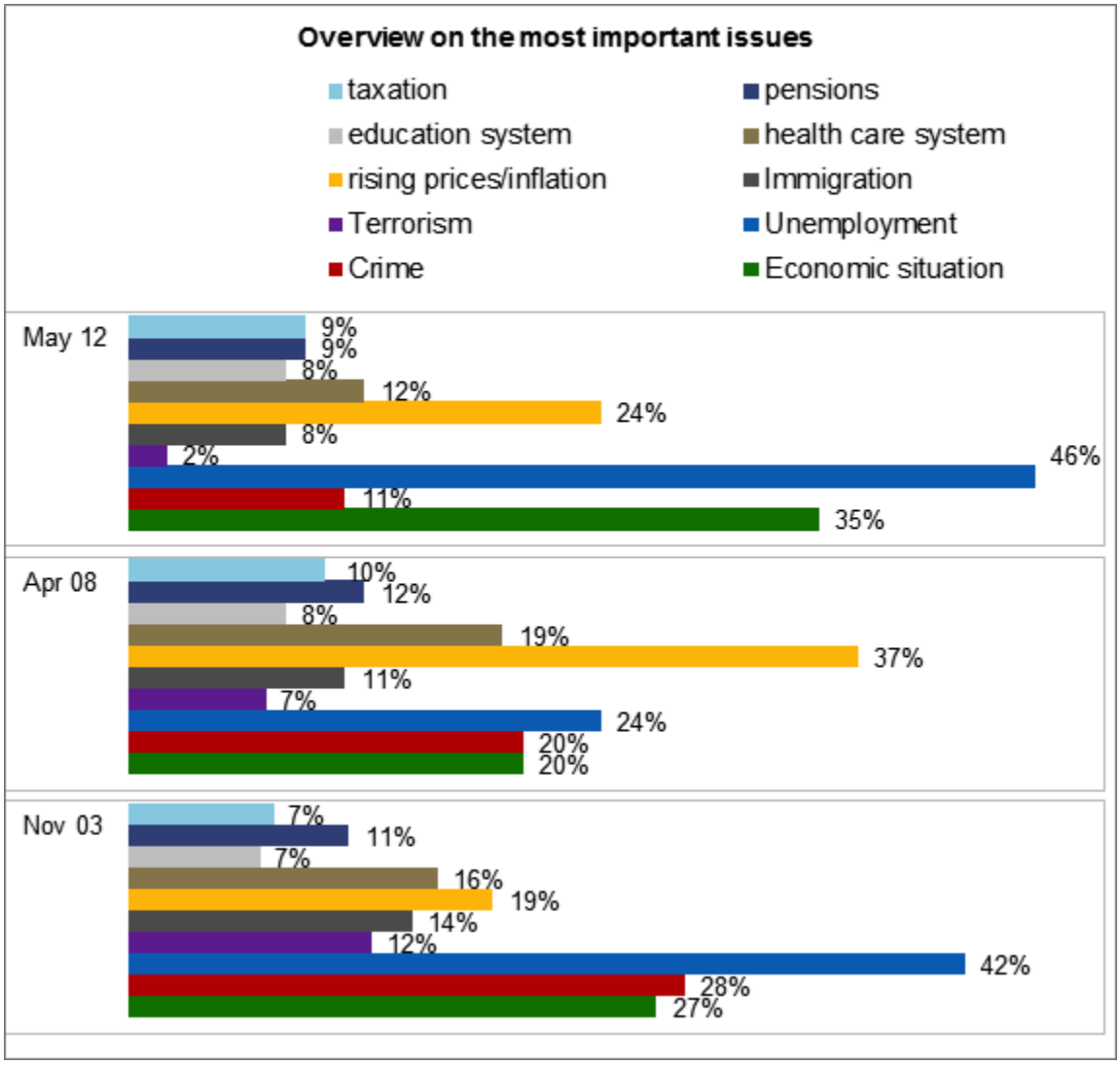

Figure 3: Europeans' views on most important issues[59]

Issues that are related to social security such as education, health care, pensions and taxation are relatively stable. Compared to that, issues that refer to internal security such as crime and terrorism are fluctuating; while the fluctuation range of economic issues is somewhat similar, economic aspects and unemployment seem relatively constant in their importance. The next figure gives a more detailed picture of the changing priorities of these varying issues from a long-term perspective that confirms this assumption.

[59] Based on the Eurobarometer Interactive Search System results http://ec.europa.eu/public_opinion/cf/index.cfm?lang=en

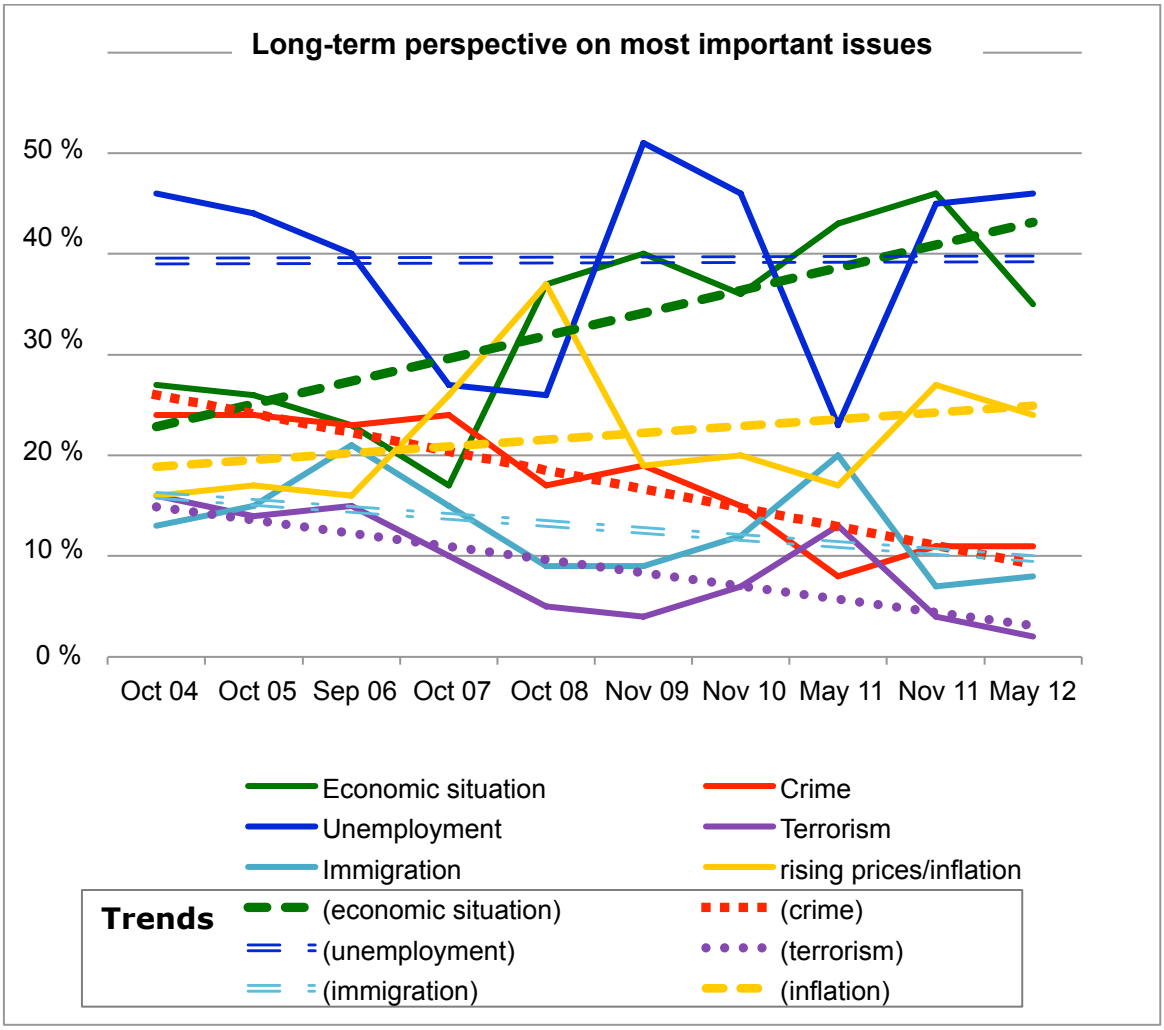

Figure 4: Progress of Europeans' perceptions on security and economic issues [60]

According to these time series, crime and terrorism have always been relevant issues in the medium range but with a fluctuation downwards. Crime has considerably lost in importance (from 28 to about 8%), terrorism is moving up and down between 5 to 15%; a rather similar development shows immigration, moving in the range between 10 to 20%. However, economic issues such as the state of the economic situation (always being approximately in the range between 20 and 40%) or the levels of unemployment (in the range between 25 and 50%) were continuously assessed as more important than terrorism. A comparison of the trend curves over the years clearly indicates a decrease of concerns regarding terrorism and crime (the dotted lines) while economic issues are increasingly problematic in the perception of the EU citizens.

This points out a particular need to take into account the wider economic and societal in policy; firstly because concerns in this regard are of top priority for European citizens, secondly, because neglecting them might lead to further economic and societal instabilities. Whereas economic and social policies as such are beyond the scope of SurPRISE, not addressing the importance of taking a global and comprehensive approach to security challenges favours a unilateral dependence on "end-of-pipe security measures" with all the entailed threats to human rights in general and privacy in particular. Here the long-term consequences are more serious than straight relationships like to petty crime. Migration,

[60] Based on the Eurobarometer Interactive Search System results http://ec.europa.eu/public_opinion/cf/index.cfm?lang=en.

although not a security problem in itself is associated with illegal or undocumented immigration and with border security technologies to prevent such entries, is strongly related to cultural/religious, economic and political factors causing insecurities and pressures of emigration. Financial and economic instabilities, as they are currently spreading throughout Europe, can also be related to surveillance technologies, e.g. by creating the need to apply crowd control technologies to combat riots due to poverty or unemployment.

When comparing the different views (EU policy, experts and citizens as outlined in this section) one might perceive a mismatch: EU security research puts strong emphasis on technological solutions in each security domain as well as on human-related threats to fight crime and terrorism; this is to some extent in contrast to the main concerns of citizens and experts, which would suggest a strong focus on economic and social measures to address security issues. In particular, the expert assessment seems to prioritize issues of protecting society and humanity from harm by addressing domains that are essential for the functioning of a society: such as maintenance of services of general public interest, e.g. domains of public services, infrastructures, etc.

Such a mismatch might suggest a demand for refocusing EU security research on current challenges incorporating citizens' and experts' views, leaving the relatively stable path followed in the last decade. From early reports (Research for a Secure Europe. Report of the Group of Personalities in the field of Security Research[61]), over the reports from ESRAB[62] report and ESRIF[63] the list of main mission areas remained by and large unchanged.

3.4 Major policy issues on privacy and data protection

While the previous chapters dealt with security challenges, this section provides an overview of major privacy challenges to point out that SOSTs are not to be seen merely as responses to security challenges but that privacy concerns are directly and indirectly related to technology-based security measures. This is of particular relevance to grasp the implications of the different forms of security measures and the selected SOSTs on privacy and other fundamental rights more in depth.

While technology is perceived as the best-fitting solution to implement security measures, on the other hand, there is an increasing number of privacy challenges linked to these choices. A relevant indicator is the number of prior checks[64] regarding processing of personal data that drastically increases as the authority in charge, the European Data Protection Supervisor (EDPS) points out in its annual report.[65] Furthermore, the EDPS also noticed a relatively constant growth in the number of complaints regarding privacy and data protection issues. Besides handling the growing amount of privacy complaints in particular cases, the EDPS also deals with requests from the public on different privacy issues that are important as regards raising awareness on these issues.

The growing number of requests on privacy and data protection and the variety of different issues give some hints on public concerns in this regard. Such requests come from a wide range of different individuals and institutions ranging from stakeholders in a European context involved in privacy (e.g. law firms, NGOs, associations, universities, etc.) to citizens asking for support in privacy issues and

---

61 European Communities (2004). Research for a Secure Europe. Report of the Group of Personalities in the field of Security Research. Office for Official Publications of the European Communities. Luxembourg. http://ec.europa.eu/enterprise/policies/security/files/doc/gop_en.pdf

62 Report from the European Security Research Advisory Board - Meeting the challenge: the European Security Research Agenda (September 2006) http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf

63 ESRIF (European Security Research and Innovation Forum) (2009). ESRIF Final Report. http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf

64 Prior checks are among the main tasks of the EDPS. It is legally defined in Regulation (EC) No 45/2001 providing that all processing operations likely to present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes are to be subject to prior checking by the EDPS (Article 27(1)).

65 European Data Protection Supervisor - EDPS (2012): Annual Report 2011 of the European Data Protection Supervisor. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2011/AR2011_EN.pdf

problems. Issues of increasing concern include online privacy, international data transfer, biometric data, large-scale IT systems (such as SIS, Eurodac, etc.), data retention and the EU data protection regulation. This situation underlines the increasing demand in assistance and informed advice among the wider public.

Privacy concerns in the Area of Freedom, Security and Justice (AFSJ)

As the EDPS highlights, questions of necessity of measures in the ASFJ have been a recurrent theme. Particularly as regards: the European Data Retention Directive, the communication on migration and the proposal for an EU Passenger Name Records (PNR) Programme. The EDPS issued its opinion on these developments and underlined that "[n]ecessity is a key concept in data protection. It is a strict rather than simply 'useful' standard: A measure can only be considered necessary if the results could not have been achieved with less intrusive means. Especially when evaluating existing measures, this standard must be applied with utmost rigour. This standard of proof is enshrined in European law and has been applied extensively by the Court of Justice of the European Union in Luxembourg as well as by the European Court for Human Rights in Strasbourg, usually closely linked to the standard of proportionality."[66]

In case of the European Data Retention Directive (2006/24/EC) the EDPS comes to the conclusion that it "does not meet the requirements imposed by the fundamental rights to privacy and data protection for the following reasons:

- The necessity for data retention provided for in the Directive has not been sufficiently demonstrated;
- Data retention could have been regulated in a less privacy-intrusive way;
- The Directive leaves too much scope for Member States to decide on the purposes for which the data might be used and for determining who can access the data and under which conditions."[67]

Addressing the EU Commission's approach to migration, the EDPS inter alia commented on the new instruments such as the Entry-Exit-System and argued for a "need to prove the necessity" of these instruments. He referred to the "standard of proof needed to interfere with the right to privacy and data protection" which is "'being necessary in a democratic society'" established by the European Court of Human Rights and the European Court of Justice.[68]

Further comments addressed the use of biometrics which are related to the issue of migration (e.g .in border control): The EDPS urged that "any use of biometrics should be accompanied by strict safeguards and complemented by a fall-back procedure for persons whose biometric characteristics may not be readable." In relation to this the EDPS also called on the European Commission, "not to reintroduce the proposal to grant law-enforcement access to Eurodac"[69].

As regards PNR, the EDPS stated that "the need to collect or store massive amounts of personal information must rely on a clear demonstration of the relationship between use and result (necessity principle). This is an essential prerequisite for any development of a PNR scheme. In the view of the EDPS, the current acts failed to demonstrate the necessity and the proportionality of a system involving large-scale collection of PNR data for the purpose of a systematic assessment of all passengers."[70]

These opinions highlight the need for including impact assessments of privacy and other fundamental rights into security policy and the process of deciding on security measures. The developments in the AFSJ show an increasing employment of security technologies and to some extent also a conflation

---

66 EDPS (2012) op. cit. p. 44

67 Ibd p. 48

68 Ibd p. 52

69 One of the achievements of the EDPS in 2011 was an inspection on advance deletion in Eurodac to improve privacy and data quality which are core problems here. Eurodac is currently under reform and a reintroduction of this proposal would raise proneness to errors (such as false positives). (cf. EDPS 2012, p. 70).

70 Ibd p. 50

between those technologies such as the pre-emptive retention of data, the collection and storage of biometrics in different databases and the increasing data exchange and interlinkage of different information systems (such as the PNR system, Eurodac, etc.).

The technological developments can be expected to boost already existing privacy challenges as well as triggering new ones. Among the pressing issues that deserve priority as regards privacy challenges and policy considerations, the EDPS refers to further developing the AFSJ and a variety of technology developments such as smart mobile devices and developments in cyberspace that are on the Digital Agenda such as internet monitoring/profiling.

In its working programme for 2012 to 2013, the Article 29 Data Protection Working Party[71] sets similar priorities. Among the technological challenges and issues with respect to their impacts on privacy are biometrics such as facial recognition, different kinds of tracking technologies, mobile computing (e.g. smartphone apps). The Working Party also focuses on a coherent and effective approach for privacy protection in the AFSJ and its different information systems that also entail increasing data exchange among authorities.[72]

3.5 Privacy concerns of citizens

The attitudes of citizens in Europe on privacy and data protection issues mirror the linkage between technological progress and privacy concerns as the results from a special Eurobarometer survey of 2011[73] reveal. Together with a further growth in the use of ICTs and online media, citizens also perceive that they are increasingly obliged to give away personal information. This development in general is seen as worrying trend.

The chart below shows to what extent European citizens perceive different kinds of information as private (in blue, lined) and which of these information they have already disclosed by using online social media (in red, dotted):

[71] The Article 29 Working Party is set up under Art. 29 of the Data Protection Directive (95(46/EC) the independent advisory body for the European Commission on privacy and data protection issues.

[72] Article 29 Data Protection Working Party: Work programme 2012-2013 00381/12/EN, WP 190, February 2012 http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

[73] European Commission (2011): Special Eurobarometer 359 Attitudes on Data Protection and Electronic Identity in the European Union. June 2011. Survey requested by the Directorate-General Information Society and Media (INFSO), the Directorate-General Justice (JUST) and the Directorate-General JRC and co-ordinated by the Directorate-General Communication ("Research and Speech Writing" Unit) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

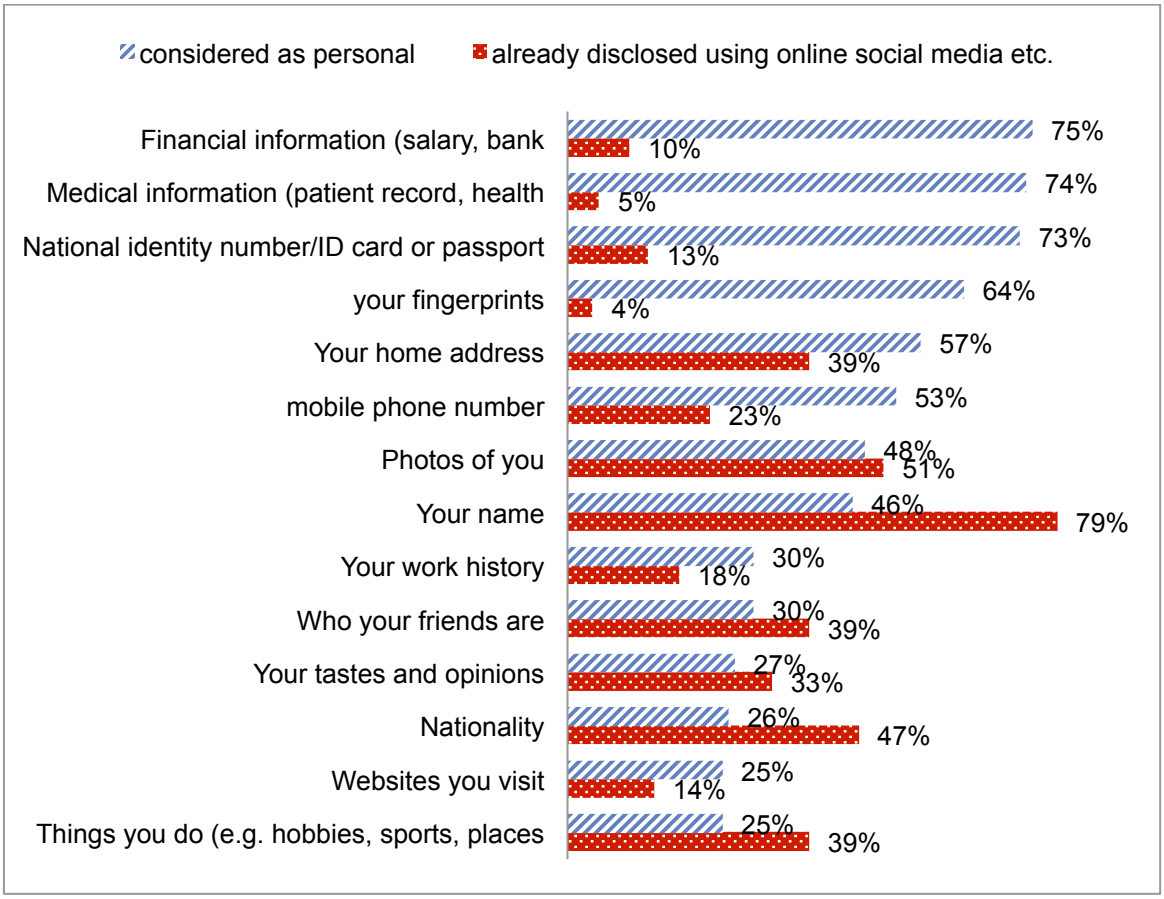

Figure 5: Perceptions of personal information and amount of disclosure due to online social media usage[74]

As shown, financial, medical information and information linked to the identity such as national ID or passport number are highest ranked as being personal. Being asked also directly on the perceived sensitivity of medical data, the vast majority of the respondents (almost 90%) wants special protection for genetic information such as DNA data.

According to these results the respondents seem to differentiate from their perception on the sensitivity of information and also to what extent information is perceived as directly linked or linkable to a particular person. This is one explanation for the low ranking of website visits as respondents might not be aware that it is linkable. The types of information already disclosed (in red) mainly correspond to the different levels of personal information. These figures also highlight an increasing difficulty of individuals to protect their personal information as further results reveal. About 50% of the European citizens have the impression that it is hardly avoidable to disclose personal information on the internet. Social media plays a significant role in this regard as shown above.

Regarding the interviewees' perception of the necessity to disclosing personal information, 74% share the opinion that disclosure of personal information is an increasing part of modern life. For the clear majority of over 60% personal information disclosure is a big issue. 64% of the respondents totally agree that the government asks for more and more personal information. About 60% of the respondents see no alternative to disclosing information in relation to obtaining products and services. Almost 30% even feel obliged to disclose personal information on the internet. More than half of the interviewees do not agree that disclosing information is justified by getting services for free.

[74] The chart is based on the responses to the questions "Which of the following types of information and data that are related to you do you consider as personal?" and "Thinking of your usage of social media and sharing sites, which of the following types of information have you already disclosed (when you registered, or simply when using these websites)?" from the special Eurobarometer 359 (2011).

The main reason among respondents for disclosing personal information is to gain access to a service. In case of social media 60% of the interviewees name this as the main reason, and in the case of online shopping as many as 80% state the same. Being asked about over-disclosure, half or nearly the half of SNS users and online shoppers have already been exposed to reveal more personal information than necessary as it was required to use a service. More than 70% of those feel (very or fairly) concerned about such cases where more information is required than is necessary.

When asked directly about profiling on the internet by advertisers and others over 50% of internet users are concerned about profiling activities even though the question was linked to positive effects such as free services. There is also a variety of concerns among the respondents about the monitoring/recording of their behavior.

Nowadays, cameras, cards and websites record your behaviour, for a range of reasons. Are you very concerned, fairly concerned, not very concerned or not at all concerned about your behaviour being recorded?

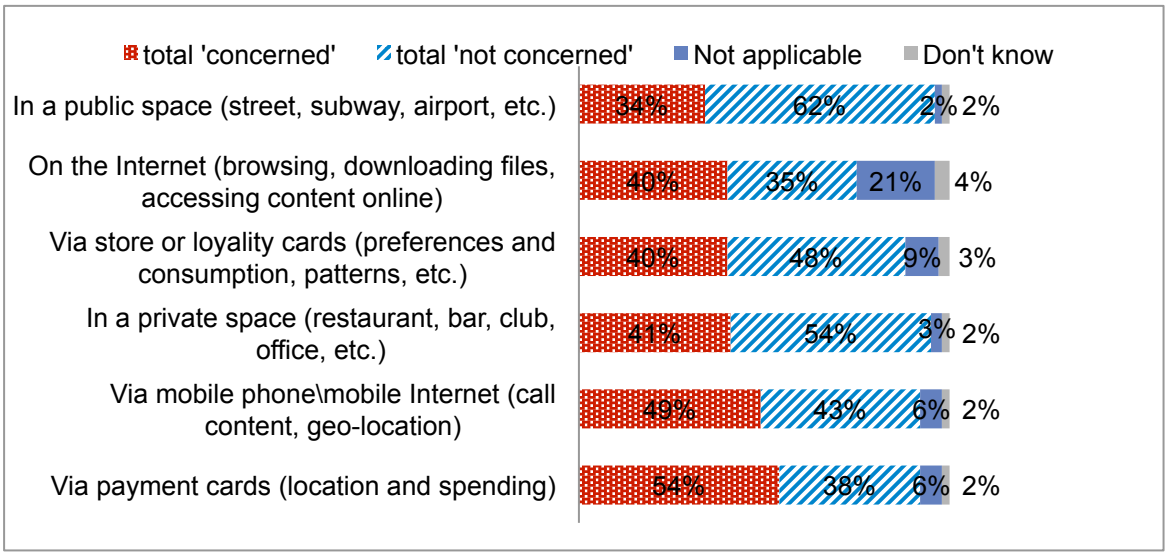

Figure 6: Citizens' concerns on profiling activities

About half of the interviewees are concerned about their behavior being monitored via payment cards (location and spending) and about being tracked via their mobile phone or mobile internet usage (such as call content or geo-location). Four out of ten respondents are worried about behavioral tracking on the internet. Excluding those who answered with "not applicable" (21%) and are non-internet users, the absolute majority of the respondents (51%) is worried about their behavior being tracked on the internet. These results underline that the wide diffusion of ICTs and not least of mobile devices such as smart phones or tablet PCs reinforces existing and emerging privacy concerns.

The growing privacy concerns represent an increasing demand for more effective mechanisms to protect personal information and control its proper usage. The survey results refer to the importance of a shared responsibility in this regard. Three-quarters of European internet users see their own responsibility for the safe handling of personal information but also perceive demand for more responsible treatment of their data by online sites. Nine out of ten Europeans are in favor of a harmonized approach for privacy regulation across the EU. 75% would like to have more control and are in preference of a right to be forgotten to induce deletion of their personal information whenever they decide so. As regards awareness on the existence of a national public authority in charge of protecting their rights regarding their personal data only one-third of the Europeans is aware about the existence of such an authority, while 63% are not. As regards trust in proper handling of personal data, public authorities and institutions such as the European Commission and the European Parliament (55%) are trusted somewhat more than private organisations such as commercial companies. 70% have concerns

about their personal data held by companies may be used for a purpose other than that for which it was collected.

Attitudes on police accessing personal data are rather ambivalent. Being asked about the circumstances in which the police should be able to access personal data of individuals, 33% agreed on such an access in case of usual measures for preventing crime. 37% answered that this should only be allowed for specific data within a specific investigation, 26% would only allow this if a judge is involved to decide on accessing these data. These results reflect the general awareness on citizens about the relevance of personal data for law enforcement and the controversial aspects related. While the survey did not ask whether prevention should be limited or dependent on judicial decision, with 63% the clear majority endorses a cautious and prudent approach and neglects access without limits or explicit judicial checks and balances.

The issues and concerns described refer to some crucial issues and challenges in privacy policy. The wide-spread use of ICT and their continuing diffusion reinforces privacy impacts in several ways. Citizens are increasingly concerned by their personal information being processed by ICT. The growing amount of requests about privacy issues brought to data protection authorities and the lack of information among European citizens on DPAs and privacy regulation in general highlight the need for more transparency and the unexploited potential to raise public awareness. Thus, the incorporation of citizens perceptions as conducted in the SurPRISE setting can also be seen as a contribution to reduce this gap. While citizens already encounter a quasi-necessity to disclose personal information, the increasing availability of this information also attracts different kinds of observers or what some scholars termed the "surveillant assemblage"[75]. Thus the citizens' perceived lack of control over their personal information flows and privacy concerns become intensified by different forms of technology-supported profiling and surveillance activities.

[75] See K. D. Haggerty and R. V. Ericson (2000): "The surveillant assemblage". In: British Journal of Sociology Vol. 51(4) December 2000, pp. 605-622. Also Cohen, J. E. (2008) 'Privacy, Visibility, Transparency, and Exposure', *University of Chicago Law Review*, 75/1: 181-201

4 The interrelations between privacy, security and surveillance

The use of security technology is mostly associated with surveillance and interventions into privacy. However, this is not given in any case. Surveillance is a controversial and complex issue and does not necessarily represent the very antagonist to privacy; at the same time, privacy is not and "was never meant to be the 'antidote to surveillance'" as Bennett (2011) points out.[76] There are a variety of security technologies without direct privacy impacts such as luggage scanners aiming at detecting weapons or explosives do not necessarily affect the privacy of the individual carrying that luggage in a direct way.[77] While technologies such as CCTV or different forms of technology-supported profiling and surveillance activities mostly do. In the context of SurPRISE, those technology-supported security measures are of particular interest that entail a certain impact on privacy; also to elaborate on possible alternatives to reduce privacy impacts and entailed risks of infringement. This section describes the role that privacy plays and the different types and dimensions of privacy in relation to security and surveillance as the interplay of these issues is at the core of SurPRISE. First, a short overview on the main legal aspects outlines the relation on security and privacy; then the different types and dimensions of privacy as well as a process-oriented perspective are described. These conceptualisations build the basis for the selection process of the SOSTs in section 5, ensuring that the final selection provide a mix of privacy types and privacy affecting activities.

The degree and kinds of privacy impact triggered by security technologies, practices and measures not least depends on the amount of interference into an individuals' private sphere by the different modes of observation and/or control applied. Or in other words: the level of direct intrusiveness, i.e., to what extent an individual is subject to surveillance (as part of a security action), comprising a sort of interference into one's privacy.

The term surveillance derives from the French *surveiller* – "to watch over", may simply refer to the "continuous observation of a person or area" as well as to the "close and continuous observation for the purpose of direction, supervision, or control".[78] The second meaning extends the implications of the concept to several areas of human activity as it might entail some kind of manipulation or redirection of the behaviour of the observed agent. Surveillance can be understood as a security practice that "comprises the targeted or systematic monitoring, by governmental organisations and their partners, of persons, places, items, infrastructures or flows of information, in order to identify hazards and manage risks and to enable, typically, a preventive, protective or reactive response, or the collection of data for preparing such a response in the future."[79] This is particular the case in the realm of technology where surveillance is related to a wide array of objectives. The use of surveillance technologies covers a broad spectrum ranging from search and rescue operations; customs and immigration checks; the protection of natural resources; uncovering illegal activities such as drug manufacture and distribution; as well as military reconnaissance and targeting operations.[80] These domains are without any doubt essential for providing security. However, surveillance is also a means of control and -- referring to Foucault[81] -- a form of disciplinary power. And as such it is capable of drastically delimiting or even taking away one's control over her very own private sphere. From this view, surveillance represents a sort of pivot between security and privacy. This relationship is used as a guideline to inspire the selection of SOSTs: if a (technology-supported) security practice includes surveillance then it is likely to affect privacy. Thus, the

---

[76] C. J. Bennett (2011): "In Defence of Privacy: The concept and the regime". In: Surveillance & Society 8(4): 485-496.

[77] However, also in this case depending on the employment as also the screening of personal belongings can lead to discrimination, e.g. http://www.huffingtonpost.ca/clay-nikiforuk/sexism-at-us-border_b_3112638.html

[78] Merriam Webster Unabridged Online Dictionary. URL: http://unabridged.merriam-webster.com/cgi-bin/unabridged?va=surveillance

[79] This definition of surveillance is based on the (SURVEILLE Project Consortium, 2011), p. 46, as modified for the purposes of SURPRISE. See also SurPRISE Deliverable 3.2, M. G. Porcedda, M. Scheinin, M. Vermeulen (2013): D3.2 – "Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy".

[80] Petersen, J. K. (2007). Introduction & Overview. Understanding Surveillance Technologies: Spy Devices, Privacy, History & Applications, Second Edition. Boca Raton, Auerbach Publications: 3-101.

[81] M. Foucault 1977: Discipline and Punish: the birth of the prison, trans. A Sheridan, London: Penguin.

degree of privacy interference is related to the surveillance activities employed in relation to a security measurement. This also addresses different modes of surveillance, i.e. a distinction between factual and pre-emptive forms of observation that refers to the interrelations between pre-emptive state mechanisms for crime prevention and privacy impacts.[82]

It seems plausible, in accordance with existing literature in surveillance studies to expect that pre-emptive security measures and technologies may receive lower public acceptance due to the lack of concrete focus on security threats. For instance, body scanners aim at detecting direct factual threats like weapons and explosives, or at least at a perceivable threat. In contrast, security measures and technologies based on the pre-emptive concept of security, such as cyber-surveillance of internet activity or the use of spyware to track and collect information in the individuals very private domain, may be much more controversial and less acceptable for the wider public. Both examples have a certain amount of privacy impact, but while the former addresses a perceivable threat, the latter also intends to prevent potential and undefined threats before they actually become a threat. The different modes of surveillance used as part of a security measure thus might affect different types of privacy. The next sections deal with privacy interference first by outlining legal norms and then by describing different types and dimensions of privacy.

4.1 Overview on legal norms defining the relation between security and privacy[83]

Both, privacy and security are part of the legal frameworks for Human Rights. Like every other human right, neither security nor privacy are absolute rights but always have to be seen in relation to the broader public interest. The very aim is to come to a "fair balance between the demands of the general interest of the community and the requirements of the individual's fundamental rights."[84] The following legal terms are essential building blocks of privacy and security.

Legal terms for right to privacy:

Article 8 of the European Convention on Human Rights (ECHR):

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.

According to **Article 12[85] of the Universal Declaration of Human Rights (UDHR)**,

"[n]o one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."

https://www.un.org/en/documents/udhr/

[82] As explored by a number of scholars from the field of surveillance studies cf. D. Lyon (2001): Surveillance Society: Monitoring Everyday Life, Oxford, University Press; D. Lyon (ed.) (2003): Surveillance as social sorting: privacy, risk and digital discrimination. Routledge; C. Bennett, K. Haggerty (eds.) (2011): Security Games: Surveillance and Control at Mega-Events. Routledge. K. Ball, Haggerty and D. Lyon (eds.) (2012): Handbook on surveillance studies. Routledge.

[83] For an in-depth analysis of legal aspects see WP3, SurPRISE D3.2: M. G. Porcedda, M. Scheinin, M. Vermeulen (2013): D3.2 – "Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy".

[84] Ursula Kilkelly (2003): The right to respect for private and family life – a guide to the implementation of Article 8 of the European Convention on Human Rights. Human Rights Handbooks No. 1, Directorate General of Human Rights, Council of Europe, Strassbourg, 2003 http://echr.coe.int/NR/rdonlyres/77A6BD48-CD95-4CFF-BAB4-ECB974C5BD15/0/DG2ENHRHAND012003.pdf

[85] Similar is Art. 17 of the UN Covenant of Civil and Political Rights, http://www.hrweb.org/legal/cpr.html

As shown above, limitations to privacy always must be in accordance with the law and (referring to the principle of proportionality and commensurability) only if necessary in a democratic society. In general, the right to privacy includes freedom from interference and aims at protecting against infringement from government or other institutions. This refers to liberty as predominating right in a democratic society. It thus is no coincidence that the right to security is always subordinated to the right to liberty or freedom:

Legal terms for the right to security:

Art. 5 ECHR: *"Everyone has the right to liberty and security of person. No one shall be deprived of his liberty (…)"*[86].

Article 3 UDHR:[87] *"Everyone has the right to liberty and security of person."*

Article 29 UDHR:

2. In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.

As those legal norms show, interference of privacy by security actions is only allowed to fulfill public interest and must be in accordance with the law and necessary in a democratic society to protect its foundations. Thus, privacy interference is by no means defined as permanent but always as the exception from the rule so to speak; While as a norm, privacy defines a state where an individual is free from interference from the institutions (both state and others). Assuming that fostering security would always entail a trading of privacy is thus misleading as it wrongly frames security as privacy interference without assessing alternative options. To its end such an assumption would raise the exception from the rule to the norm, (i.e. privacy interference as per se necessary for security).

Against this background, a trade-off model based on this assumption that privacy has to be weighed against security holds the danger to neglect that security is subordinate to liberty and liberty is the superior linkage between both – privacy and security. The prominent role of liberty and freedom in the legal frameworks is thus no coincidence but underlines this aspect.[88]

4.2 Types and dimensions of privacy

Privacy has many different types and dimensions. The most common notion of privacy is the classical definition as "the right to be left alone"[89]. Westin (1967) defined privacy as "the claim of individuals, groups or institutions to determine for themselves, when, how, and to what extent information is communicated to others." [90]

Privacy is not to be misunderstood as an individuals' right to decouple from society. On the contrary it relieves from different kinds of social frictions and is a societal achievement that "enables people to engage in worthwhile activities that they would otherwise find difficult or impossible"[91]. Privacy is thus

[86] This right includes the right to be protected from unlawful detention, i.e. due to lack of sufficient cause or evidence.

[87] Similar Art. 9 of the UN Covenant of Civil and Political Rights, http://www.hrweb.org/legal/cpr.html

[88] For a legal (US-based) discussion on the roles of so-called "preferred freedoms" to ensure a social and democratic state of law, see The Oxford Companion to the Supreme Court of the United States, 2nd edition, K. L. Hall (ed.), Oxford University Press, New York, 2012.

[89] S. D. Warren and L. D. Braneis (1890): "The Right to Privacy". In: Harvard Law Review 193 (1890) Vol. IV Dec. 15 1890, No. 5 http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm

[90] A. Westin (1967): Privacy and freedom. Atheneum, New York.

[91] D. Solove (2006): "a taxonomy of privacy". In: University of Pennsylvania Law Review". Vol. 154 (3). Pp. 477-560. p. 484

also a substantial enabler of individual involvement in society, and harms to privacy "affect the nature of society and impede individual activities that contribute to the greater social good"[92].

To substantiate to what extent privacy is effective and can be affected, several scholars distinguish different types of privacy. This is not least important as different kinds of technology today entail several types of (potential and real) privacy infringements. With the rapid development of technologies and applied techniques it becomes further complicated to identify which types and dimensions of privacy are intruded by a particular technology. Also the boundaries between the different types are more and more diminishing.

Clarke provides a valuable classification in four major types of privacy: privacy of the person, privacy of personal behaviour, privacy of social communications and privacy of personal data. The first type of privacy makes reference to what is also known as bodily privacy, and aims at protecting the physical space and the body of a person. The second type of privacy aims at safeguarding the personal behaviour of individuals, such as for instance including religious practices and sexual activities. The third type of privacy somewhat covers the set of relationships and social ties that any individual builds and operates in. Finally, the privacy of personal data refers to the integrity and protection of all the sensitive data possessed by an individual.

Clarke definition of Privacy (http://www.rogerclarke.com/DV/Privacy.html)

Privacy of the Person, sometimes referred to as 'bodily privacy', is concerned with the integrity of the individual's body, and is related to the Physiological and Safety levels of the Maslowian hierarchy. At its broadest, it could be interpreted as extending to freedom from torture and right to medical treatment, but these are more commonly seen as human rights rather than as aspects of privacy. Issues that are more readily associated with privacy include compulsory immunization, imposed treatments such as lobotomy and sterilization, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and requirements for submission to biometric measurement.

Privacy of Personal Behavior, including what is sometimes referred to as 'media privacy', is related to both the Belonging and Self-Esteem levels of Maslow's hierarchy, and perhaps to Self-Actualization as well. Many issues that come to attention relate to sensitive matters, such as sexual preferences and habits, political activities and religious practices. But the notion of 'private space' is vital to all aspects of behavior, is relevant in 'private places' such as the home and toilet cubicle, and is also relevant in 'public places', where casual observation by the few people in the vicinity is very different from systematic observation and the recording of images and sounds.

Privacy of Personal Communications, including what is sometimes referred to as 'interception privacy', is also related to both the Belonging and Self-Esteem levels of Maslow's hierarchy, and perhaps to Self-Actualization as well. Individuals desire the freedom to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organizations. Issues include mail 'covers', use of directional microphones and 'bugs' with or without recording apparatus, telephonic interception and recording, and third-party access to email-messages.

Privacy of Personal Data, sometimes referred to as 'data privacy' and 'information privacy', is again related to the upper layers of Maslow's hierarchy. Individuals claim that data about themselves should not be automatically available to other individuals and organizations, 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. The last five decades have seen the application of information technologies to a vast array of abuses of data privacy (e.g. Clarke 1988, 2003).

[92] Ibd, p. 488

Mobile computing and ICT-supported mobility refer to a further privacy type:

Locational privacy: The increasing relevance of mobile devices such as smart phones and the particular nature of location data entail a wide array of additional modes of surveillance to track individual location and movements. Blumberg & Eckersley 2009) define locational privacy as "the ability of an individual to move in public space with the expectation that under normal circumstances their location will not be systematically and secretly recorded for later use"[93]. Adding aspects of control it can be described as "the interest an individual has in controlling information about their sequence of locations"[94].

In their classification, Finn et al (2013)[95] provide an extended approach. They complement additional dimensions to Clarke's typology and name seven types of privacy:

(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.

(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".

(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.

(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.

(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).

(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

[93] A.J. Blumberg & P. Eckersley (2009) 'On locational privacy, and how to avoid losing it forever' Electronic Frontier Foundation, August 2009, at https://www.eff.org/wp/locational-privacy

[94] R. Clarke 2012: Location tracking of mobile devices: Ueberveillance stalks the streets. http://www.rogerclarke.com/DV/LTMD.html

[95] Rachel L. Finn, David Wright, and Michael Friedewald (2013) "Seven Types of Privacy" in Gutwirth, S.; Leenes, R.; de Hert, P.; Poullet, Y. (Eds.), "European Data Protection: Coming of Age", Chapter 1, Dordrecht: Springer. DOI 10.1007/978-94-007-5170-5_1.

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.

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.

This typology allows to reconsider and reflect upon different kinds of SOSTs and their impinge on privacy and how particular SOSTs cross the boundaries between different privacy types. The most common technology that intrudes the privacy of the body is CCTV. Another recent and prominent example are body scanners at airports. With the combination of CCTV and a database for processing the images taken by the camera this technology also touches informational privacy. With the wider diffusion of „smart" CCTV, also behavioral privacy is affected. A further, very rather comprehensive example, capable of affecting all types of privacy is cyber-surveillance. Depending on its level of intrusion, it can be understood as a conglomerate of different intertwined privacy infringing actions that affects e.g. privacy of data, individual communication and behavior, thoughts and feelings, privacy of association.

4.3 A process-oriented view on privacy affecting activities

A different approach that emphasizes the privacy interference including modes of surveillance is provided by Solove (2006)[96]. His privacy taxonomy points out the interrelations between the different forms of privacy infringing actions. He distinguishes between four basic groups[97] of interrelated activities that are harmful to privacy:

- Information collection
- Information processing
- Information dissemination and
- Invasion

[96] D. Solove (2006) op. cit.

[97] Each of these consist of further subgroups. These are not discussed in detail here.

The figure below illustrates how these activities are related:

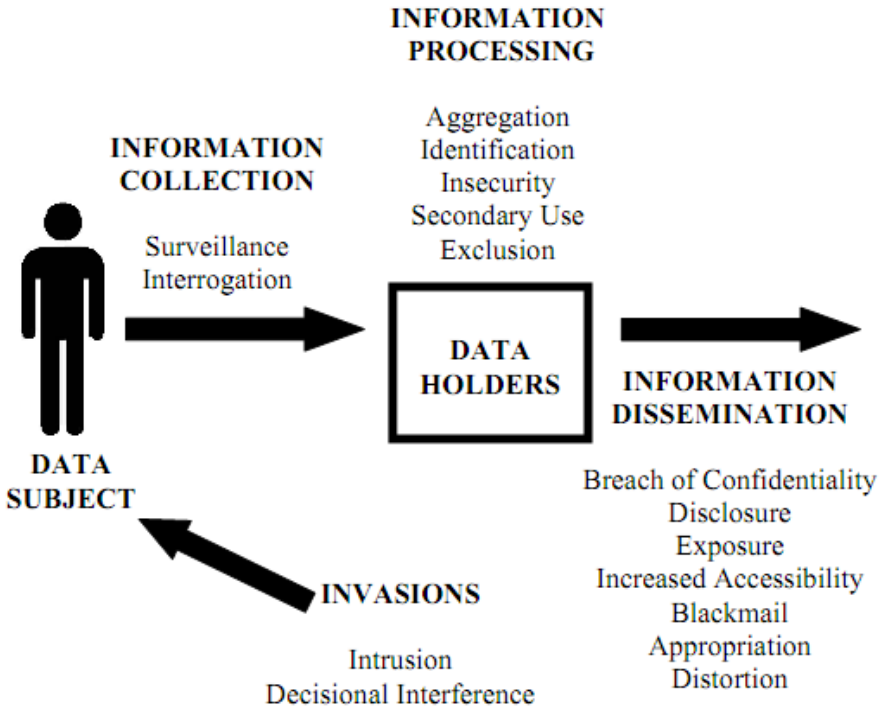

Figure 7: Groups of privacy affecting activities (Solove 2006, 490)

The model starts with the individual (data subject) whose privacy is affected by different activities. Information related to that individual is collected by various entities (e.g. government, business, other individuals). Surveillance is a subgroup which Solove here defines as "watching, listening to, or recording of an individual's activities"[98]. Interrogation means different forms of questioning or probing for information. The information collected by those entities is processed further. Once stored information opens up a broad scope of different forms of usage such as aggregation, search, manipulation, etc. Aggregation means the combination of various data about a person, identification here is linking information to a particular individual; with insecurity, Solove means the vulnerability of the stored information to leaks and improper access; secondary use addresses the problem of purpose extension without the concerned individuals consent; exclusion means that the individual is excluded from knowing and controlling how data is processed by whom, for what purpose etc.

The next group addresses different kinds of dissemination, i.e. that the information can also be released and transferred by the data holder to other parties. This includes a variety of subgroups: breach of confidentiality, disclosure, exposure, increased accessibility (here the problem that information is widely accessible without the data subjects control), blackmail (i.e. threating the individual to disclosure information), appropriation (i.e. the abuse of the individuals' identity for other purpose, e.g. identity theft) and distortion (i.e. spreading false or misleading information about individuals).

From information collection to processing and dissemination the information more and more moves away from the control of the individual. While the first three groups draw away the information from the individual and limiting his amount of control, the final group -- invasion involves direct impingements on the concerned individual and his or her private affairs. In this group information is not necessarily involved (though it is in several instances). Invasion activities interfere into one's tranquility or solitude.

[98] D. Solove (2006) op. cit. p. 490

Decisional interference means government's incursion into the individuals' decisions regarding private affairs. [99]

Soloves model provides a more process-oriented view on privacy affecting activities and mechanisms. It is a particular useful benchmark in the SurPRISE context as it allows to classify the different forms and roles of information gathering in relation to privacy intrusion. With its reference to the role of control it is also useful in considering different degrees of surveillance. For instance aggregation is the combination of already collected information while surveillance (at least in Soloves definition) is based on information collection. Thus, surveillance can be a process prior to aggregation of information. However, while the collection of some information might not be privacy infringing, linkage and aggregation with other information could trigger surveillance. Depending on how information is processed, surveillance can also be triggered by combining once separated information that is already existing. Surveillance-oriented techniques that are based on aggregation and linkage are pattern recognition, data mining to identify e.g. behavioral patterns, different kinds of de-anonymization techniques, DNA profiling such as anonymously collected medical records that become combined with other databases containing identity information, etc. While surveillance might already be part of information collection, the degree of surveillance can become fostered due to further processing (e.g. the storage and further processing of body scanner images, or the transfer of health records to law enforcement, etc.). The increasing amount of data exchange and interagency between security authorities (exemplified by police databases, such as Eurodac, SIS, DNA databases or other databases that process biometric data such as fingerprints[100]) refer to such a setting.

Solove's model together with Clarke's typology and the extended approach of Finn et al provide a valuable heuristic to substantiate the concept of privacy and its different types and dimensions. We used these approaches to specify the criteria and guidelines in the selection process for choosing which SOSTs to explore further in the SurPRISE setting. The number of privacy dimensions and types affected by a particular SOST is one major consideration in this regard. The following sections describe the selection process including the criteria and the final selection of SOSTs.

[99] Ibd pp.487-491

[100] Eurodac stands for European Dactyloscopy (fingerprint identification) and is a database containing fingerprints for identifying asylum seekers and illegal border-crossers. SIS is the Schengen Information System that is used for national security, law enforcement and border control across Europe. It aims at automated profiling of suspects. Schengen member states share and exchange information on individuals via SIS. A new and extended version - SIS II - is currently in development.

5 The selection process

This section describes the criteria for the selection of SOSTs. SurPRISE does not provide options to justify adopted, emerging or prospective security technologies but aims at gaining deeper insights into social, cultural and political factors affecting public acceptance and acceptability of existing and emerging security measures. Thus, the development of an innovative, participatory method to grasp different perceptions, opinions and informed contributions of citizens is a core part of the project (particularly in WP4 and 5). The SOSTs chosen in this Deliverable build the basis for developing the material for the participatory process in the further work packages. The central focus of SurPRISE lies on exploring the impacts of security measures along the threshold between privacy and security. As a consequence, a general selection criterion is to identify examples from different security domains that entail significant impact on privacy and/or other fundamental rights. From this basis, the number of security domains can be narrowed down as not every security challenge directly triggers privacy implications. For instance, securing infrastructures and utilities can be expected to have less privacy impact than for instance intelligent surveillance and border security. The protection of facilities and infrastructures through security technologies does not explicitly aim at observing and controlling individuals. Of course, this always depends on the concrete example taken, whether the protection of critical infrastructures does or does not directly imply privacy infringement. A further, related criterion is policy relevance; the selected SOSTs should represent one or more domains that are relevant in security policies, particularly in a European context. Frames, challenges, debates and responses to the challenges may vary across these different security domains. This is not least depending also on the national peculiarities within EU countries regarding the implementation of security technologies and practices. Different measures may be adopted at national levels, and the adoption of these measures may give raise to quite different issues and public debates, which may or may not filter up to the EU level. Therefore, based on EU security strategies and foci, the concrete implementation and related discourse of security measures on a national level (among those countries involved in the project) are also considered in the analysis (such as in Deliverable 2.2). This is also important in order to provide an adequate level of heterogeneity of those measures that will be evaluated by citizens along the project. A more in-depth revision of challenges, the current state of the art of SOSTs in general (Deliverable 3.1), the political and legal implications of privacy and security (Deliverable 3.2) and potential non-surveillance oriented alternatives (Deliverable 3.3) have been carried out in work package 3.

5.1 General typology of security measure

The degree of privacy infringement is an important guideline in the SurPRISE context to select a relevant spectrum of existing and emerging security technologies based on surveillance-oriented measures. Although a variety of such security measures exist that deeply affect privacy, one should be aware that non-technological, non-surveillance-oriented security measures do exist and often have been in place for years before being replaced by technological devices. Moreover, security challenges may be addressed through different responses, which may or may not involve surveillance and privacy infringements. Though not as part of this deliverable, exploring alternative approaches such as different forms of organizational measures that allow to address security challenges in a less-intrusive way is thus also an objective of SurPRISE. For instance, urban architectonic solutions may reduce criminal activity in given sensitive areas, neighbourhood-watch programmes and police deployment may also be effective under given circumstances, as well as urban planning concepts may increase security awareness and empower citizens in order to help them taking care of the their own safety.[101] Making comparison among these challenges and responses, within the same domain, may reveal interesting information to enlighten the comparison we make also across different domains. WP3 (and in particular Deliverable 3.3) also addresses alternative security concepts and gathering citizens' opinions on these alternatives is a core element of the participation process (WP5).

[101] Theories, concepts and approaches that can be taken into account as alternatives to SOSTs are discsussed in SurPRISE Deliverable 3.3: R. Berglenz, R. Kreissl (2013): "D3.3. Report on security enhancing options that are not based on surveillance technologies."

As described above, those SOSTs are of particular interest that are surveillance-oriented and affect different types of privacy. To come to an informed choice, several methods were conducted during the selection process. As a starting point we identified different general dimensions of a security measure. This allows us to narrow down the range of possible SOSTs.

The first important distinction we made to analyse responses to security challenges in this regard refers to the **degree of reliance on technological tools** and the technical solutions adopted. A certain preference toward technological-fix approaches has been increasingly characterizing European public policies over the years, the security field being certainly one of those areas where the race for technological innovation plays a particularly important role. Law enforcement has to keep pace with technological advances to understand, foresee and contrast criminal activity. Several technologies and techniques[102] are also constantly developed as potential solutions to new and old problems. A well-known example of the technical measures developed to tackle security challenges is represented by biometrics, which is used in several contexts as an identification method. However, security measures can also be very low-tech, but still effective in reshaping the organisational landscape. Crime prevention through environmental design is an example of a set of measures that enhance security without depending on sophisticated technology. Street lightening and correct definition of sidewalk routes can improve safety by simply diminishing the risks of becoming vulnerable to malicious attacks.[103]

The second element to be considered at the time of categorizing security measures is whether or not, and **to what extent, surveillance functionalities have been embedded** in the design or implementation of the measure. Closed-circuit television (CCTV) combined with abnormal behaviour and automatic face recognition is an example of a security measure whose functioning implies visual surveillance and identification of both behavioural characteristics and personal identity. The monitoring of the internet through deep packet inspection (DPI) is an example of a surveillance-oriented security measure that facilitates information surveillance. This technique enables, indeed, internet service providers (ISPs) and law enforcement officers to scan all data packets that pass through a network. This practice may be used for different purposes from eavesdropping to data mining and even censorship, as communications can be interrupted. The presence of surveillance functionalities embedded in security measures must be carefully analysed for its serious privacy implications. Not all security measures though are surveillance oriented. Weapons, from guns to missiles, can be used as security and defensive tools and being very destructive without pursuing any surveillance purposes besides targeting.

The third dimension that must be considered in assessing security measures refers to the **role of the agent for whom the measure has been envisioned.** Broadly speaking security measures may either serve to prevent and punish criminal offence or to diminish risks coming along systems' and users' vulnerabilities. While the majority of measures adopted in forensic investigations aim at identifying criminals, several other measures, from self-defence courses to antivirus or perimeter security, serve the goal of protecting both individuals and infrastructures.

Finally, the fourth general category refers to the **use of the physical-digital dichotomy** as an effective way to draw the line between the virtual and the real world (although the boundaries between both worlds are more and more diminishing).

In general, all measures meant to tackle cybersecurity problems fall into the digital category. On the other hand, all measures concerned with real human bodies and geographical spaces can be considered physical security measures, despite the fact that they can create signals that may be digitally recorded or analysed. Prisons, for instance, are physical security measures. Profiling to detect criminal activity can be considered a digital security measure.

---

[102] Technologies here refer to the actual technological devices developed, used and implemented to improve actual and perceived security levels, whilst techniques refers to the socio-technical practices that allow these technologies to operate. For instance, the smart CCTV is a technology, whilst the algorithm that coordinates and guides the way they work and operate is a technique. The same can be observed with biometric devices and biometric criteria and measures that discipline the actual functioning of the devices.

[103] See for example: Crime Prevention through Environmental Design, Architectural Liaison Officer, Planning Policy Section, Town Hall, Penrith CA11 7QF, UK. URL: http://www.eden.gov.uk/your-community/crime-and-disorder/crime-prevention-through-environmental-design/

Based on these dimensions, security challenges and responses related to technology in relation to the major security domains (as described in section 3) were further elaborated (an overview on the material produced to assist the selection process can be found annexed to this document).

5.2 The selection criteria

Finally, there are criteria that are more associated with policy priorities and with the degree of familiarity that citizens may have with the selected security responses. Given the European focus of the project, it is important that the high priority security areas, concerns and responses identified in European security strategies and policies are widely represented by the selected SOSTs. A further criterion is the actuality of a technology. In order to preserve a prospective approach, the project addresses the aspects of technologies that are already in use as well as technologies that are emerging. We are aware that the latter might be to some extent more difficult for citizens to evaluate and assess due to the lack of familiarity. Thus we also consider the potential societal impact in a wider sense and how this can be presented in an understandable way to the citizens (this will be part of WP4). This combined approach constitutes an added value with regards to the elaboration of future policy strategies and legal guidelines.

Based on the initial classifications together with major aspects on policy (section 3) and on the interplay between privacy, security and surveillance (section 4), the following criteria were considered for the selection process and further elaboration:

- **Relevance** in relation to contemporary security and privacy policy: SOSTs and the addressed challenges should be fairly relevant across the member states, at least those represented in the consortium.
- **Multiplicity** of security domains affected: Different security domains should be represented. Of particular interest are SOSTs that exemplify the blurring boundaries between different domains and threats addressed.
- **Impact on privacy** and other fundamental rights: Security measures and technologies that affect the different notions and types of privacy in different respects. The SOSTs should provide a mix of different infringements and related privacy problems and related policy challenges on privacy.
- **Modes of surveillance** entailed (e.g. factual or pre-emptive): Whenever possible, the selection should represent different surveillance-oriented measures; i.e., SOSTs that address actual security threats whilst others are mainly based on the pre-emptive approach.
- **Actuality** (mix of existing and emerging technologies): Existing and emerging technologies/solutions should be equally represented
- **Priority** of SOSTs in EU policy: Attention should be given to domains and challenges highly prioritized by the EU Commission.
- **Diffusion** of SOST and degree of **familiarity** among the general public: The security challenges/responses should be attached to citizens' experience, in the sense that the existence of public awareness of the challenge and familiarity/resistance to the proposed solutions is a prioritizing factor in the selection.
- **Representativeness**: The selection should reflect the interplay of security measures and privacy aspects in relation to technologies in a EU context with according relevance among the member states.

5.3 The selected security-oriented surveillance technologies (SOSTs)

The selection is the outcome of a stepwise analysis where the general classifications and criteria combined with the different types and dimensions of privacy (as described in section 4.2 and 4.3) where used as a heuristic. The result covers a relevant spectrum of some core elements of contemporary security technologies and related measures that build the basis for further elaboration within the SurPRISE project. The selection provides the foundation for the material presented in work package 4 addressing the different aspects of these technology-related security measures for the participatory

methodology implemented in work package 5. While this section provides a quick overview, a more detailed analysis of SOSTs is conducted in Deliverable 3.1.

The collection was based on an extensive review of European as well as international security research programs, examining of specific reports, policy documents, press articles and online sources, making use of the vast research experiences related to surveillance, privacy and security available within the consortium partners. This selection represents technology-related security measures that are already in use and/or are expected to become issues of wider societal concern. As shown in the previous sections, most of these SOSTs explicitly occur in security policy and also raise several privacy implications. In order to gather a bigger picture also the perceptions of EU citizens as regards major privacy challenges were considered (e.g. different concerns about personal information). As part of the analysis of the initial sets of challenges and responses, different approaches were used for further specification within the project setting.
Based on a combined approach of major (policy) challenges for privacy and security (such as described in section 3 and 4) and the concepts and criteria (described in section 6), the final selection addresses a broad scope of privacy affecting activities induced by these SOSTs and also refers to emerging policy challenges from both perspectives - security and privacy:

- Cyber surveillance, as it is a sort of meta-SOST and entails a magnitude of privacy impacts also in relation to the other SOSTS. A focus is on data retention and DPI as prominent examples.
- (Smart) CCTV, as surveillance cameras are most familiar and smart CCTV triggers a variety of additional privacy impacts
- Location tracking, due to the rapid progress of smart phones and mobile computing referring to concepts such as ambient intelligence, augmented reality, etc.
- Biometrics due to its high relevance for law enforcement and emergence in many security-related actions
- (Behavioural) profiling, as it also represents a sort of crossover SOST that is increasingly employed in a variety of contexts such as passenger screening.
- Drones as peculiar form of a SOST that is expected to become an issue of wide societal concern

This selection represents core elements of contemporary security technologies and measures and all are widely in accordance with the selection criteria: the mentioned systems and applications are highly relevant and prioritized in policies and strategy documents, addressing both the Commission criteria and the priorities of citizens as emerged in the most recent Eurobarometer and national surveys, widely used in multiple domains and relevant in a European context, relatively familiar to the general public, represent a combination of both existing and emerging technologies, entail different degrees of privacy impacts and include different modes of surveillance. In addition, these technology-aided security measures are interrelated in a variety of ways. The selection covers a broad spectrum of privacy-security issues in a sense that they affect different forms of privacy intrusion (as explained above). This is also relevant in order to further analyse the role of the security-privacy trade-off model in relation to these SOSTs.

Table 2: Overview on privacy types affected by the SOSTs

Privacy type / **SOST**	Person	Location and space	Behavior	Communi-cation	Data & image	Thoughts & feelings	Associ-ation
Biometrics	x	(x)			x		(x)
Profiling	(x)	(x)	X	(x)	x	(x)	x
Cyber-surveillance		x	x	X	x	x	x
(Smart) CCTV	X	x	X	(x)	x		x
Location tracking		x	x	(x)			x
Drones	x	x	x		x		

The mapping of table 2 gives some overview on each of the selected SOSTs capability to affect several of the different privacy types and dimensions.[104] In combination with Solove's taxonomy and its process-view on privacy affecting activities, the selection provides a valuable basis from a wider perspective to further examine the privacy-security interplay. For the sake of manageability, i.e. not to overburden the citizen summits the examination of these SOSTs will be split between work package 4 (and implemented in WP5) which focus on cyber-surveillance, (smart) CCTV and location tracking; and work package 7 which addresses the remaining SOSTs (biometrics, drones and profiling).

Brief overview on the selected SOSTs[105]

Biometrics[106]. The gathering and processing of biometric data and the employment of information systems handling such data is a high ranked issue in many security strategies. Biometrics refers to automated methods of recognizing individuals based on measurement of their physical or behavioral characteristics. In its broadest sense, biometrics focus on information about the human body, most common are technologies like fingerprint or iris scanners[107]. The primary biometrics based on physical characteristics currently include ocular recognition (that is, retina and iris), facial recognition, fingerprints/palm prints, hand geometry, and vein pattern recognition. A biometric system is basically an automated pattern recognition system that either makes identification or verifies an identity by establishing the probability that a specific physiological or behavioural characteristic is valid.[108] The field of application of biometric technologies is wide and ranges from access control in security areas to border and migration control or different kinds of profiling activities. Their main objective is the identification of individuals, whether criminal offenders, undocumented migrants, terrorists, or other suspects.

---

[104] This mapping can only be general, as the privacy impact of a SOST is also strongly depending on its application context. Hence, a SOST can affect even more privacy types at the same time. E.g., as the mapping suggests, (behavioural) profiling is a particular case as it can be applied in combination with other SOSTs and thus is capable of affecting each privacy type.

[105] A discussion of the contexts, social controversies and uses of these technologies is part of Deliverable 2.2.: V. Pavone, S. D. Esposti, E. Santiago (2013): "D.2.2 – Draft report on key factors" pp. 69-75.

[106] The US National Research Council defines biometrics in technical sense as "the automated recognition of individuals based on their behavioral and biological characteristics." http://www.theiai.org/disciplines/biometrics/index.php

[107] A particular case are body scanners which are, though also scanning physical characteristics, not directly related to biometrics but based on different technologies (e.g. backscatter x-ray). They are mainly used to scan persons to detect illegal substances or potential explosives, liquids and non-metallic objects (while this does not necessarily include identification it might affect human dignity.)

[108] Wilson, C. (2010). Biometric Modalities. Vein Pattern Recognition: A Privacy-Enhancing Biometric. C. Wilson, CRC Press**:** 19-50.

These technologies are obviously mainly employed at airports and central train stations, although recently biometric identification devices or body scanners are making their way also into governmental buildings, major public buildings or even densely populated offices. Besides the direct scanning of biometric information, the further processing of this information for profiling, pattern recognition and other forms of data mining is becoming more and more common for law enforcement and security related measures. Besides the obvious impact in privacy of the person or body, biometrics in a wider sense also affect other types of privacy as privacy of data and image. This is also to be seen in relation with the increasing cooperation between national and international security authorities, which is a crucial part of the European security agenda. A major part includes enhanced data exchange, interoperability and shared access to EU-databases for security authorities (e.g. Eurodac, SIS I & II) whereas biometric data receive particular attention. In this regard also DNA[109] as a specific form of biometric information is becoming increasingly important. DNA profiling is an emerging issue with growing relevance in the next few years in a variety of domains (as the occurrence in several policy documents underline).

(Behavioural) Profiling[110] and data linkage**.** Profiling is the process of collecting and analysing data on people's individual characteristics, personal information, or activities by either monitoring their actions or other surveillance technologies that can be interfaced with a database. It refers to all those sets of statistical and mathematical data mining techniques applied to datasets containing information about people's choices, preferences and characteristics (this mostly includes data merging from different data sources into larger databases). Part of profiling activities is clustering people into groups that respond to specific criteria, such as the extent to which their behaviour may be considered risky or dangerous. Based on analysing data structure and properties, profiling allows identification of certain individuals or groups.[111] The kind of targeted behavior depends on the context of observation and the consequent nature of the data gathered. In the realm of money laundering, for instance, financial data are analysed in search of unusual transaction patterns, while in enacting visual surveillance through smart CCTV, videotapes are analysed in search of abnormal or suspicious behaviours. Behavioural profiling, therefore, can be considered as a set of multiple sociotechnical practices, which can address different challenges in different domains. They are relatively new, but their implementation is growing rapidly and in all EU countries. Citizens may be more or less familiar with them, but in general should possess at least a basic idea of what behavioural profiling is. Behavioural profiling address potential and actual threats, and has serious privacy implications especially in terms of privacy of personal behaviour.

PNR and APIS[112] are prominent examples for profiling activities. Reinforced screening and monitoring activities of flight passengers for aviation and border control is high prioritized on EU security agenda, such as by processing Passenger Name Records (PNR) and the Advanced Passenger Information System (APIS) which can also contain biometrical data. These approaches mainly affect privacy of personal behaviour, privacy of personal data and, potentially, privacy of personal communication. Besides the primary aims for flight and border security, collected data are also used for law enforcement (e.g. to combat terrorism and crime but also for immigration control) and are exchanged among different national authorities. Partly they rely on the active cooperation of travelling customers as some measures are optional for passengers to accelerate security checks.

(Smart) CCTV[113]. CCTV is among the most common surveillance technologies to serve a large array of security objectives from detection, to deterrence and enforcement.[114] It is used to monitor different

[109] Deoxyribonucleic acid.

[110] http://www.chrc-ccdp.ca/research_program_recherche/profiling_profilage/page4-eng.aspx

[111] Petersen, J. K. (2007). Computers. Understanding Surveillance Technologies: Spy Devices, Privacy, History & Applications, Second Edition, Auerbach Publications**:** 947-977.

[112] E. Brouwer (2009): The EU Passenger Name Record (PNR) System and Humand Rights: Transferring Passenger Data or Passenger Freedom? Centre for European Policy Studies (CEPS) Working Document No. 320, Sept. 2009 http://aei.pitt.edu/11485/1/1903.pdf

[113] Closed Circuit Television. Its widespread diffusion is related to the mass production of transistors and the invention of videotape during the Sixties.

kinds of objects or subjects and are extensively used many domains in public and private spaces such as national borders, airports, train stations, shopping malls, public transport and urban environments and as such widely diffused. While most traditional CCTVs (comprising a camera, coupled with a cable to a screen) were used to monitor remotely, the capability to record is standard in current systems. Regardless of its limited effectiveness in reducing crime overall, CCTV plays a significant role in the post-incident investigation of serious crime and CCTV footage has provided a major investigative tool.[115] Their privacy implications, in terms of privacy of the persons and privacy of personal behaviour and personal communication have been widely studied. Yet, behavioural CCTVs may also have non-physical privacy implications, as they monitor what you do (and supposedly think) rather than who you are or how are you made. With next generation CCTV, surveillance cameras are becoming more sophisticated "intelligent" systems that are capable of advanced monitoring and tracking. Such smart CCTV systems are on the rise and provide different forms of recognizing behaviour ranging from suspicious movements to face recognition and and identifying behavioral patterns (thus also refer to behavioral profiling). As smart CCTVs are emerging technologies and are yet not widely installed, the familiarity among the public is relatively low at the moment. Due to the widespread use of CCTV in a variety of domains worldwide, the privacy impacts of smart CCTV are also accordingly high.

Drones (UAVs[116]). Drones are unmanned air vehicles that can be used for a broad range of surveillance activities in almost every security domain. The technology is relatively new and its origins lie in the military sector. However, it is more and more entering further domains of public and private sector ranging from traffic observation to monitoring neuralgic points of criminal activities, tracking people or vehicles, or are even available for private use. At large-scale events like the Olympic Games, drones are used to control crowds and their relative movements in closed and articulated spaces. In some countries, drones are also applied to control borders or to monitor critical infrastructures. The wide array of applicability entails an enormous set of privacy implications; Not least as a drone can be equipped with additional technologies (such as CCTV, different sensoring devices like heating sensors, etc.). It mainly affects bodily privacy, privacy of personal behaviour and location privacy. So far drones are not widely used in civil environments and thus rather unfamiliar to European citizens but can be expected to become an issue of wider societal concern as there is a growing economic interest in developing civil applications for UAVs and similar.

Location tracking technologies. Location Tracking Geo-Data, RFID[117], GPS and Mobile Tracking are part of a set of responses, which aim mainly at tracking the movement and location of both people and objects. Their relation to security is somewhat indirect, given that the security challenge is essentially related to the potential threats that the located people or objects constitute. The related privacy implications are quite evident but depending on its implementation can also affect different privacy types. They are now in use in several different areas, although the use of location tracking is mainly for law enforcement there are also applications in the private sector. Given the wide scope of the subjects and objects potentially traceable, this technology measure can be applied to a variety of challenges, although its most common use are in the domains of rescuing people, tracking valuable objects or locating criminal suspects. Mobile computing, usage of smart phones and other mobile devices are significantly growing and refer to the increasing relevance of once theoretical concepts such as ambient intelligence, pervasive computing or augmented reality. The increase in mobile computing entails rapid

---

[114] D. Litzau (2007). Closed-Circuit Television and Video Surveillance. Information Security Management Handbook, Sixth Edition. H. F. Tipton and M. Krause. Boca Raton, CRC Press**:** 1349-1356.

[115] Clive, N. (2010). Closed-Circuit Television. International Handbook of Criminology. S. G. Shoham, P. Knepper and M. Kett, CRC Press**:** 395-424.

[116] Unmanned Airial Vehicle or another term is RPV – remotely piloted aircraft vehicle or system (RPAS). The European Commission plans a strategy for the development of civil applications of RPAS: http://ec.europa.eu/enterprise/sectors/aerospace/uas/index_en.htm

[117] Radio frequency identification (RFID) tags are small, wireless devices that allow to mark and identify objects and persons. While typical uses were based in logistics, RFID diffusion grows e.g. in every-day-products, some manufacturers integrate tags in clothing. Increasing use can be expected in the domain of near-field-communication (NFC).

growth in related applications and services and triggers huge amounts of personal information that foster traceability of individuals, e.g. via GPS, radio cells of mobile phones, location based services or smart tags such as RFID etc. As always-on is already the default setting due to these devices, location tracking can be expected to intensify already high impacts on privacy.

Cyber-surveillance[118]. The widespread diffusion of ICTs and digital networks creates a variety of new possibilities to extent surveillance practices. Cyber surveillance describes modalities in this regard for monitoring and observing "persons, objects or processes that is based on new technologies and that is operated from and on data networks, such as the Internet"[119]. Cyber surveillance has become a part of contemporary society and includes a broad array of (technology-related) actions. National and international security authorities (as well as intelligence agencies) strengthen their efforts to monitor and observe all kinds of web-based interactions ranging from information provision, exchange to communication or transactions. The conduction of cyber surveillance spans across a range of sectors aiming inter alia at managing risks, fostering security of persons, places, data, infrastructures and processes.[120] Cyber surveillance affects fundamental rights in multiple respects. At first glance it primarily affects the privacy of personal data, of personal communication; however depending on specific applications it can affect each privacy type. Deep invasion of individual privacy is accompanied by attempts to control digital information flows entailing a broad scope of impacts that complicate freedom of expression, the trustworthiness of communication and other core values in democratic societies. For a deeper understanding in particular as regards government activities of cyber surveillance it is to be seen in relation to lawful interception. Due to its wide array of applications (e.g. Data-Analysis/Filtering & Screening, Deep Packet Inspection, Data-Mining, surveillance of web 2.0 and social media, etc.) and its multiple impacts on privacy, cyber surveillance is most obvious to be among the selected SOSTs. Within the already broad domain of cyber-security (and even beyond) it comprises an emerging set of technological responses whose development follows closely the parallel developments of ICTs and thus represents a sort of meta-challenge for current and future developments. For a more in-depth analysis, controversial issues that are specific occurrences of this category will be examined. Prominent ones in a European context are Data Retention (DR) and Deep Packet Inspection (DPI).

Data retention technologies and practices gather personal data in a pre-emptive manner. Data is thus stored without a particular suspicious fact to have data available in case of a crime. The aim is to investigate committed crime and terrorism. In Europe the Data Retention Directive obliged member states to implement data retention on a national scale and store phone call detail records and internet traffic and transaction data of their citizens. It thus represents an example for cyber-surveillance. The high impact on all types of privacy as the variety of data than can be retrieved and stored is potentially unlimited, from consumption behaviour to health data, political beliefs and social relations.[121] Data retention is thus highly controversial and the Directive has been heavily criticized across Europe by many concerned actors ranging from privacy, legal and technical experts, public and private institutions, NGOs as well as individual citizens. Public awareness is thus relatively high, though on a general level not as regards details about data retention and its practices in a wide implications. DPI was initially used by internet service providers to monitor and protect their networks against attacks, viruses, malware, spam, etc. in combination with firewalls and for bandwidth management and load balancing of their services. However, DPI is more and more becoming a matter of concern in a broader societal context as it could be used to remove net neutrality and the openness of the internet. It is already used in a wide range of applications by enterprises, service providers and increasingly debated for copyright protection and government monitoring of internet activity including the content. DPI is highly controversial as it enables censorship, large-scale real-time surveillance and thus entails enormous impacts on privacy and

---

[118] Cyber surveillance includes network surveillance which is a more technically coined term.

[119] M. Tremblay (2012): "Cyber-Surveillance", in L. Coté and J.-F. Savard (eds.), Encyclopedic Dictionary of Public Administration [online], www.dictionaire.enap.ca

[120] Cf. C. Bennett, A. Clement, K. Milberry (2012): „Editorial: Introduction to Cyber-Surveillance" In: Surveillance & Society 9(4): 339,347. www.surveillance-and-society.org

Tremblay (2012) op. cit.

[121] Since the Directive became effective, there were already discussions on extending access to the gathered data for other purposes such as smaller crimes, copyright delicts.

other human rights such as freedom of information, freedom of expression and related democratic core principles. Authoritarian governments and political regimes already employ DPI as a means for censorship and control of public communication (e.g. Libya, Syria, China, Iran). The Qaddafi regime used the technology for capturing e-mails, chat conversations and web use of Libyan citizens.[122]

[122] Gallagher (2012): Big Brother on a budget: How Internet surveillance got so cheap. Arstechnica.com Sept 27 2012. http://arstechnica.com/information-technology/2012/09/big-brother-meets-big-data-the-next-wave-in-net-surveillance-tech/

6 Conclusion

The selection of SOSTs reflects some of the major issues concerning contemporary security and privacy discourse. The transformation of security policy towards a broad understanding of security that spans across a variety of domains in line with the process of securitization is a double-edged sword: while on the one hand, it is a reaction to the changing conditions that security policy and strategy have to encounter in a global and networked society. On the other hand, the incorporated framing of security as a holistic concept combined with increasing attempts to prevent a multitude of rarely predictable (and sometimes blurry) threats has also amplified several tensions on the relation between privacy and security respectively freedom and security. Such a view produces a strained relation between these concepts as if tensions in between would per se exist by dismissing that freedom (or more precisely liberty) is the defining value: "democracy, the rule of law and fundamental rights are designed to protect the liberty of the individual within the society."[123].

Thus security is only a concept to support freedom but can never be a value equated to liberty. As an unintended side-effect, the crucial focus on securing domains that are essential for the functioning of a society such as protecting infrastructures, emergency management etc. from harm, might become threatened to become distracted at the costs of political security discourse reinforced by securitization. The use of technology is surely an important means in different domains to address security challenges in an effective manner. However, the increasing employment of SOSTs highlights that these technologies also carry the weight of securitization if they are introduced without prior assessment of their societal impacts. Entailed is a neglected view on the appropriateness of its use in accordance with privacy and other fundamental rights. This often results in a lack of safe and sound balancing of use contexts *before* deploying SOSTs, whereas its main precondition of being a supportive tool for security without self-purpose seems to get out of sight. Consequences are not merely low security achievements but also the problem of function creep and rule-breaking SOST usage that undermine privacy and other fundamental rights. To alleviate this situation is among the relevant aspects in the SurPRISE project. The selection of SOSTs presented in this document provides an entry-point for their further exploration; in particular regards the perceptions of citizens, also in relation to public acceptance and acceptability, privacy-by-design concepts and alternative options to avoid privacy infringements, and to overcome the fallacy of trading privacy against security.

[123] E. Guild, S. Carrera, T. Balzacq (2008) op. cit. p. 9

7 Bibliography

Article 29 Data Protection Working Party: Work programme 2012-2013 00381/12/EN, WP 190, February 2012 http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

K. Ball, K. Haggerty and D. Lyon (eds.) (2012): Handbook on surveillance studies. Routledge.

T. Balzacq (2005): The three faces of securitization: Political agency, audience and context. In: European Journal of International Relations 11(2): 171-201.

T. Balzacq (2008): "The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policy", Journal of Common Market Studies, Vol. 46, No. 1, 2008.

C. J. Bennett (2011): "In Defence of Privacy: The concept and the regime". In: Surveillance & Society 8(4): 485-496.

C. Bennett, K. Haggerty (eds.) (2011): Security Games: Surveillance and Control at Mega-Events. Routledge.

C. Bennett, A. Clement, K. Milberry (2012): „Editorial: Introduction to Cyber-Surveillance" In: Surveillance & Society 9(4): 339,347. www.surveillance-and-society.org

R. Berglenz, R. Kreissl (2013): "D3.3. Report on security enhancing options that are not based on surveillance technologies.". SurPRISE Deliverable 3.3

D. Bigo (2000): "When two become one: Internal and external securitisations in Europe." In: International Relations Theory and The Politics of European Integration. Power, Security and Community. M. Kelstrup and M. Williams (eds.), London, Routledge, pp. 171-204.

A.J. Blumberg & P. Eckersley (2009) 'On locational privacy, and how to avoid losing it forever' Electronic Frontier Foundation, August 2009, at https://www.eff.org/wp/locational-privacy

B. Buzan, O. Weaver, J. de Wilde (1998): Security: A New Framework for Analysis. Lynne Rienner: Boulder, 1998.

E. Brouwer (2009): The EU Passenger Name Record (PNR) System and Humand Rights: Transferring Passenger Data or Passenger Freedom? Centre for European Policy Studies (CEPS) Working Document No. 320, Sept. 2009 http://aei.pitt.edu/11485/1/1903.pdf

R. Clarke (2006): "What's privacy?" Version 7 August 2006 http://www.rogerclarke.com/DV/Privacy.html

R. Clarke 2012: Location tracking of mobile devices: Ueberveillance stalks the streets. http://www.rogerclarke.com/DV/LTMD.html

N. Clive (2010). Closed-Circuit Television. International Handbook of Criminology. S. G. Shoham, P. Knepper and M. Kett, CRC Press: 395-424.

J. E. Cohen (2008) 'Privacy, Visibility, Transparency, and Exposure', University of Chicago Law Review, 75/1: 181-201

Council of the European Union, Prüm Convention Brussels January 7 2005 http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf

European Council, Tampere European Council 15 and 16 October 1999 Presidency Conclusions http://www.europarl.europa.eu/summits/tam_en.htm

European Council, Communication on Delivering an Area of Freedom, Security and Justice for European citizens - Action Plan implementing The Stockholm Programme. COM(2010) 171 http://www.statewatch.org/news/2010/apr/eu-com-stockholm-programme.pdf

European Council, Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data [COM(2012) 10 final, Brussels, 25.1.2012, 2012/0010 (COD)] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF

H. Engerer (2009): "Security Economics: Definition and Capacity". Economics of Security Working Paper 5, Berlin: Economics of Security. http://www.diw.de/documents/publikationen/73/diw_01.c.94891.de/diw_econsec0005.pdf

European Commission, Communication on The Hague Programme: Ten priorities for the next five years – The partnership for European renewal in the field of Freedom, Security and Justice, COM(2005) 184 final, Brussels. http://ec.europa.eu/home-affairs/doc_centre/docs/hague_programme_en.pdf

European Commission (2010). Communication from the Commission to the European Parliament and the Council - The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. Brussels. http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf

European Commission (2010). Communication from the Commission to the European Parliament and the Council - The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. Brussels. http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf

European Commission (2011). Special Eurobarometer 371 - INTERNAL SECURITY. Report Number 371.

European Commission (2011): Special Eurobarometer 359 Attitudes on Data Protection and Electronic Identity in the European Union. June 2011. Survey requested by the Directorate-General Information Society and Media (INFSO), the Directorate-General Justice (JUST) and the Directorate-General JRC and co-ordinated by the Directorate-General Communication ("Research and Speech Writing" Unit) http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf

European Commission (2012). Ethical and Regulatory Challenges to Science and Research Policy at the Global Level. Brussels, Directorate-General for Research and Innovation. http://ec.europa.eu/research/science-society/document_library/pdf_06/ethical-and-regulatory-challenges-042012_en.pdf

European Commission April 2013, http://ec.europa.eu/rea/funding_opportunities/security/index_en.htm

European Commission (2010). Communication from the Commission to the European Parliament and the Council - The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. Brussels.

European Communities (2004). Research for a Secure Europe. Report of the Group of Personalities in the field of Security Research. Office for Official Publications of the European Communities. Luxembourg. http://ec.europa.eu/enterprise/policies/security/files/doc/gop_en.pdf

Report from the European Security Research Advisory Board - Meeting the challenge: the European Security Research Agenda (September 2006) http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf

European Data Protection Supervisor - EDPS (2012): Annual Report 2011 of the European Data Protection Supervisor. http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Annualreport/2011/AR2011_EN.pdf

EDRI (2012): European Digital Rights (EDRI) EDRi's Position on the Directive Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (COM 2012 final). https://dpreformlawenforcement.files.wordpress.com/2012/12/edri-position-papers-directive1.pdf

ESRIF (European Security Research and Innovation Forum) (2009). ESRIF Final Report.http://ec.europa.eu/enterprise/policies/security/files/esrif_final_report_en.pdf

Rachel L. Finn, David Wright, and Michael Friedewald (2013) "Seven Types of Privacy" in Gutwirth, S.; Leenes, R.; de Hert, P.; Poullet, Y. (Eds.), "European Data Protection: Coming of Age", Chapter 1, Dordrecht: Springer. DOI 10.1007/978-94-007-5170-5_1.

M. Foucault 1977: Discipline and Punish: the birth of the prison, trans. A Sheridan, London: Penguin.

Gallagher (2012): Big Brother on a budget: How Internet surveillance got so cheap. Arstechnica.com Sept 27 2012. http://arstechnica.com/information-technology/2012/09/big-brother-meets-big-data-the-next-wave-in-net-surveillance-tech/

F. Geyer (2008): Taking Stock: Databases and Information Exchange in the Area of Freedom, Security and Justice, CHALLENGE Research Paper No. 9, CEPS, Brussels.

E. Guild, S. Carrera, T. Balzacq (2008): The changing dynamic of security in an enlarged European Union. Research paper No. 12, The changing landscape of European Liberty and Security - www.ceps.eu http://aei.pitt.edu/11457/1/1746.pdf

K. D. Haggerty and R. V. Ericson (2000): "The surveillant assemblage". In: British Journal of Sociology Vol. 51(4) December 2000, pp. 605-622.

P. Hobbing 2006: Security and Information: SIS II and the Interoperability of JHA Databases, Centre for European Policy Studies (CEPS), Brussels.

K. L. Hall (ed.) (2012): The Oxford Companion to the Supreme Court of the United States, 2nd edition, Oxford University Press, New York, 2012.

B. Hayes (2006). Arming Big Brother. The EU's Security Research Programme. TNI Briefing Series. Amsterdam, Transnational Institute.

B. Hayes (2009). "NeoConOpticon. The EU Security-Industrial Complex." http://www.statewatch.org/analyses/neoconopticon-report.pdf

M. Ibrahim (2005): "The Securitization of Migration: A Racial Discourse". In: International Migration, Vol. 43 (5), pp. 163-187.

R. Jolly and D. B. Ray (2006): "The Human Security Framework and National Human Development Reports: A Review of Experiences and Current Debates". United Nations Development Programme, National Human Development Report Unit.

G. Karyotis (2011): "The fallacy of securitizing migration: elite rationality and unintended consequences". In: G. Lazaridis (ed.): Security, Insecurity and Migration in Europe. Ashgate, Surrey, Great Britain, pp. 13-30.

U. Kilkelly (2003): The right to respect for private and family life – a guide to the implementation of Article 8 of the European Convention on Human Rights. Human Rights Handbooks No. 1, Directorate General of Human Rights, Council of Europe, Strassbourg, 2003 http://echr.coe.int/NR/rdonlyres/77A6BD48-CD95-4CFF-BAB4-ECB974C5BD15/0/DG2ENHRHAND012003.pdf

D. Litzau (2007). Closed-Circuit Television and Video Surveillance. Information Security Management Handbook, Sixth Edition. H. F. Tipton and M. Krause. Boca Raton, CRC Press: 1349-1356.

D. Lyon (2001): Surveillance Society: Monitoring Everyday Life, Oxford, University Press;

D. Lyon (ed.) (2003): Surveillance as social sorting: privacy, risk and digital discrimination. Routledge.

OECD (2004): The Security Economy. http://www.oecd.org/futures/16692437.pdf

T. Owen (2004): Challenges and opportunities for defining and measuring human security, in: Human Rights, Human Security and Disarmament, disarmanet forum 2004 Vol 3. 15-24

M. G. Porcedda, M. Scheinin, M. Vermeulen (2013): D3.2 – "Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy". SurPRISE Deliverable 3.2

J. K. Petersen (2007): Introduction & Overview. Understanding Surveillance Technologies: Spy Devices, Privacy, History & Applications, Second Edition. Boca Raton, Auerbach Publications: 3-101.

J. K. Petersen (2007). Computers. Understanding Surveillance Technologies: Spy Devices, Privacy, History & Applications, Second Edition, Auerbach Publications: 947-977.

G. Quille (2004): The European Security Strategy: A Framework for EU Security Interests? In: International Peacekeeping, Vol.11, No.3, Autumn 2004, pp.1–16 http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede20040728_ess_/sede20040728_ess_en.pdf

M. Raguse, M. Meints, O. Langfeldt, W. Peissl (2008): "D6.2 - Criteria for privacy enhancing security technologies". Deliverable 6.2 of the PRISE project

D. Solove 2006: "a taxonomy of privacy". In: University of Pennsylvania Law Review". Vol. 154 (3). Pp. 477-560.

D. Solove (2011): Nothing to hide: the false tradeoff between privacy and security. Yale University Press. New Haven and London.

M. Tremblay (2012): "Cyber-Surveillance", in L. Coté and J.-F. Savard (eds.), Encyclopedic Dictionary of Public Administration [online], www.dictionaire.enap.ca

United Nations – UN (1994): New dimensions of Human Security. Human development report 1994, United Nations Development Programme, New York, Oxford University Press.

United Nations - UN (2004): The UN Secretary General's High-level Panel on Threats, Challenges and Change. 2004. A More Secure World: Our Shared Responsibility. New York: United Nations Press.

S. D. Warren and L. D. Braneis (1890): "The Right to Privacy". In: Harvard Law Review 193 (1890) Vol. IV Dec. 15 1890, No. 5 http://faculty.uml.edu/sgallagher/Brandeisprivacy.htm

S. Watson (2011): The 'human' as referent object? Humanitarianism as securitization. In: Security Dialogue 42(1):3-20. DOI:10.1177/0967010610393549

A. Westin (1967): Privacy and freedom. Atheneum, New York.

O. Weaver (1995): Securitization and desecuritization. In: Lipschutz R. (ed.) On Security. New York: Columbia University Press, 46-79.

C. Wilson, (2010). Biometric Modalities. Vein Pattern Recognition: A Privacy-Enhancing Biometric. C. Wilson, CRC Press: 19-50.

World Economic Forum (2013). Global Risks 2013. An Initiative of the Risk Response Network. Geneva. Eighth Edition. http://reports.weforum.org/global-risks-2013/

M. Yar (2011) "From the 'Governance of Security' to 'Governance Failure': Refining the Criminological Agenda", Internet Journal of Criminology (Online)

8 List of Figures

9 List of Tables