"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 3.4 – Exploring the Challenges - Synthesis Report

Lead Beneficiary: IRKS

Author(s): Reinhard Kreissl (IRKS), Regina Berglez (IRKS),

Maria Grazia Procedda (EUI), Martin Scheinin (EUI), Matthias Vermeulen (EUI),

Eva Schlehahn (ULD)

Due Date: April 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
ATM	Automatic teller machine
CCTV	Closed-circuit Television
DPI	Deep Packet Inspection
ECHR	European Court of Human Rights
ECJ	European Court of Justice
ENISA	European Network and Information Security Agency
EUCFR	European Charter of Fundamental Rights
FIP	Fair Information Principle
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communication Technology
IPR	International Property Right
LEA	Law Enforcement Agencies
PAwS	Public Awareness of Science
PbD	Privacy by Design
PET	Privacy-enhancing Technology
PIA	Privacy Impact Assessment
PUS	Public Understanding of Science
SOSS	Surveillance-oriented Security Solution
SOST	Surveillance-oriented Security Technology
TEU	Treaty on European Union
UDHR	Universal Declaration of Human Rights
VIS	Visa Information System

Abstract

This report represents a synthesis, connecting key findings of three individual reports (D3.1 to D3.3) which reviewed and explored challenges and options for technological, legal, political, and societal developments on privacy and security. It elaborates on the concept of privacy, illustrating the evolution of the right to privacy. Key concepts of security and threat are discussed and the problems of using technological solutions to handle threats are highlighted. Three surveillance technologies (smart CCTV, digital network surveillance and location trackers) are exemplified in more detail looking at effects on privacy rights and also broader societal effects. Having focused on technological solutions and their legal governance, societal alternatives to maintain security will be presented. The report ends with a brief overall assessment of the security debate advocating for what we term balanced risk awareness and does also offer an executive summary with a number of policy recommendations.

1. Introduction[1]

Legal provisions to protect the right to privacy have evolved over the last century, always following new socio-technical developments creating new threats to privacy through new ways of collecting, storing and processing person-related data.

Conceptually this right can be justified from different perspectives. It can be perceived as the right to do in a more or less bounded physical space whatever one wants. Extending this view from individuals to groups, the political implications of the right to privacy become obvious. Individuals should have the right to exchange their views, discuss and deliberate their opinion. The social history of the so-called secret societies from the 18th century onwards can be read as an exercise of the right to privacy before its legal codification. The state should refrain from interfering with the private sphere of citizens and guarantee their privacy. Here we see the right to privacy in its classical form as a negative right, defining the relation between the state and its citizens.[2]

On the other hand, and in a more modern reading, the right to privacy can also be seen as a sort of symbolic property right, endowing the person with the right to determine who is entitled to do what with her person-related data. In its contemporary form this is called the right to informational self-determination, emerging in a "datafied" society. No other person should make use of an individual's person-related data, unless granted permission by this individual to do so (or being entitled by a contractual agreement or legal provision). This argument rests on the assumption that person-related data constitute a kind of symbolic or informational property. It also perceives of person-related data as a kind of quasi-material asset the owner can control, protect or transfer at will under an existing legal regime.

Historically, privacy has been closely linked to proximity. The idea of privacy is rooted in a spatial understanding, drawing a distinction between the home (or the Greek Oikos) and the public space (the market place or Agora), between the private inside and the public outside. This intuitively useful difference is losing its grip in a society where time and space are compressed, social interactions of all kinds are based on electronic media, and locally contained forms of social life become increasingly replaced by institutionally mediated long distance encounters and exchanges. What is private and what is public no longer depends on a spatial arrangement. Spatial arrangements also define social relations. But categories like neighbour or stranger are difficult to apply on the Internet. While questions of identity used to be negotiated socially and culturally (your neighbours could tell who you are, and strangers were easily identified in a local village, your dress and habitus could tell your status in the city) in present day societies the default attitude in public space is generalized "suspicion": identities are no longer negotiated face-to-face with others but checked, using machine-readable codes linking a physical object (person) to person-related information in a remote data-base. Pin codes and passwords, swipe cards and biometric measures are typical contemporary person identifiers also serving as gate keepers for authorisation and access purposes. They are the keys to products, services, spaces, and other persons and are gradually replacing paper-based identity documents like traditional passports.

These data, used to identify an individual are distributed across a great (and growing) number of databases. Furthermore every institutionally-electronically mediated social exchange produces data traces that can be linked to the particular individuals involved in this exchange. Ordering goods on the Internet, buying an airline ticket, using a mobile phone, posting or sending a message through social media or E-mail, using a credit card, a loyalty card, etc. adds to these data traces and produces more person-related data beyond the control of the individual.

Is there a meaningful way to use the idea of a privileged private sphere to be protected by law under these conditions? What precisely is it that has to be protected? To address this question a distinction

[1] By IRKS

[2] For an elaborate debate see Richard Sennett, *The fall of public man,* New York, London: W.W. Norton (1996) [1977].

should be drawn between person-related data produced as side effect of modern consumer society (such as e.g. consumption and mobility patterns of an individual), person-related data gathered for the exclusive purpose of surveillance (like images from CCTV cameras or information gathered through active intelligence gathering strategies, like e.g. the use of Trojans and the like) and dataveillance or data mining operations performed on either set of these data. The first type, person-related data, produced as side effects of commercial transactions and/or communication, is based on a – more or less informed, more or less voluntary – decision of the individual providing the data. The second type, data gathered for surveillance purposes, does not require the consent of the persons affected. The same is true for all data mining operations that are performed without active participation and/or consent.

A breach of privacy in an everyday understanding could be the act of making public information that is considered private. The prototype here would be the Paparazzi. He "takes" the picture out of the individual's private sphere and posts it in a public medium, exposing the person in a private situation to public gaze – against her will. But this "old school" scenario is not the type of privacy infringement that is relevant here. In most cases data linked to an individual are processed, transmitted and used in different ways without the person being immediately affected or even aware of it, nor is any public involved in these processes. In the age of electronic consumerism it also would be impossible to maintain the traditional idea of person-related data as a kind of symbolic property under the exclusive control of an individual.

Legal safeguards are weakened, when security issues are at stake and interested parties such as Law Enforcement Agencies (LEA) can claim that a deeper and broader intrusion into the thick layers of person-related data is necessary to combat crime, terrorism and other evils.

For such surveillance operations to be effective there has to be an adequate infrastructure allowing for the use of intelligence created from person-related data. There are two interconnected logics of surveillance, based on social sorting and targeting single individuals respectively. Both require the machine-readable individual, and for the second approach a powerful retrieval or search mechanism is required. Social sorting and targeting of individuals can be seen as activities having an effect on individual citizens. Social sorting creates differential access to goods and services, providing privileges for some while others are disadvantaged. Targeting may trigger more intrusive actions by LEA on single individuals.

Machine-readability can be a problem if a person is not tied into the mundane processes of bureaucratic-consumerist culture. Migrants from outside the EU have to be made machine-readable through fingerprinting, DNA-sampling or other means of digitalized identification.

Defining the right to privacy as the right to protection of person-related data against use outside a legally defined framework, the conflict between privacy advocates on the one hand and LEA or the military and security industrial complex on the other arises over the necessity and efficiency of privacy intrusive surveillance measures: do the perceived security threats justify the measures suggested and can these measures (or technologies) provide the intelligence necessary to address the security problem?

The first question can be addressed by an informed critical analysis of the claims brought forward by LEA, the second by an analysis of the technical capabilities of the solutions suggested. In order to limit privacy intrusions threat potentials should be scrutinized and technological options reviewed to select the least intrusive alternatives.

Unfortunately the Law Enforcement community rarely provides independent evidence for their threat assessments. They either refer to secret intelligence sources that cannot be disclosed or point to the fact, that nothing so far has happened and many attacks could be prevented due to their activities. But such non-events do not make good evidence and in a number of cases the presumptive prevented attacks were induced by Agents provocateurs in the first place.[3] The problem here seems to be that security is left exclusively to the experts of the LEA community and the judiciary is relying on threat assessments

[3] Gary T. Marx, "Thoughts on a Neglected Category of Social Movement Participant: The Agent Provocateur and the Informant." *American Journal of Sociology*. vol. 80, pp. 402-442. (1974).
And also: (No author), „Rechtsextremismus: Bis zu hundert V-Leute in der NPD aktiv" *Zeit Online* (2011) http://www.zeit.de/gesellschaft/zeitgeschehen/2011-11/npd-verfassungsschutz

that can hardly be questioned. While it is possible to defend privacy rights from an abstract legal perspective it is hard to curtail the rights of the LEA once society as a whole has been securitized. Any social field can be 'securitized', i.e. talking about a social object or process in terms of security changes the dominant discourse, mind-set and policy options. Securitization demonstrates this complex transformation and remodelling of (societal) issues into matters of security and also the process in which these issues are then exposed to surveillance measures. Any subject, issue or condition securitized is taken out of the general political debate, gets framed as either a special kind of politics or as above politics and can therefore be (re-)created as an entity of security matters.[4]

Nonetheless there are some minor windows of opportunity for broadening the basis of debate and probably contributing to a more complex and rational public discourse about security. Security has to be taken back from the experts to the general public, i.e. what counts as a secure environment and what is conceived as an adequate measure to maintain or increase security should not be narrowed down to an experts' view of worst case scenarios. Also the range of expertise could be extended including security experts from outside the LEA community to challenge narrow views in this field. This entails also the establishment and regular audit of best practice guides and qualification standards for the laboratories and the further personnel involved within the LEA community working with computer forensics and the like,[5] Additionally the expertise from relevant fields of technology assessment to critically investigate the use-value and side effects of surveillance technologies, and to identify the potential for function creep or abuse.

As will be shown in the following chapters a cumulatively uncontrollable securitizing move can be countered from a different angle: defusing exaggerated threat assessments while offering alternative solutions to improve societal security and dismantling the rhetoric and promise of transparency through surveillance based security technologies while providing realistic options for a socially acceptable use of surveillance technology in line with legal requirements for the protection of privacy rights.

1.1 Interdependencies within the SurPRISE project

This paper represents the Synthesis Report (Deliverable 3.4) of the work package 3 – Exploring the Challenges – within the SurPRISE project. The main aim of work package 3 was to review and explore main challenges and options for technological, political, legal and societal developments on privacy and security and to identify (non-technological) alternatives to surveillance-focused security investments. This deliverable is condensing the individual findings of the three reports created in the tasks 3.1 to 3.3 and is putting "Exploring the Challenges" into a broad perspective, compiling expertise in the fields of technological, legal and social sciences.

work package 3 is - along with work package 2- one of the theoretical work packages within the SurPRISE project, and was meant to create some of the theoretical greound and background for the empirical work packages 4,5 and 7 to follow within SurPRISE.

Deliverable 3.4 connects to work package 2 (Framing the Assessment) and informs work package 4 (Questionnaire and Information Material); and it will furthermore provide background analysis for work package 6 on the analysis and synthesis report within the whole project.

The identified alternative security measures, options and strategies will be pertinent for the planning process carried out for conducting the participatory assessment exercises: the findings and results of this task will feed into the structural planning of the citizen consultations; the exemplifies technologies are in line with the information material packages created in work package 4. These information material worked out within work package 4 is to serve as the main input for the multi-national participatory citizens' events to follow in work package 5.

[4] Barry Buzan, Ole Waever, and Jaap De Wilde, *Security: A New Framework for Analysis*, Lynne Rienner Publishers (1998).

[5] This point was raised by Nina Tranjo who is a member of the SurPRISE Advisory Board.

1.2 Outline

In the following pages we will first elaborate on the legal concept of privacy, discussing the evolution of the right to privacy (2.1 and 2.2). It will be shown how security and privacy enter into a complex relationship in modern legal discourse (2.3) and how the problems arising in this discourse might be solved (2.4). Against the backdrop of the legal analysis the key concepts of security and threat will be discussed and the problems of using technological solutions to handle threats will be highlighted (3). Chapter 4 will discuss different surveillance technologies in more detail looking at their effects on privacy rights (4.1 – 4.3) and will then ask how the application of these technologies can be constrained in the face of their societal effects, using legal arguments (4.4). Since surveillance technologies are introduced to reduce security risks, these technologies also have to be critically analysed whether they live up to the promised effects (4.5). Having focused on technological solutions and their legal governance, some of the societal alternatives to enhance security will be presented (5). The report ends with a brief overall assessment of the security debate (6) suggesting what we call balanced risk awareness as the basis for a rational debate about privacy and security. An executive summary (7) is listing a number of policy recommendations.

2. Privacy[6]

2.1 The societal value of the fundamental rights to privacy and data protection

The rights to privacy and data protection express crucial societal values. An analysis of the origin of both rights can help illustrating this. The right to privacy was legally formulated for the first time in the United States in a seminal article written over a century ago by Warren and Brandeis.[7] The right was quickly labelled as 'the right to be let alone,"[8] but the authors articulated it further. Firstly, privacy was described as embodying the need to legally protect an emerging societal, moral and philosophical need, "a right to personality" or identity, namely the expressions of one's life, such as emotions, sentiments, facts of life, happenings, actions, sexual life and relationships with others. Secondly, the formulation of such a right would counter unpredictable negative effects of technological evolutions (such as – at that time – the improvement of photography allowing taking pictures at a distance) and related consequences (i.e. the proliferation of sensational periodicals publishing unwanted pictures).[9]

There are two defining elements of the right to privacy that may be seen as informing its legal development. On the one hand, privacy "refers to the sphere of a person's life in which he or she can freely express his or her identity, be it by entering into a relationship with others, or alone."[10] Such a private sphere allows "individuals and groups to be able to think and develop ideas and relationships".[11] It is based on the liberal idea of autonomy and freedom of action,[12] manifested in the private sphere as individuals free from the State's interference (home, body and correspondence), and in the public sphere as citizens,[13] which seems to belong in different forms to all cultures,[14] and is indeed included in many constitutions.[15] Some authors refer to privacy as a meta-right, serving as the basis for civil and political rights such as freedom of expression, association, and movement, which could not be effectively enjoyed otherwise.[16] Furthermore, privacy puts normative limits to technological advances and related practices, which enhance human possibilities in either sense, and in particular interfere with autonomy and freedom[17].

---

6 By EUI

7 Samuel D. Warren and Louis D. Brandeis, 'The Right to Privacy', Harvard Law Review, 4/6 (1890).

8 Which was borrowed, in turn, from a formulation of Judge Cooley. Ibid.

9 Ibid. Stefano Rodotà, *Elaboratori Elettronici E Controllo Sociale*, Bologna: Mulino, (1973).

10 See A. R. Coeriel et al. v. the Netherlands, 453/91, p. 79 in John Blair, The International Covenant on Civil and Political Rights and Its (First) Optional Protocol. A Short Commentary Based on Views, General Comments and Concluding Observations by the Human Rights Committee, Frankfurt: Peter Lang (2005).

11 Martin Scheinin, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism', Geneva: General Assembly (2009b) at 13.

12 Lars Adam Rehof, 'Universal Declaration of Human Rights – Common Standard of Achievement', in Asbjorn Eide and Gudmundur Alfredsson (ed.), Norway: Scandinavian University Press (1995), pp. 251-64.

13 Manfred Nowak, 'Chapter on Article 17 ', in Manfred Nowak and Felix Ermacora (ed.), *Un Covenant on Civil and Political Rights, Ccpr Commentary*, Kehl: N.P. Engel, (2005 (2nd edition)), pp. 377-405, Yves Poullet and Antoinette Rouvroy, 'The Right to Informational Self-Determination and the Value of Self-Development. Reassessing the Importance of Privacy for Democracy', in Serge Gutwirth et al. (eds.), *Reinventing Data Protection?* (2009).

14 Alan Westin, *Privacy and Freedom,* Atheneum Press (1967).

15 Drafting Committee on an International Bill of Human Rights (1st Session), 'International Bill of Rights Documented Outline ' (1947).

16 Stefano Rodotà, 'Data Protection as a Fundamental Right', in Yves Poullet Serge Gutwirth, Paul De Hert, Sjaak Nouwt and Cécile De Terwangne (ed.), *In Reinventing Data Protection?* Springer (2009), Scheinin, 'Report of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism'.

17 On this point, see also Vincenzo, Pavone, Sara Degli Eposti and Elvira Santiago, *SurPRISE project D2.2* (2013), chapter "4.4.1 Privacy expectations and concerns", p.58 – 68.

A noticeable development was (and still is) the appearance of computerized systems and their applications. They enabled unprecedented (personal) data processing capabilities, which opened up social, cultural, and economic opportunities (including in the administration of the welfare state), also abroad.[18] Trans-border flows of personal information, i.e. the point-to-point exchange of data containing personal information for national and international business purposes (shipping, travelling), or as a business itself (i.e. for marketing), led to the 'internationalization of privacy threats.' This paved the way to the acknowledgement of the value of personal information contained in electronic, machine-readable data. It called for the development of a right to data protection safeguarding 'the digital/electronic persona' as distinct from the physical persona, needing specific legal protection, substantiated in procedural rights allowing to control the dissemination of personal information.[19] The ubiquitousness of computing and related applications (e.g. the Internet of Things), and the success of "big data", are pushing the legal discussions further, and call for the development of the right to be forgotten.

2.2 The evolution of privacy and data protection as relative rights

Such values, already enshrined in many constitutions,[20] informed the legislative development of the right to privacy, formally initiated by the adoption of the Universal Declaration of Human Rights (hereafter UDHR) 1948.[21] The latest formulation of the rights to privacy and data protection is enshrined in articles 7[22] and 8[23] of the European Charter of Fundamental Rights (hereafter EUCFR).[24] These two articles incorporate the progress made by earlier instruments applicable in the EU.[25] Consequently, it can be argued that the three main functions performed by all relevant instruments – the determination of the legal substantive meaning, mechanism of protection, and boundaries, of the rights – should be read together.

---

18 Younger (Hon.), Kenneth (Chairman), 'Report of the Committee on Privacy', in Home Office (ed.), (London: H. M. Stationery Office, 1972), Abraham L. Newman, Protectors of Privacy. Regulating Personal Data in the Global Economy, Ithaca: Cornell University Press (2008), Rodotà, Elaboratori Elettronici E Controllo Sociale, Giovanni Sartor, L'informatica Giuridica E Le Tecnologie Dell'informazione. Corso Di Informatica Giuridica, Torino: Giappichelli Editore (2010).

19 Article 12, Anonymous, 'Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data', in Council Of Europe (ed.), (CETS No. 108; Strasbourg, 1981), Anonymous, 'Additional Protocol to the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Regarding Supervisory Authorities and Trans-Border Data Flows', in Council of Europe (ed.), (Strasbourg, 2001), Organization for the Economic Cooperation and Development, 'Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data', in Council of the Organization for the Economic Cooperation And Development (ed.), (1980).

20 Johannes Morsink, *The Universal Declaration of Human Rights: Origins, Drafting and Intent*, Philadelphia: University of Pennsylvania Press (1999).

21 General Assembly (3rd Session), 'Universal Declaration of Human Rights. Resolution 217', in United Nations (ed.), (1948).

22 Article 7 EUCFR reads, Everyone has the right to respect for his or her private and family life, home and communications.

23 Article 8 reads: 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.

24 'Charter of Fundamental Rights of the European Union', Official Journal C 303/1, (2007) pp. 1–22.

25 As clarified by the comment to articles 8 and 52.3 of European Parliament, Council, and Commission, 'Explanations Relating to the Charter of Fundamental Rights' (2007).

2.2.1 Legal formulations of the values underlying the two rights

The first formulations of the right to privacy attest to its universal relevance.[26] "Privacy" appears as an umbrella term encompassing the protection of mental and physical (spatial and bodily) integrity, intimate relationships, and information relating to such spheres, often grouped into four categories of privacy: bodily, relational, informational and territorial. Courts (and legal scholarship/jurisprudence) upheld and contributed to this versatile understanding. In fact, while they have adopted an expansive interpretation over time, particularly in relation to technical/technological developments, they have appeared reluctant to formulate a strict definition of the meaning/scope of the right. This may be functional to such technological developments, or the flexibility of issues pertaining to personal choice rather than morality or public policy. In fact, the meaning of privacy has expanded detailed with the progressive limitation of the power of religious or political institutions to regulate and sanction behaviours.

Informational privacy, or the right to personal data protection, has been the object of the most recent legal instruments, and is defined in more procedural terms. The OECD Privacy Guidelines[27] introduced norms, or 'principles'[28] to regulate the processing of the data (drawing substantially from the Fair Information Principles or FIPs), which were converted into law by the Council of Europe Convention 108[29]. Convention 108 further introduced the category of sensitive data, i.e. data that should not be processed unless specific safeguards apply.[30] Directive 95/46/EC and 2002/58/EC built on these two texts to refine the definition of personal data and the architecture surrounding them.

2.2.2 Creating mechanisms for the protection of the two rights

Article 12 UDHR, 8 ECHR and 17 ICCPR *(International Covenant on Civil and Political Rights)* focus on the activities of states. They clarify that states are under the legal obligation to refrain from unduly interfering with the right to privacy, and have positive obligations to take the necessary legislative measures to ensure that public or private parties do not unduly interfere with this right.

The data protection instruments, i.e. the OECD Guidelines and Convention 108, introduced procedural duties for data controllers. Data should only be processed for legitimate and clearly enumerated purposes, in line with the principles on data quality, security, information and transfers. Moreover, all instruments entitle data subjects with procedural rights to control the dissemination of their personal information. Furthermore, Convention 108 introduced the norm, codified in article 8 EUCFR, of independent oversight, entrusted to a data protection authority. The Convention 108 provisos were

---

[26] Article 12 UDHR, article 8 of the Council of Europe, 'Convention for the Protection of Human Rights and Fundamental Freedoms, as Amended by Protocols No 11 and 14', (CETS n° 005; Rome, 1950). Article 17 of the United Nations, 'International Covenant on Civil and Political Rights', (New York, 1966). Article 7 of the EUCFR should be read in line with article 8 ECHR, which it mirrors.

[27] Council of Europe, 'Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data', Organization for the Economic Cooperation and Development, 'Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data'.

[28] These are: collection limitation; data quality (ca. FIP information management); purpose specification (ca. FIP use limitation); use limitation (ca. FIP disclosure limitation); security safeguards (ca. FIP information management); openness; individual participation; and accountability

[29] For a more detailed account of the relation between the drafting of the OECD Guidelines and Convention 108, please refer to Porcedda, Maria Grazia, Mathias Vermeulen and Martin Scheinin, 'Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy. *Deliverable 3.2,* SurPRISE Project. Forthcoming', Florence: European University Institute (2013).

[30] Article 6 of 'Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data'. These are data revealing racial origin, political opinions, religious or other beliefs, health and sexual life, and data relating to criminal convictions, which are by their nature sensitive, susceptible of affecting the exercise and enjoyment of other civil and political rights.

further refined in the general data protection Directive 95/46/EC[31], the e-privacy Directive 2002/58/EC[32] and Regulation 2001/45/EC[33] (which established the European Data Protection Supervisor).

2.2.3 Setting boundaries to their application: privacy and data protection as relative rights

In all legal instruments referred to above, the right to privacy is not an absolute right. In other words, it can be interfered with by means of permissible limitations, which must respect a number of criteria that have been interpreted and clarified by case law.[34] Limitations must be provided for by the law of the member state (principle of legality), be non-arbitrary, and adopted for explicit purposes 'necessary for the protection of fundamental values in a democratic society', such as for reasons of state security,[35] public safety, monetary interest of the state, suppression of criminal offences, protection of the data subject, or protection of the right and freedoms of others.

2.3 Privacy and security: a complex relationship

2.3.1 In theory: privacy and security

The established meaning of the rights to privacy and data protection allowing for permissible limitations implies that, in principle, there is no opposition between their protection and the achievement of individual or public security. In fact, pursuant to article 2 of the Treaty on European Union (hereafter TEU), the EU is "founded on the values of respect for human dignity, freedom, democracy, equality, the rule of law and respect for human rights, " which include the rights to privacy and data protection. As acknowledged by the Court of Justice of the European Union, "The fundamental rights recognized by the Court are not absolute (…). Consequently, restrictions may be imposed on the exercise of those rights (…) provided that those restrictions in fact correspond *to objectives of general interest* pursued by the Community and do not constitute, with *regard to the aim pursued*, a disproportionate and intolerable interference, impairing the very substance of those rights."[36]

Objectives of general interest, or aims, pursued by the EU are "the promotion of peace, the preservation of its traditions and citizens' wellbeing."[37] This translates, first and foremost,[38] into the creation of an internal, borderless area, protecting citizens' fundamental rights, guaranteeing a high level of security and fostering access to justice, in respect of the different legal systems and traditions proper of member states: the Area of Freedom, Security and Justice (hereafter AFSJ).[39] Consequently, security is

---

[31] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, p. 31-50 (23 November 1995).

[32] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal L 201, p. 37-47 (31 July 2002).

[33] Regulation 45/2001/EC of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, Official Journal L8 , 1-21 (12.1.2001).

[34] For a complete discussion, see Porcedda, Maria Grazia, Mathias Vermeulen and Martin Scheinin, 'Report on Regulatory Frameworks Concerning Privacy and the Evolution of the Norm of the Right to Privacy. *Deliverable 3.2, SurPRISE Project*. Forthcoming', Florence: European University Institute (2013).

[35] As put by the Explanatory Memorandum, "The notion of "State security" should be understood in the traditional sense of protecting national sovereignty against internal or external threats, including the protection of the international relations of the State."

[36] Emphasis added, Court of Justice of the European Union (1089), 'C 5/88, Wachauf V Bundesamt Für Ernährung Und Forstwirtschaft', Judgment of the Court (Third Chamber) at paragraph 18.

[37] Article 3 TEU ('Consolidated Versions of the Treaty on European Union (Teu) and the Treaty on the Functioning of the European Union (TFEU)', (Official Journal C 83/01)).

[38] Paul Craig and Gráinne De Búrca, *European Union Law: Text, Cases and Materials*, Oxford (2011) 1320.

[39] Article 3.2 TEU, and article 67 of the TFEU ('Consolidated Versions of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU))'.

instrumental to the pursuit of the objective of general interests by the EU, and the protection of fundamental rights, including the right to privacy and data protection. In other words, national security can be regarded as a public good. The protection of public or national security is thus seen as a legitimate aim justifying restrictions on the exercise of the rights under analysis in a democratic society.

While ECHR article 5 and ICCPR article 9 refer to 'security of the person' as an individual right, the relationship between privacy and security is usually not formulated as a tension between two competing individual human (or fundamental) rights, but as a question of how far the collective goal of public security can constitute a legitimate aim that justifies permissible limitations to the individual right to privacy, or data protection. That is a meaningful question that can be addressed through legal analysis. The individual human right to security of the person has obtained little independent relevance, occasionally being applied by the UN Human Rights Committee as a right of a person living under violent threats from the side of third parties, to obtain positive measures of individualised protection from state authorities, such as a police escort.[40] The European Court of Human Rights, however, routinely addresses this issue as a positive obligation stemming from the right to life (ECHR article 2) or the prohibition against inhuman treatment (ECHR article 3), rather than as an issue under ECHR article 5.[41]

2.3.2 In practice: security versus privacy

In practice, after the terrorist attacks of the past decade, the already existing trend towards intelligence-led policing, i.e. law enforcement activities driven by the collection of personal information, has exponentially increased, leading to the increased use of security-oriented surveillance technologies (SOSTs) and related policies, also for petty crimes. In the security context, surveillance comprises *the targeted or systematic monitoring, by governmental organizations 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*.[42]

The ensuing policies framed the relationship between privacy (together with data protection) and security predominantly in terms of the need to "strike a balance" or establish a "trade-off" between security and rights.[43] Part of the problem of the "security vs. privacy" debate lies in the contested nature of the concept of security. "Security" is vaguely referred to in TEU articles 3.2 and 3.5, 21.2 (a) and (c). AFSJ-related policy documents describe it through "risks" or "threats" *'which have a direct impact on the lives, safety, and well-being of citizens.'*"[44] Threats are usually grouped in broad categories, which inform the basis of policy making in the AFSJ, and include "serious and organised crime, terrorism, drugs, trafficking in human beings and smuggling of persons" as well as "cybercrime, the management of (…) external borders and (…) natural and man-made disasters."[45] The vagueness of the concept, coupled with the emotional thrust for strong responses in the wake of security failures, such as terrorist attacks, have led to the adoption of policies based on the extensive processing of personal information, which

---

[40] See, William Eduardo Delgado Paez v. Colombia (Communication No. 195/1985), Final Views by the Human Rights Committee 12 July 1990.

[41] See, Opuz v. Turkey (Application No. 33401/02), Judgment by the European Court of Human Rights 9 June 2009.

[42] This definition of surveillance is based on the definition adopted in the FP7 project SURVEILLE, as modified for the purposes of SurPRISE. See, Surveille Project Consortium, 'Description of Work', Surveillance: Ethical Issues, Legal Limitations and Efficiency', (Seventh Framework Programme, European Union, 2011) at 46.).

[43] Ashworth, Andrew, 'Security, Terrorism and the Value of Human Rights', in Benjamin Goold and Lazarus Liora (eds.), *Security and Human Rights*,Portland: Hart (2007), pp. 203-226, Frank Dumortier et al., 'La Protection Des Données Dans L'espace Européen De Liberté, De Sécurité Et De Justice', *Journal de Droit Européen,* 166 (2010), 23, Stefano Rodotà, *Il Diritto Ad Avere Diritti* (Bari: Editori Laterza, 2012), Martin Scheinin, 'Terrorism and the Pull of 'Balancing' in the Name of Security', in Martin Scheinin (ed.), *Law and Security, Facing the Dilemmas* 11; Florence: European University Instite (2009a).

[44] Council, 'Draft Internal Security Strategy for the European Union: Towards a European Security Model', (5842/2/10; Brussels, 2010) at 3.

[45] European Commission, COM (2010) 673 Final. The Eu Internal Security Strategy in Action; Five Steps Towards a More Secure Europe,' (Brussels, 2010) at 2.

claim to 'strike a balance', i.e. weigh fairly security interests and privacy (and data protection) rights, but de facto often result in introducing excessive limitations to such rights, questioning their significance in our society.

2.3.3 Permissible limitations in recent legal instruments in the AFSJ

Some of the legal instruments disciplining the use of personal data for police and judicial cooperation recently adopted follow this trend. The Council Framework Decision 2008/977/JHA provides a clear example.[46] Firstly, the Framework Decision has a limited scope, as its provisions do not apply to domestic situations. Secondly, its articles 3.2, 11 and 12.2, taken together, almost provide for a blanket exception to the purpose limitation principle.[47] Thirdly, article 13 allows member states to transfer personal data received from another member state to either third states or international bodies without strict safeguards. Another departure from the purpose limitation principle is the increasing use by national law enforcement authorities (LEAs) and relevant EU agencies, such as Europol and Eurojust, of personal data stored in EU databases that were not exclusively set up for law enforcement purposes, such as Eurodac[48] and the Visa Information system (VIS).[49]

The general trend, whereby LEAs increasingly access data of individuals, who, in principle, are not suspected of committing any crime, informs also the Data Retention Directive.[50] According to the Article 29 Data Protection Working Party and the EDPS, its permissible limitations are insufficient.[51] The data

---

46 Council, 'Council Framework Decision 2008/977/JHA of 27 November 2008 on the Protection of Personal Data Processed in the Framework of Police and Judicial Cooperation in Criminal Matters', (OJ L 350), pp. 60 –71.

47 Article 3.2 provides an exception to the purpose-limitation principles insofar as it allows further processing if (a) it is not incompatible with the purposes for which the data were collected; (b) the competent authorities are authorised to process such data for such other purpose in accordance with the applicable legal provisions; and (c) processing is necessary and proportionate to that other purpose. The competent authorities may also further process the transmitted personal data for historical, statistical or scientific purposes, provided that Member States provide appropriate safeguards, such as making the data anonymous. Article 11 states that data may be further processed only for the following purposes other than those for which they were transmitted or made available: (a) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties other than those for which they were transmitted or made available; (b) other judicial and administrative proceedings directly related to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; (c) the prevention of an immediate and serious threat to public security; or (d) any other purpose only with the prior consent of the transmitting Member State or with the consent of the data subject, given in accordance with national law. Article 12 states that Member States shall not apply restrictions regarding data transmissions to other Member States or to agencies or bodies established pursuant to Title VI of the Treaty on European Union other than those applicable to similar national data transmissions.

48 European Commission, 'COM (2012) 254 Final, Amended Proposal for a Regulation of the European Parliament and of the Council on the Establishment of 'Eurodac' for the Comparison of Fingerprints for the Effective Application of Regulation (EU) No [.../...] (Establishing the Criteria and Mechanisms for Determining the Member State Responsible for Examining an Application for International Protection Lodged in One of the Member States by a Third-Country National or a Stateless Person) and to Request Comparisons with Eurodac Data by Member States' Law Enforcement Authorities and Europol for Law Enforcement Purposes and Amending Regulation (EU) No 1077/2011 Establishing a European Agency for the Operational Management of Large-Scale It Systems in the Area of Freedom, Security and Justice (Recast Version)', (Brussels, 2012).

49 European Parliament and Council, 'Regulation 2008/767/EC of 9 July 2008 Concerning the Visa Information System (Vis) and the Exchange of Data between Member States on Short-Stay Visas', (Brussels, 2008).

50 European Parliament and Council, 'Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC (Data Retention Directive)', (Brussels, 2006), pp. 54–63.

51 Article 29 Data Protection Working Party, 'Report 01/2010 on the Second Joint Enforcement Action: Compliance at National Level of Telecom Providers and Isps with the Obligations Required from National Traffic Data Retention Legislation on the Legal Basis of Articles 6 and 9 of the E-Privacy Directive 2002/58/Ec and the Data Retention Directive 2006/24/Ec Amending the E-Privacy Directive', (Brussels, 2010), Giovanni (Assistant EDPS) Buttarelli, 'What Future for the Data Retention Directive. General Remarks', in Discussion on the Commission Evaluation Reporteu Council Working Party on Data Protection and Information Exchange (Dapix - Data Protection) (ed.), (Brussels, 2011).

retained shall be provided to (1) the competent national authorities, (2) in specific cases, (3) for the purpose of the investigation, detection and prosecution of serious crime, as defined by each member state in its national law. The Data Retention Directive does not provide any further details on the procedures to be followed and the conditions to be fulfilled in order to gain access to retained data, which leaves room for heterogeneous interpretations in the acts transposing the directive into national law. Indeed, an evaluation by the Commission showed that "[M]ost transposing Member States, in accordance with their legislation, allow the access and use of retained data for purposes going beyond those covered by the Directive, including preventing and combating crime generally and the risk of life and limb".[52]

2.4 An alternative way of framing the debate: a core/ periphery approach

This deliverable challenges the assumption that the collective interest to, or public good of, security and the rights to privacy and data protection are irreconcilable in the EU. An analytical alternative to the security vs. privacy approach is the core/periphery approach based on a reinterpretation of Robert Alexy's theory of rights.[53] According to this constitutional law scholar and legal theorist, all legal norms are either rules (either/or) or principles (more/less). Even if Alexy sees constitutional rights mainly as broadly formulated principles, the theory can be applied to explain how any fundamental right would have an inviolable core (or more than one such core) sealed in a rule, and a periphery surrounding that core and subject to permissible limitations, such as those foreseen by article 8 ECHR, and articles 7 and 8 of the EUCFR, for privacy and data protection. Such a core/periphery approach to rights, reflected in EUCFR article 52(1), lays the basis for combining compliance with the rights to privacy and data protection and the needs of LEAs when conducting an investigation and, in a more general fashion, privacy and security, as opposed to simple theories of abstract balancing. The latter easily results in a choice between the two, and usually in always prioritizing security, hence eroding privacy to an empty shell. In contrast, the core/periphery approach allows a defence of privacy rights, so that they establish both absolute prohibitions in extreme cases and a rational frame for concrete assessment of permissible limitations in other areas.

It needs to be emphasized that the notion of a core, which corresponds to the term of "essence" in the text of the EUCFR, is of course just a metaphor. Some human rights are complex umbrella concepts that host a number of quite different substantive elements, or attributes.[54] A single human rights treaty provision is capable of hosting multiple "cores". Speaking of an "essence" or a "core" should not be seen as preventing contextual assessment, as the essence or core can be defined through a multitude of factors. In other words, it is not suggested that each human right has one and only one "core" that can be defined in absolute terms and would then remain the same for all situations and all times. Rather, the idea is to say that, in respect of a proposed intrusion, there is a need to question whether the intrusion would go so far that it would affect the essence or core of the right.

Three different criteria have been preliminary suggested as candidates to determine the scope of the core of the right to privacy: sensitive data as privileged content, information produced in the course of confidential personal relationships, and methods of intrusion.

---

52 European Commission, 'COM (2011) 225 Final, Report from the Commission to the Council and the European Parliament, Evaluation Report on the Data Retention Directive (Directive 2006/24/EC)', (Brussels, 2011) at 8.

53 Scheinin, 'Terrorism and the Pull of 'Balancing' in the Name of Security'. Robert Alexy, ' Constitutional Rights and Legal Systems', in Joakim Nergelius (ed.), *Constitutionalism - New Challenges: European Law from a Nordic Perspective* (2008).

54 The notion of 'attributes' was chosen to refer to the main substantive dimensions of a human rights provision in a project with the UN Office of the High Commissioner for Human Rights to identify indicators for the assessment of compliance with human rights treaties. The methodology for defining the attributes representing each human right was based, inter alia, on the General Comments of the respective treaty body and on an effort to find attributes that as far as possible are at the same time mutually exclusive and taken together comprehensive in relation to the substantive scope of the treaty provision.United Nations High Commissioner for Human Rights (Ohchr), 'Human Rights Indicators. A Guide to Measurement and Implementation', (New York and Geneva: United Nations Human Rights Office of the High Commissioner, 2012).

The inviolability of the essential core of any human right – in this case the right to privacy – is one of the steps in an analytically rigorous test for the permissibility of restrictions, whereby all of the following cumulative conditions must be met: (a) any restrictions must be provided by the law; (b) the essence of a fundamental right is not subject to restrictions; (c) restrictions must be necessary in a democratic society; (d) any discretion exercised when implementing the restrictions must not be unfettered; (e) for a restriction to be permissible, it is not enough that it serves one of the enumerated legitimate aims; it must be necessary for reaching the legitimate aim; (f) restrictive measures must conform to the principle of proportionality, they must be appropriate to achieve their protective function, they must be the least intrusive instrument amongst those which might achieve the desired result, and they must be proportionate to the interest to be protected; and (g) any restrictions must be consistent with other fundamental rights.

The test could also be interpreted as an instrument to determine the acceptability of the use of new technologies, whenever an interference with the right to privacy is the outcome (for a practical implementation of the test *see chapter 4.4*).

3. Security and the threat debate[55]

3.1 Securing security

Security problems are perceived as major challenges to modern societies. Terrorist threats, petty crimes, vulnerable infrastructures, global logistic chains, tightly knit, high speed, volatile international financial markets and networked computer technologies produce threat potentials that cannot easily be ignored. Also, it cannot be overlooked that many nation states are excessively extending their military and security industrial complexes and that this process is accompanied by an on-going and extensive readjustment of national and international legal regulations. With enormous technological progress, surveillance has become within a few decades an irrevocable part of everyday life. The wide array of threats seems to leave societies and their governments with a fundamental dilemma along the scales of *securing security* on one hand and *protecting privacy* on the other which is in the public debate most often explicitly or implicitly oversimplified as a trade-off between these two conflicting values or social goods.

Reviewing the legal provisions to defend a realm or the fundamental right of privacy against intrusions justified with imminent security threats reveals a kind of vicious cycle. Privacy defined in terms of data-protection is difficult to defend when the modern subject becomes increasingly "datafied" and the discourse about security threats takes on a dynamic of its own, producing ever more encompassing scenarios of future attacks affecting those fundamental values that justify a limitation of the right to privacy. The two concepts of *security* and *threat* constitute the Achilles heel for the legal protection of privacy. Unfortunately both concepts do not easily lend themselves to crisp legal definitions. This creates a problematic interface between law and intelligence (or between normative and cognitive arguments) when it comes to the definition of what constitutes a permissible limitation. Do the threat descriptions produced by LEAs justify a permissible limitation or not? Is there really a security threat requiring a highly intrusive exemption from the fundamental rule? To answer these questions a clear definition of threat, privacy and security would be required. [56]

One of the most general definitions of security as a "dynamic non-event"[57] demonstrates the problem of pinning down the concept with a precise definition. From a strictly logical point of view, the fact that no major incident has occurred does not constitute proof these things will not happen in the future. Starting from a worst-case scenario, i.e. from the assumption that major security threats can and will materialize in some near or distant future, justifies all measures deemed to prevent this from happening. Defining a state of the world through reference to the fact that "nothing happens" is disingenuous.

For operational clarity three readings of security can be distinguished: *objective*, *perceived* and *discursive* security. Objective security mainly falls into the realm of engineering, measuring the statistical probability of an event and relating this to the scale of damage caused (probability x damage = security risk). Such a statistical index measure may be used to support decisions and make projections about future events, but whether it is sufficient to justify a severe limitation of the fundamental right of privacy, requires a thorough debate. Perceived security refers to an individual's subjective perception of feeling secure or insecure. A number of studies in criminology[58] have demonstrated the so-called "security paradox": individuals may feel insecure despite the fact of low victimisation risks and vice

[55] By IRKS and ULD

[56] Issue related to the perception of security threats are further debated in: Pavone, Vincenzo, Sara Degli Eposti and Elvira Santiago, *SurPRISE project D2.2* (2013), chapters "3. Security, technology and democracy: the rise and implications of the trade-off between security and liberty", p. 25 - 43.

[57] Petra Badke-Schaub et al. (eds.) *Human Factors*, Springer: Heidelberg (2008) p. 21.

[58] See: Klaus Boers, *Kriminalitätsfurcht*, Pfaffenweiler: Centaurus (1991),
Jason Ditton, and Stephen Farrall, *The Fear of Crime*, Dartmouth: Ashgate (2000),
Dan A. Lewis and Greta W. Salem, *Fear of Crime: Incivility and the Production of a Social Problem*, New Brunswick: Transaction Publishers (1986).

versa. Objective and perceived security can produce conflicting results and while a high level of perceived insecurity may serve as a political pretext for intrusive security measures, affecting the fundamental right of privacy, it should not count as a sound argument in legal and political discourse.

Security as a discursive object has been elaborated in political science.[59] As has been demonstrated in security studies any social field can be "securitized", i.e. talking about a social object or process in terms of security changes the dominant discourse, mind-set, and policy options. Securitization demonstrates this complex transformation and remodelling of (societal) issues into matters of security and also the process in which these issues are then exposed to surveillance measures. Once a policy domain has been successfully securitized all other lines of argument (like social justice, fairness, or for that matter fundamental rights like privacy) are difficult to defend.

Furthermore the attempts on *securing (national) security* are flanked by an enormous increase of the national and international industrial-security-complex, ringlead by the global players in the security sector and shadowed by lobbyist groups.[60] The international industrial–security complex is on the global scale one of the fastest-growing industries. The European Commission recently proposed an action plan for the European security market to stabilize its share in the world security market, stating that the security industry is '*one of the sectors with the highest potential for growth and employment in the EU*', with a market value of between €26 billion and €36.5 billion.[61]

The security discourse appears to be highly contested and used in strategic contexts to promote vested interests. Loader and Walker state that security has become *the* political vernacular of our times.[62] Since the practice of government is becoming increasingly one of risk management[63] and risk management has become – especially under neo-conservative political ideologies – a growing industry[64] the visibility of a threat respectively the public visibility of some action taken against this threat seems to become increasingly more important than an actual threat level.

One of the key problems here is that security has become a sole responsibility of the LEA. Their expertise in the final instance provides the politically relevant information in the debate about privacy infringements and it is difficult to introduce any counter evidence into the political debate. A standard phrase of the security hawks states, that the absence of evidence is not the evidence of absence.[65] Hence even if no immediate evidence for a security threat can be produced, this is not considered as a proof to the contrary and according to the logic of LEAs privacy intrusive measures should legitimately be applied.

The dominant logic of security policies requires these measures to be applied comprehensively to each and every individual in order to sort out the potential predators. This again is easy to achieve in a society where each individual leaves many data traces that can be connected to a real person. Taking highly dramatized security threats as a justification (or pretext) these measures can be put to use to implement a large-scale, population-wide surveillance regime. Security then becomes the overriding and all-encompassing rationale for policies perceived as contributing to the prevention or detection of such an

---

59 Barry Buzan, Ole Waever, and Jaap De Wilde, *Security: A New Framework for Analysis*, Lynne Rienner Publishers, (1998).

60 For an overview of the development of the European Industrial Security Complex, see:
Ben Hayes, 'NeoConOpticon. The EU-Security Industrial Complex', Transnational Institute in association with Statewatch (2009). Statewatch ISSN 1756-851X.

61 European Commission Website: Enterprise and Industry: Security Industries:
http://ec.europa.eu/enterprise/newsroom/cf/itemdetail.cfm?item_id=6117&lang=en

62 Ian Loader and Neil Walker, *Civilizing Security*, Cambridge: Cambridge University Press (2007) p. 9.

63 Reece Walters, *Deviant knowledge : criminology, politics, and policy*, Cullompton; Portland, OR: Willan (2003). p.139ff.

64 Pat O'Malley, *Crime and Risk*, London et al: Sage (2010).

65 On the subtleties of the logic of prediction see: Nassim Taleb, *The black swan : the impact of the highly improbable*, London: Penguin (2008).

event. Reasonable assessment of proportionality is almost impossible, when security threats are framed in highly moralized terms. Nobody would want to be seen as supporting child pornography or sexual exploitation of children, offences typically used as pretext for the implementation of highly intrusive and all-encompassing forms of Internet surveillance.

But does the fact, modern communication technologies may be used by potential perpetrators coordinating their actions justify a comprehensive screening of Internet traffic to detect suspicious conversations or data traffic? Ample evidence suggests that only a tiny fraction of Internet traffic can be linked to criminals, nonetheless from a security logic this is irrelevant. Proportionality is not considered in the mind-set of a security expert. Any judgement about proportionality would require an assessment of the seriousness or magnitude of security threats. This however is difficult. Either the crimes to be prosecuted or the offences to be detected through surveillance are highly moralized (like with child pornography) or the preventive logic prevails, claiming that early detection of preparatory acts requires an in-depth screening of electronic communication.

The frame of reference or mind-set based on the logic of prevention assumes a world of full transparency and causality, where the future effects of events can be predicted or rationally calculated and hence a retro-prospective type of analysis can be applied chaining events in a clockwork fashion to identify the adequate points of preventative intervention. This is due to their very nature: security threats are projections of future events, typically perceived from a perspective of risk logic or risk-based reasoning. It is not the present state of affairs that matters, but the projected course of events and in order to identify tomorrow's perpetrators today's suspects have to be identified and this requires massive surveillance following the defensive reasoning of "better safe than sorry".

3.2 How threatening are the threats?

The security threats with the highest public and political priority are difficult to define. Terrorism for example is a catchall category, applicable to almost all situations. The word terrorism has been emotive to the European public throughout the late 20th century as it is primarily associated with murderous attacks on civilians. However in the 21st century this has become particularly emotive following devastating terrorist attacks in New York, London or Madrid. With the 9/11 attacks in the USA an empowered Islamist network provided the new "suitable enemy"[66] that the USA and Europe had been without since the collapse of the Soviet Union. This in particular enabled the perception of threats to domestic national security to move from the relative passive "Reds under the beds" Cold War spying fear to an active fear of neighbours with "guns, gas, germs or grenades under their pillows". Attacks by e.g. Islamic groups on domestic territories gave a justification for continued military expenditure for defending against international targets and also massive increases in domestic securitisation using the emotive threat of terrorism as a justification.[67] In public debates sometimes a faulty logic prevails claiming that since terrorists are Muslim, many Muslims must be terrorists (or at least supporting terrorist movements). As studies in newsmaking criminology have demonstrated, threat perception can be reinforced by media coverage and public fears are shaped by media images and stories since "crime sells".[68] Taking public arousal and concern about perceived threats seems not a valid basis to assess the magnitude or seriousness of threats.[69]

Modern societies have to come to terms with a main paradox. As Edwards points out, '*As individuals we have never been safer, wealthier (in spite of the current recession) or healthier. We have never had so many*

[66] see Loic Wacquant, 'Suitable enemies', *Punishment and Society*, Vol 1(2), (1999) p.215–222.

[67] Jason Burke, *Al-Qaeda: The True Story of Radical Islam*, London: I.B. Tauris (2004).

[68] Gregg Barak (ed.) Media, process, and the social construction of crime: studies in newsmaking criminology, New York: Garland (1994).

[69] See Pavone, Vincenzo, Sara Degli Eposti and Elvira Santiago, *SurPRISE project D2.2* (2013), chapter "2. Securiy, surveillance and technology: trends and issues" and chapter 3 "Security, technology and democracy: the rise and implications of the trade-off between security and liberty", p. 10 – 43.

tools to help us live our lives, but as a society our complicated lives, individual fears and increasingly high expectations have led us to believe that we are more at risk than ever.'[70]

This leads back to above mentioned problems of defining security. Measuring the magnitude of a threat and assessing probabilities of attacks is a difficult task. Furthermore debates about security enhancing counter-measures are often narrowed down to what has been term a "tech-fix approach". Alternative solutions are not considered. This raises two questions: do the proposed surveillance technologies (SOSTs) live up to their promises and what could alternative solutions look like?

3.3 Evidence based use of technology

Technological solutions to security problems do not necessarily work in the way they are intended to in the first place, sometimes even creating highly problematic side effects. Approaches focusing on a philosophy of more-of-the-same and using a techno-fix strategy tend to create perpetual mobiles, and the irrefutable logic of securing security based on non-events seems to become the dominant narrative of late modernity. In many cases, surveillance measures are prone to function creep; also, mechanisms of what Schneier neatly named "security theatre'"[71] are to be observed. While creating the feeling of improved security, these measures do not really reduce risks. The continuous increase of airport security provides a perfect case for this "theatrical approach".[72]

A good example for the lack of evidence regarding the often claimed security enhancement by surveillance technologies would be Smart CCTV. Studies related to the effectiveness of Smart CCTV differ greatly in their assessment of the technology. In other fields of SOSTs, there is no research at all giving insight to the question whether the individual technology in question provides any benefit in security matters. In general, technologies collecting data promoted to enhance security have in the recent years facilitated a shift from crime investigation towards a much stronger focus on crime prevention[73]. However, this shift does not come without severe issues tied to the civil rights of individuals. For example, Internet surveillance by means of Deep Packet Inspection (DPI) performs a mass surveillance of a large number of the population without a tangible indication of crime in the first place. Rather, this technology is used as a tool to generate an initial momentum of suspicion, triggering further actions of governmental entities entrusted with security tasks. It must be said that at this stage, the suitability of such data collections as evidence in crime persecution seems doubtful since this data often seems out of context (e. g. by searching for mere keywords in emails, in tweets etc.) and does not take into account other factual circumstances of the case at hand. Thus, such extensive data collections are often part of legally ambiguous dragnet investigation situations factually establishing a contradiction to the general presumption of innocence. Moreover, the adherence to concrete purpose-boundaries and the aforementioned general presumption of innocence is a basis foundation of a democratic society respecting citizens' rights. The more vague the purpose and factual requirements of such a technology deployment are, the more difficult it becomes finding a proper and acceptable balance between the desired security enhancement and the severity of the intrusion on citizens' rights. Thus, an assessment of technologies' usefulness with regard to the proposed security benefit is needed right from the start. (*See chapters 4.1 - 4.3.)*

What can be observed here is the gradual erosion of the legal safeguards built into the institutional arrangement of modern societies. Policing as an element of law enforcement was historically understood as a reactive move: should there be a reasonable suspicion brought forward against an individual, the police would begin to investigate and collect evidence to find out whether this suspicion could be substantiated. Should this be the case, further legal action would follow. There used to be a

---

[70] Charlie Edwards, *Resilient Nation*. Demos, (2009) p. 16.

[71] Bruce Schneier, Beyond Fear: Thinking Sensibly About Security in an Uncertain World, New York: Springer (2003).

[72] Comp. also Matt Richtel (2012), 'The mystery of the flying laptop', The New York Times (2012) http://travel.nytimes.com/2012/04/08/travel/the-mystery-of-the-flying-laptop.html?pagewanted=1&src=dayp Jeffrey Goldberg 'The things he carried', *The Atlantic* (2008). http://www.theatlantic.com/magazine/archive/2008/11/the-things-he-carried/307057/

[73] Comp. also: Schlehahn, Eva, SurPRISE project D.3.1 (2013).

strong link between norms or norm-breaking actions and legal sanctions. With the so-called preventive turn of policing, or law enforcement in general, this link was loosened.[74] Surveillance oriented security policies are implemented before any substantiated suspicion emerges, they do not have to be targeted to a specific suspicious individual and they may have negative consequences without a formal legal decision against the person(s) targeted. Moving into the field of preventive action and implementing surveillance technologies to detect suspicious behaviour it is difficult to assess the effectiveness of any given technology. Technologies implemented to improve security (through better detection or prevention of criminal acts) are difficult to evaluate since typically there is no independent evidence presented. In few cases (like CCTV) where a sufficient number of studies have been conducted, the evidence is mixed. The problem remains that the implementation of surveillance technologies is justified with regard to their presumed effectiveness in preventing or detecting serious criminal offences (or security threats) while at the same time no evidence is produced to substantiate such claims.

Here the crucial problem at the interface of law and technology becomes obvious. Legal provisions to protect privacy entail the option of permissible limitations. While from a normative legal point of view there are well defined criteria for the protection of an individual's privacy, it is difficult to assess in a rational way the seriousness of security threats justifying an intrusion into the private sphere and at the same time, it is very difficult to assess the impact of the technological measures suggested as necessary tools for surveillance in a given scenario. So while privacy in legal discourse seems to be well defined and normatively entrenched, the permissible limitations are not. [75] We will return to this problem below *(see chapter 4.4)*.

[74] Rosamunde van Brakel and Paul De Hert, 'Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies', *Journal of Police Studies*, (2011), Issue 20, Vol. 20, No. 3, pp. 163-192. Richard Ericson and Kevin D. Haggerty, *Policing the Risk Society*, Oxford: University Press (1997).

[75] Daniel J. Solove, *Understanding Privacy*, Harvard: University Press (2008).

4. Surveillance technologies in context

All across the globe, public debates have been criticizing surveillance-oriented security technologies (SOSTs) as being tools skirting or even crossing the boundaries of constitutional principles and ethics. In some areas, the human rights impact of such technologies is already acknowledged. But in some aspects, the decision over of the acceptability of surveillance technologies for security reasons is still very difficult. Technologies initially created in the military field become increasingly used domestically; even more so as an after-effect of the terrorist events of 9/11 and beyond. Governments worldwide are struggling to find the best options to maintain and enhance the security of their state, increasingly relying on technological solutions in doing so. There is a vast amount of new possibilities to process collected information, for example through Big Data techniques, creating a new dimension of surveillance. In fact, such possibilities enable a much more comprehensive scrutiny of European citizens, fully embracing their personal habits, beliefs, and life conditions.[76] So it seems logical that the impact of those technologies must be assessed closely and individually. This should include an assessment of possibilities to ensure or at least enhance privacy by design solutions. The concept of privacy by design (PbD) promoted by the Canadian Information & Privacy Commissioner Ann Cavoukian since the 1990s foresees that IT processes with their whole infrastructure and system as well as business and organisational processes should be designed with consideration of privacy issues right from the start, entailing the following core principles:

- Enabling privacy should be proactive, not reactive;
  privacy should be preventive, not remedial
- Privacy should be implemented as the default setting
- Privacy should be embedded into the design of the service/product from the very beginning
- Accommodation of all legitimate interests/objectives (positive-sum, not zero-sum)
- End-to-end security – full lifecycle protection of personal data
- Visibility and transparency should keep component parts and operations open to independent verification and forensics
- Respect for user privacy by offering knowledge and control[77]

To give an impression of such an improved contextual view of surveillance-oriented security solutions, we will in the following provide a brief synthesis review of the three different technologies, that will be discussed in the participatory events in work package 5: Smart CCTV, Deep Packet Inspection, and location trackers,[78] which have relevance for European citizens due to their use in domestic security contexts.

---

[76] Cf. Nick Taylor in Surveillance & Society, V 1, N 1 (2002) 'State Surveillance and the Right to Privacy' http://www.surveillance-and-society.org/articles1/statesurv.pdf

[77] Ann Cavoukian, Information & Privacy Commissioner Ontario, Canada, "Privacy by Design – The 7 Foundational Principles", originally published: August 2009, latest revision December 2012: "Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices" for a further overview of the initial concept, see http://www.privacybydesign.ca/

[78] This review is based on the findings of the previous research work being disseminated by the public deliverables D3.1, D3,2 and D3.3 conducted for the SurPRISE project. Moreover, these are the technologies exemplified in work package 4, serving as the main input for the multi-national participatory citizens' events (work package 5).

4.1 Smart CCTV[79]

In D3.1, we found that the current and on-going technological development to equip cameras with advanced functions and elements makes CCTV much more powerful than it has ever been. This "smarter" deployment of CCTV eventually enables a significantly more comprehensive surveillance of citizens in public space areas, thus affecting a number of fundamental rights and privacy issues.[80] Such advanced equipment is designed to encompass a number of the most different functions, such as, face and motion detection, crowd and directional flow detection, unattended/missing object detection, facial recognition, license plate recognition, targeting/positioning/tracking of subjects and objects, behavioural pattern and anomaly recognition, image quality and camera zooming enhancement, audio recording, and additional data matching and analytics capabilities.[81]

Does it work? Is it effective?

Drawbacks for the merely technical effectiveness have been especially found in lack of necessary prerequisites for camera positioning, lighting and other conditions to produce adequate image qualities.[82] So the overall configuration of the whole CCTV system setup is the most important factor to provide accurate results. Still, even advanced CCTV systems simply fail due to the sheer complexity of the scenery observed. Especially in the field of behavioural and anomaly pattern recognition, the technology is not yet advanced enough to provide fully adaptive systems.[83] Rather, these systems still rely on stereotypical predefinitions of unwanted behaviour to be matched to any actions captured by the camera, giving the entities developing and maintaining these algorithms the power to determine which kind of behaviour in public is deemed acceptable and which is not.[84]

Proportionality

Considering the dependence of behavioural pattern recognition enhancements on humanly controlled and stereotypical pre-definition has some impact on human rights matters, they pose inherent risks of discrimination of minorities as well as discouragement of citizens to exercise their own fundamental rights, such as privacy, freedom of expression and freedom of association.[85] Moreover, an omnipresent and all-permeating atmosphere of surveillance in all public spaces comes at the cost of significantly affecting citizens' behaviour. While being under constant watch, citizens start to act more adapted and restrained, reigning in carefree social behaviour. This has an especially strong effect on citizens belonging to minority groups by exposing them to an increased risk of social stigma, mobbing, stalking, or discrimination. However, at times it seems that in turn, the deployed technology provides only marginal benefit in terms of security enhancement.[86]

---

79 By ULD

80 For an overview of the increasing deployment of CCTV from the global perspective until 2004, see Clive Norris, Mike McCahill and David Wood, "The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space" titled 'The Politics of CCTV in Europe and Beyond', published in *Surveillance & Society,* vol. 2, no. 2/3 (2004).

81 For an in-depth description of Smart CCTV capabilities, see the analysis conducted within D3.1, chapter 2.2.

82 These weaknesses were also described in the ADDPRIV "*Deliverable 2.1:* Review of existing smart video surveillance systems capable of being integrated with ADDPRIV project" see p. 45.

83 See D3.1, chapter 2.2.1 on Smart CCTV, subsection on effectiveness of Smart CCTV and civil rights impact.

84 This is for example a weakness of the aforementioned "automatic action recognition" functionality, which pre-determines certain actions of individuals and thus is not yet able to ascertain unforeseen activities of individuals, see the article by Adi Robertson, "Military-backed surveillance prototype can read people's actions on video". It should be noted that these technologies rarely live up to the promises made by the system providers. The number of false positives/negatives and other malfunctions still is high.

85 See also Benjamin J. Goold, University of British Columbia, in 'CCTV and Human Rights' p. 27 ff.; published in the "Citizens, Cities and Video-Surveillance" paper of the *European Forum for Urban Security publication* of June 2010, titled 'Citizens, Cities and Video Surveillance - Towards a democratic and responsible use of CCTV'.

86 Peter Squires, Professor of Criminology and Public Policy at the University of Brighton examined the results of related studies in his article "Evaluating CCTV: Lessons from a Surveillance Culture" published on pp. 39 ff. in the "Citizens, Cities and Video-Surveillance" paper of the *European Forum for Urban Security publication* of June 2010, titled 'Citizens, Cities and Video Surveillance - Towards a democratic and responsible use of CCTV'.

Possible PbD approaches for smart CCTV

Potential Privacy by Design approaches in the field of CCTV are conceivable. These could for example be encryption techniques, comprehensive authorisation/access concepts and correlating access controls, including secure credentials and also logging functions for auditing/forensics. More tangible examples may be derived from the practical execution in individual use cases and specifically tailored privacy enhancing CCTV solutions offered by several vendors. A precise examination of the camera's pan, tilt and zoom capabilities shall be made with the issue of citizen's privacy in mind. Also, a specific setup regarding camera location, viewing angles, number of cameras, and time of monitoring, image quality and resolution may be a good first step to minimize the data collection to the level absolutely necessary.[87] In this context, the exclusion of certain areas not relevant for the intended surveillance purpose might also be executed by pixelating, blurring, or blackening (obfuscating/masking) of the not relevant areas within camera vision. This concerns persons and objects as well as sensitive areas within camera vision range. Such a process makes it possible e .g. to prevent the identification of individuals within camera vision range or to hinder the recording of areas belonging to private property.[88] However, dependant on which concept is realised, the process may be still be reversible. So preferable would be a method that does not record the areas in the video in the first place.

In short, the exclusion of certain areas (no insight to private property through doors/windows), exclusion of audio recording, recording limited to alarm-triggered events, de-identification of individuals (pixelating, blurring, obfuscating/masking), protection of recordings via encryption etc., access controls, and deletion routines may be of help to reduce the impact of this measure. We found that a prior use-case based Privacy Impact Assessment (PIA) might support a less intrusive and ethical deployment of the security measure.[89] Still, in some cases even this may not lead to satisfactory results, making the mere limitation of governmental surveillance necessary.

4.2 Digital network surveillance - DPI[90]

Internet surveillance entails the monitoring of data and traffic on the Internet. Often, security agencies are interested in the content of emails and social media websites. Deep Packet Inspection (DPI) is one technical possibility to conduct such surveillance. This is mostly facilitated through the Internet service providers deploying this technology on their servers which transmit the communication data of their customers. DPI inspects data packets arriving at and leaving from a device, thereby inspecting all seven layers of the data packets. By doing so, it recognizes varying information contained in Headers and Payload of each data packet, such as protocols, applications, URLs (Internet addresses), media content (specific instances of recorded music, movies, images or books), text strings, and data that with a specific format (e.g., credit card numbers, Social Security Numbers). Thus, this technology is well equipped to learn the content of the communication between many users.[91] DPI can be deployed by Internet Service Providers within their own infrastructures to scan the traffic being routed via their servers. However, for merely being able to provide the network services, only more shallow analysis of the data packets would be needed to extract the general technical information needed. Still, those companies often exercise full DPI for a multitude of purposes, ranging from own benefits in terms of obtaining data for targeted

---

87 Cf. the EDPS Video Surveillance Guidelines by the European Data Protection Supervisor, published March 17th 2010, p. 24 ff.

88 Cf. the Decision of the German Federal Administrative Court of January 25th 2012, (Az. BVerwG 6 C 9.11). The court decided that the capture of private property during a public space surveillance at the Hamburg Reeperbahn in Germany, where window, door and balcony images of a citizen's house was made, is unlawful and violated the concerned citizen's right to informational self-determination and privacy. The court determined that these sensible areas of private property shall be excluded from the surveillance measure.

89 Cf. Peter Hustinx, European Data Protection Supervisor, 'Video surveillance guidelines', March 17th 2010, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf

90 By ULD

91 Mark Bedner, 'Rechtmäßigkeit der Deep Packet Inspection" (translated „Lawfulness of the Deep Packet Inspection' p. 6 f., analysis created for the "Projektgruppe verfassungsverträgliche Technikgestaltung (provet)" at the Universität Kassel, published 2009 and available in German at: kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-2009113031192/5/BednerDeepPacketInspection.pdf

advertising to serving the demands of governmental security agencies.[92] For generic email surveillance, the data routed via the ISPs servers is screened and eventually, pre-defined additional actions could be taken, such as filtering or altering content. To endeavour a comparison with the non-digital world, it can be said that DPI technology matches the postman overstepping his boundaries to open all letters he is assigned to transport, and being able to read, alter, or delete content. In social networks, the above described DPI network monitoring is often conducted with new technologies of data mining. In doing so, filtering algorithms are tuned in for atypical behavioural patterns and the automated removal of inappropriate and illegal content.[93]

Does it work? Is it effective?

The surveillance of communication and social network content is mostly conducted to fight not only terrorism, but also other crimes, such as child pornography, copyright infringements, or even less serious offenses.[94] But the effectiveness regarding security enhancement in social networks remains doubtful since the predefinition of atypical user behaviour not always lead to satisfying results. The automated filtering and censoring of data for example triggered by certain keywords may still remain out of context and requires further human decision-making. There is little to no data how effective the above-described Internet surveillance technologies really are with regard to preventing and identifying terrorist and other criminal activities on the Internet.

Proportionality

In contrast to the dubious benefits of DPI being able to monitor, filter, analyse, store away and manipulate all kinds of digital citizen data, this technology has high potential to be misused for social discrimination, political repression, censorship and serious infringement on sensitive areas of private life.[95] Due to the intrusive nature of this technology, the risk of so-called over-enforcement by the installation of mass surveillance affecting a large number of the population is very high.[96]

Possible PbD approaches for DPI

At the moment, this technology provides no known Privacy by Design implementations. It must be said that since the very nature of this tool is the surveillance of all communication data packets being transmitted through the network server, the integration of privacy-preserving restrictions seems very difficult if not even impossible. Thus, is appears doubtful whether a less intrusive and ethical deployment of this technology is possible without at the same time neglecting its security purpose. Though restraints upon DPI deployment for privacy risk mitigation by limiting depth, breath and the retention of obtained data may be thinkable, the possibilities of communication interception remain vast and unlimited. However, public awareness focused in the recent times more on the aspect of DPI enabling mass surveillance at the point of network nodes of Internet service providers, showing the fairly broad scope of this tool as well as the inherent risks to the civil rights of European citizens. Moreover, not only the citizens themselves are at risk. Rather, this technology is also prone to be used by foreign countries, e. g. for industrial espionage. Thus, it may be of interest for a European state to prevent this broad DPI surveillance of internet communication in genera. This can e.g. be achieved by

---

92 Cf. Seth Schoen, Electronic Frontier Foundation (EFF), 'Legal Struggles Over Interception Rules in the United States' https://www.eff.org/pages/legal-struggles-over-interception-rules-united-states

93 Robert Booth "Government plans increased email and social network surveillance", *The Guardian,* April 1st 2012, http://www.guardian.co.uk/world/2012/apr/01/government-email-social-network-surveillance

94 Christian Fuchs, 'Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society", The Privacy & Security Research Paper Series, Issue #1 (July 2012). http://www.projectpact.eu/documents-1/%231_Privacy_and_Security_Research_Paper_Series.pdf

95 Cf. Ben Wagner, "Deep Packet Inspection and Internet Censorship: International Convergence on an 'Integrated Technology of Control", p. 2 f.; Christian Fuchs, "Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society" p. 25.

96 Cf. Hiram A. Meléndez-Juarbe, University of Puerto Rico Law School, "Intermediaries and Freedom of Expression" p.1 f., Essay translated by University students Edgardo Canales and Marini Rodriguez, available at: http://www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/04-Intermediaries_Freedom_of_Expression_Hiram_Melendez_Juarbe.pdf

end-to-end-encryption, anonymising technologies, and efforts to enable a routing of domestic communication solely or at least mostly within the state's own borders.

4.3 Location tracking[97]

In the digital era, mobile communication enables the use of a variety of location services having become an integrated part of our lives. These services cover a multitude of different purposes in several areas, ranging from military, health care, retail, postal, and civil use. The most common uses of such services are precise timing, frequency calibration, and location for further service provision such as mobile communication and navigation.[98] The mobility of persons and assets has thus become another aspect of security in public space, thus reinforcing the desire of intelligence and police agencies to obtain location or even more precise geo-location information where needed. In this context, most real-time location systems nowadays are in-built components of wireless systems. In D3.1, we have described different methods to obtain location information from mobile devices in order to track individuals. This e.g. can be done, but not exclusively, by GPS positioning, cell tower records for mobile phone location data, and Silent SMS. Typically, the network, i. e. the telephone service providers are involved by security agencies to obtain precise geo-location or simple location data from GPS satellites or cell towers. Moreover, so-called Silent SMS or Stealth Ping can be used to determine of a mobile phone is switched on and to test the network performance. To achieve this, specific Short Message Services (SMS) are sent to the device without the device owner being able to notice the arrival of an incoming message. This quiet message triggers a backping to the network provider, transmitting the IMSI code of the device, which allows further identification and localisation.[99]

Does it work? Is it effective?

In the recent years, it was revealed in several countries that the mass application of location trackers by security agencies has significantly increased[100] All these above mentioned methods of location tracking have one thing in common: some location data is collected and processed in order to provide the network services of a mobile device. Whether it is the routing of incoming or outgoing calls, an accurate geo-location, the provision of navigation and timing services, the data thereby being collected and processed are needed by the network providers to be able to perform these tasks. Due to this fact, these tools to obtain location data are fully functional and may reveal the location of an individual searched for. Still, this preconditions that the active security agency knows which mobile device this person is using, e.g. by matching the obtained data sets to a unique identifier known beforehand (e.g. the IMSI/IMEI numbers of a phone, or the phone number).

Proportionality

Especially repeatedly collected or requested location data, even in anonymised or pseudonymised form, may reveal information about frequently visited places, enable predictions about future whereabouts, determination of means of transportation (by foot, car, etc., how fast is the person moving?), allow an assessment of likely living or work places, and last but not least make the identification of the individual possible.[101] The positioning, location and tracking of mobile devices may be prevented or circumvented

---

97 By ULD

98 Jim Gray, Microsoft Research San Francisco, in the foreword of 'Location-Based Services' published by Jochen Schiller & Agnés Voisard (2004).

99 See D3.1, chapter 2.2.4 on Location tracking.

100 For examples, see: F-Secure Blog entry of December 29th 2011, "440,783 '"Silent SMS" Used to Track German Suspects in 2010'. https://www.f-secure.com/weblog/archives/00002294.html;
Eric Lichtblau, 'Wireless Firms Are Flooded by Requests to Aid Surveillance', *The New York Times,* July 8th 2012. http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?_r=2&ref=surveillanceofcitizensbygovernment; Kevin Bankston, article of December 1st 2009 for the Electronic Frontier Foundation, "Surveillance Shocker: Sprint Received 8 MILLION Law Enforcement Requests for GPS Location Data in the Past Year" https://www.eff.org/deeplinks/2009/12/surveillance-shocker-sprint-received-8-million-law

101 Hilty/Oertel/Wölk/Pärli, 'Lokalisiert und identifiziert – wie Ortungstechnologien unser Leben verändern', p. 71 *Zentrum für Technologiefolgen-Abschätzung (TA-Swiss)* (2012). http://www.ta-swiss.ch/ortungstechnologien/

by using different techniques. But these come along with significant disadvantages and dangers.[102] As far as these methods of surveillance are used, critics have pointed out that some do not allow for a limitation of the data collection. This is especially the case of the cell tower records, which have been repeatedly requested en masse by security agencies, and often without sufficiently substantiated indication of criminal threats. So such broad measures mostly concern data of innocent citizens being subjected to comprehensive surveillance.

Possible PbD approaches for location trackers

Due to the above described nature of the communication, navigation and timing services being offered by the respective network providers, the collection and processing of personal data seems very difficult if not impossible to avoid if one wants to use these services at all. In this context, potential Privacy by Design approaches from the technological side are yet to be developed. Already, some first tentative steps have been taken to undertake research, trying to address these issues e.g. by means of anonymous authentication towards the network, pseudonymisation of network identifiers, new techniques of pinpoint location dissipation or obfuscation, and improved encryption of communications.[103] However, until such research has achieved a sufficient level of efficiency and deployment, the most effective privacy-preserving approach so far is at the time being the merely organisational measure of restricting access to the databases.

4.4 The test for permissible limitations in practice[104]

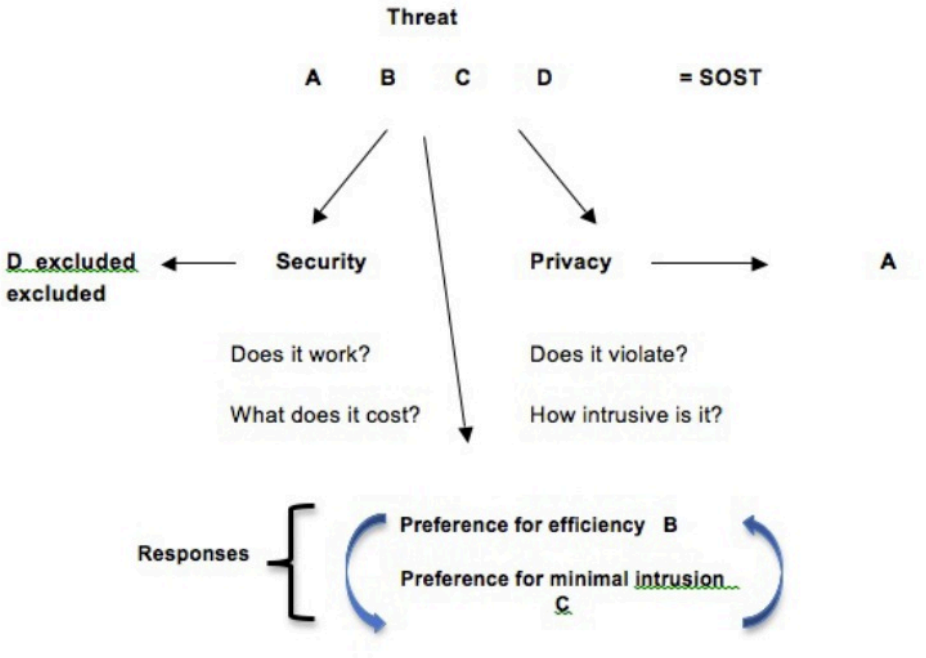
As this brief review of publicly announced threats and surveillance technologies demonstrates there are severe imbalances between security gains, privacy intrusions and effectiveness of surveillance oriented security technologies. Plotting the technological perspective against the test of for permissible limitations as developed from a legal perspective yields a number of interesting results.

The overall logic of this test can be summarized in the following graphical representation, starting with a "threat" and scrutinizing a number of technologies (A, B, C, D) against the relevant criteria of security gain and privacy intrusion.

[102] See D3.1 chapter 2.2.4 for details per technology on this aspect.

[103] Cf. Julien Freudiger, "When Whereabouts is No Longer Thereabouts: Location Privacy in Wireless Networks" École Polytechnique Féderale de Lausanne, p. 29 ff. (2011).

[104] By EUI



We assume that this test for permissible limitations modified by the core/periphery theory, illustrated in the model above, could provide a tool for evaluating the acceptability of SOSTs and SOSSs.

For each threat requiring a solution 'necessary in a democratic society', multiple SOSTs: A, B, C, and D, are existing. The first step consists in appraising the effectiveness of the technology, or answering the question "does it work?" (but see the limitations expressed *supra*, *chapter 3.3*) In our model, we imagine that, since D does not work in actually producing better security, it should be excluded. Therefore, the second step consists in appraising whether A, B, and C violate the core or otherwise go beyond the permissible limitations of privacy. In our illustration, we imagine that A does not pass the test for permissible limitations, and should thus be excluded.

The final choice between SOST B and C depends on a proportionality assessment. It is not self-evident that the more efficient SOST B should be selected, if, at the same time, it is much more intrusive into privacy than its alternative C is. If a clearly greater protection of privacy can be achieved through C, and if simultaneously a level of security close to that guaranteed by B can be reached, or even exactly the same degree of security at a minimally higher (financial) cost, then C should be selected. If, on the other hand, B provides for a much higher degree of security than C, then an effort should be made to reduce B's intrusiveness into privacy and data protection (i.e. in-built Privacy by Design, security features, data quality features etc.), and one is allowed to choose B, while securing that after the modifications the privacy intrusion is proportionate to the security benefit obtained.

This model illustrated how a proper assessment of proposed SOSTs can result in the optimization of both security and privacy, instead of a simple, abstract choice between them. Either B or C can be modified to produce the optimal result so that both security benefits and privacy protection are obtained at a high degree.[105] This corresponds to Alexy's theory of principles as optimization norms. However, before reaching the stage of optimization (between SOSTs B and C) we had already excluded SOST A as it was incompatible with the core of privacy (with the normative quality of a rule).

[105] For an alternative approach, see the DESSI project, http://www.tekno.dk/subpage.php3?article=1763&survey=15&language=uk.

The core-periphery test can thus be applied to the technologies described in the *chapters 4.1 to 4.3:* GPS-based location trackers, smart CCTV, network surveillance by means of deep-packet inspection engines (and surveillance by means of Trojan Horses).

Smart CCTV

If smart surveillance measures want to be compliant with the applicable fundamental rights legal framework, they must be based on a particularly precise domestic law, which must give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to such measures.

In particular, the use of such measures has to be proportionate 'to the prevention of concrete risks and specific offences – e.g., in premises that are exposed to such risks, or in connection with public events that are likely reasonably to result in such offences'.[106] In order to avoid abuses, an independent authority should have access to the source code of smart surveillance cameras in order to ensure compliance of these technologies with the rule of law.

GPS-based location trackers

A core/periphery theory of rights would suggest that only investigations into the most serious offences would justify the combination of GPS data with other datasets. In practice, however, it seems unclear how a judge would be able to prevent law enforcement officials from entering a specific location in a tool such as Google Maps in order to get more information about certain facilities that are nearby a suspect's location.

DPI/Trojans

In D3.2 we explained in detail how DPI violates several facets of the rights to privacy and data protection. DPI treats all citizens as potential suspects, since it can screen the communications of innocent citizens. In fact, the determination of what constitutes an "anomaly" can be made on discriminatory grounds, and on technical parameters that are difficult for LEAs to control and appraise from a legal perspective.

Moreover, DPI could violate the prohibition of processing sensitive data enshrined in article 8 of Directive 95/46/EC, and as such could violate one potential element of the core identified in section 4. DPI infringes data protection principles such as openness (most users are unaware of the existence of the system, which often is deployed covertly) and individual participation (users cannot oppose the processing, as is usually the case for surveillance technologies). As such it is always used without the knowledge of the user, which makes it a more intrusive technology to the core of the right to privacy.

Since the integrity of the gathered data cannot be verified and unlimited information can be easily accessed and used for a wide variety of purposes, DPI is very hard to square with key data protection principles such as data quality, collection limitation and purpose specification (if the extra data collected leads to further uses than the one initially envisaged).

Crucially, it can breach the prohibition of automated individual decisions enshrined in article 15 of Directive 95/46/EC.[107]

Its use by Internet Service Providers for their own purposes,[108] and for security purposes, such as data retention (laid down by the Data Retention Directive),[109] and child pornography,[110] is highly unlikely to

---

[106] Article 29 Data protection Working Party (2004) at 13.

[107] For a discussion of the legal uses of DPI, see European Data Protection Supervisor (EDPS), 'Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data' (2011) (OJ C 34/01).

[108] Court of Justice of the European Union (2012), 'Case C 360/10, Belgische Vereniging Van Auteurs, Componisten En Uitgevers Cvba (Sabam) V Netlog Nv', Judgment of the Court (Third Chamber).

[109] European Parliament and Council, 'Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC (Data Retention Directive)'.

pass the very first part of the permissible limitation test, namely the principle of legality. It would breach, among others, article 15.1 of the e-Commerce Directive (31/2000/EC) (prohibition to monitor the information which they transmit or store), article 5 of the e-privacy Directive (2002/58/EC) (prohibition of violating the confidentiality of communications), and article 5.2 of the Data Retention Directive (prohibition to retain the content of communications).

As such, most uses of DPI would be legally questionable. The use of a less intrusive technology should be preferred, such as the surveillance of individual devices, and their incoming and outgoing traffic, by means of Trojan Horses, in strict accordance with the permissible limitations test.

In order for Trojans to be legally acceptable, the restrictive measures should be in line with the principles of law (lawfulness), and leave no room for ambiguous interpretation, as elucidated by the ECtHR and the ECJ. The essence of privacy and data protection should be protected and in particular sensitive data and data that is the product of intimate, confidential relationships shall not be processed, or their use kept to the minimum necessary for the investigation. By means of illustration, sensitive data could be processed (under ethical review, i.e. by a panel of independent and trustworthy experts) only if a court order provides for it[111]; otherwise, the data should be promptly discarded, and considered inadmissible as evidence.

Also, unauthorized use must be prohibited: Trojans shall only be used in conjunction with an order issued by the judiciary. Restrictions must be necessary in a democratic society, either by genuinely meeting the objectives of general interest recognised by the EU (and the European Court of Human Rights) or by protecting the rights and freedoms of others. The performance of surveillance by Trojan horses must be proportional to the objective pursued and subject to scrutiny. Moreover, it should be necessary and the most appropriate instrument for reaching the legitimate aim it is used for. Restrictions to privacy and data protection must be consistent with safeguards provided by the ICCPR, the ECHR and the EUCFR.

4.5 Security impact and side effects[112]

Technology is neither good nor bad nor is it neutral.[113] Technological systems like mobile phones, credit cards, or location trackers and GPS are not explicitly designed as surveillance measures but can be used for surveillance purposes.

Location trackers

Experts from the law enforcement community often point to the positive effects location trackers can have to prove innocence by providing an alibi. As seductive as this argument may sound, at face value it is based on the assumption that the odds are high to be (wrongly) identified as a potential suspect. It also demonstrates a specific mind-set: it is the authorities who will determine – based on more or less

---

[110] European Data Protection Supervisor (EDPS), 'Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on Combating the Sexual Abuse, Sexual Exploitation of Children and Child Pornography, Repealing Framework Decision 2004/68/Jha', (2010), European Parliament and European Council, 'Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and Replacing Council Framework Decision 2004/68/JHA', (OJ L335/1).

[111] This is particularly urgent, especially since the use of Trojans takes place in the context of public-private partnerships, or is leased to private companies. As a result, LEAs may not have full control on the functioning of Trojans, especially due to possible lack of competence in ICTs, and should thus be assisted by independent competent technical expertise. See, for instance, Ronald J.Deibert, 'Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace', *Millenium - Journal of International Studies,* 32/2 (2003), pp. 501-30.

[112] By IRKS

[113] Melvin Kranzberg, 'Technology and History: "Kranzberg's Laws"', *Technology and Culture* 27, Nr. 3 (July 1986): pp. 544–560.

sophisticated surveillance-based evidence – who deserves to be seen as innocent and who doesn't. While there may be crimes where technologies for location tracking can prove useful for police work, the low thresholds for the applicability of such technologies outside the narrow realm of thief taking is highly problematic. While from a technology perspective location tracking seems to be a promising solution for target hardening and tracking of stolen goods[114] smart systems can be used to collect intelligence on public gatherings of e.g. political activists, providing the basis for a ecology of political unrest; they can work as a low cost and informal type of electronic necklace and they can provide the database for all sorts of social sorting[115], providing circumstantial evidence and fostering social exclusion and control also outside a law enforcement context.[116] The privacy issues related to these technologies are manifold and have been discussed for quite some time.[117]

Internet surveillance (DPI/Trojans)

Cybercrime as a comparatively new threat is for instance triggering hitherto unprecedented efforts by state authorities to gather data in order to combat the perceived threats emanating from the new cybercriminals. Although it is from a critical perspective far from clear whether cybercrime really creates big damages, there are nonetheless all sorts of surveillance measures justified with reference to this threat.[118] Mattelart observed *'as soon as the internet emerged as a public access network, geostrategists sought to define the stakes and the protagonists involved in noopolitik, i.e., the politics of knowledge in the broad sense. This notion, introduced in 1999, encompasses the (civil ('netwar') and military ('cyberwar') aspects of strategic control of information, knowledge and know-how, with a view to achieving given global political and economic objectives.'* [119]

ENISA published in 2013 the "Threat Landscape Report"[120] defining cyber threat agents as *'any person or thing that acts (or has the power to act) to cause, carry, submit or support a threat*'. This is followed by a list of these threat agents basically including almost everyone: nation states, terrorists, cybercriminals, hacktivists, corporations and also employees.[121] This demonstrates that almost everything and everyone is perceived as a potential threat to security in cyberspace. As pointed out above *(see chapter 4.4.1)* it is hardly possible to limit DPI in a meaningful way, when "screening" the Internet. Any targeted measures, like the use of Trojans almost always collects data from individuals that would infringe the entrenched "core" of their privacy

With regard to threats justifying privacy infringements it should be noted, that some of the presumably criminal offences discussed here are similar to the discussion about privacy protection. Illegal downloads defined as violations of IPR show the same basic structure as infringements of privacy rights:

---

[114] Rainer Mautz, Washington Ochieng, David Walsh, Gary Brodin, Andy Kemp, John Cooper and Thanh Son Le 'Low Cost Intelligent Pervasive Location Tracking (iPLOT) in All Environments for the Management of Crime', *Journal of Navigation*, 59, pp. 263-279.

[115] See Roger Clarke, 'Person-Location and Person-Tracking: Technologies, Risks and Policy Implications, *Technology & People* ,Vol. 14, No. 2 (2001) pp. 206-231.

[116] What can neatly be shown in this domain of surveillance technology is the cross-fertilization of crime science and social science, see Irvin B. Vann and G. David Garson, 'Crime Mapping and Its Extension to Social Science Analysis' *Social Science Computer Review*, Vol. 19. No.4 (2001), pp. 471-479.

[117] See e.g. Robert P. Minch, 'Privacy Issues in Location-Aware Mobile Devices', *Proceedings of the 37th Hawaii International Conference on Systems Sciences* (2004) pp. 10-19;
Laura Perusco and Katina Michael, 'Location-Based Services and the Privacy-Security Dichotomy', *Proceedings of the 3rd International Conference on Mobile Computing and Ubiquitous Networking*, London (2006) pp. 91-98.

[118] See for instance, Dinei Florencio and Cormac Herley, 'The cybercrime wave that wasn't', *The New York Times Sunday Reviev* (2012). http://www.nytimes.com/2012/04/15/opinion/sunday/the-cybercrime-wave-that-wasnt.html?_r=0

[119] Armand Mattelart, *The Globalization of Surveillance,* Cambridge, Malden: Polity, (2010), p. 137.

[120] ENISA: Website: http://www.enisa.europa.eu/media/press-releases/new-report-on-top-trends-in-the-first-cyber-threat-landscape-by-eu2019s-cyber-agency-enisa

[121] ENISA; Ibid; "Threat Landscape Report" p. 24ff, for download on the ENISA-website: ENISA Threat Landscape Published.pdf

no material objects are involved and no intrusion of any physical space takes place. What happens is the use of data without the consent of the person/organisation claiming a property right with regard to this use. Spelling IPR as Individual or Informational Property Right makes the point clear. Using person-related data for surveillance purposes can be seen as a violation of such Informational/Individual Property Rights or the right of informational self-determination.[122]

Obviously there are offences (or threats) materializing exclusively in virtual space. The damage caused by illegal downloads involves a violation of the right of legal use of an abstract data structure. On the one hand there are threats, where legally protected data are used to perform illegal acts and cause tangible damage in the material world (e.g. using a stolen PIN code to draw cash from an ATM, or manipulating software controlling complex technical systems like power plants, public transport systems, etc.). Threat scenarios presented by the security community and LEA do often not distinguish between these two forms. Both figure as "cybercrime" and are used to ask for more control of virtual space including more use of person-related data for surveillance.

The rise of the World Wide Web could be perceived either as one of the greatest chances in the history of mankind, allowing for access to sheer indefinite knowledge resources and global communication or as a curse, opening up sheer indefinite possibilities for violation of intellectual property rights, copy rights and privacy rights. Which direction the course will take on a global scale in the near future is impossible to determine. Although serious attempts are being made to regulate and restrict cyberspace on a global basis, they have not led to any consensus so far. The most recent attempt at global regulation – made at the International Telecoms Union (ITU) Conference in Dubai at the end of 2012 aiming at ratification of an UN Treaty of International Telecommunications Regulations (ITR) failed.[123]

Smart CCTV

As already elaborated, the security enhancement of smart CCTV is highly dependent on specific technology and context of deployment. Studies for Smart CCTV have shown varying results. Affective crimes and crimes committed under the influence are typically not preventable by the visual observation of a public space. This is also true in cases where the observation is not sufficiently complemented by correlating action of responsible security agencies once an incident occurs. Moreover, the perceived feeling of security by the mere perception of CCTV surveillance seems rather doubtful. In fact, it could be assumed that by the presence of CCTV cameras in public space, citizens rather become more aware of the lacking security of this place and thus creating feelings of insecurity.

Similar concerns may apply to location trackers and DPI, which both may be effective from a pure technical point of view but also do not provide reliable facts about the real security impact of these technologies. What can be said at this time is that under the impression of the terrorist events of 9/11 and afterwards, governments of the European Union and beyond have been lacking in finding objective and effective assessment of security-oriented surveillance technologies, shifting the focus towards a surplus of security and thereby often valuing the personal freedoms and rights of their citizens considerably less. In doing so, the distinction between the individuals' security perception on the one side and real threat potentials on the other has become blurred, leading to the frantic deployment of security solutions mostly promoted by suppliers without reflecting upon their factual usefulness for the intended purposes. The security engineer Bruce Schneier fittingly described this phenomenon already in 2008, stating *'Security is both a feeling and a reality. And they're not the same'*, [124] highlighting the fact that a warped perception of the real circumstances and facts may lead to false assumptions in various ways, including the severity and probability of security risks, the effectiveness of (also technical) countermeasures, the magnitude of costs and other relevant side effects, such as the impact on civil liberties.[125] Nowadays, knowledge even slightly seen as relevant for countering security threats is

[122] Comp. also: Vincenzo, Pavone, Sara Degli Eposti and Elvira Santiago, *SurPRISE project D2.2* (2013), p.24.
[123] Charles Arthur 'Internet remains unregulated after UN treaty blocked', *The Guardian* (2012) http://www.guardian.co.uk/technology/2012/dec/14/telecoms-treaty-internet-unregulated
[124] Bruce Schneier, "Psychology of security", January 18th 2008, http://www.schneier.com/essay-155.html
[125] Ibid.

increasingly sought to be obtained intelligence-driven, meaning that a lot of surveillance occurs covertly, often intransparently, even sidestepping supervision and accountability.

Conclusion: It may remain an open question if the magnification of governmental power over citizens via access to new technologies is just a side or a core effect; unambiguously, it is an effect that also counts for attackers on the security of a state. Consequently, it must be said that even with ultimately pre-emptive security measures, perfect security can never be achieved. Whether this dilemma can be resolved by focusing more on resilience rather than national security in the face of threats[126] is a debate not yet advanced enough to substantiate a final conclusion. However, in cases security-oriented technologies are considered to encounter threats, a more contextual view is needed to objectively take into account the capabilities of these technologies as well as the possible complementation by freshly inaugurated ways of data matching, linkage and profiling. Moreover, it must be kept in mind that while the impact of such security measures may find some relief by possible Privacy by Design approaches, PbD concepts are not an all-embracing solution and sometimes may be misused as a universal bogus pretence of legal, societal and ethical deployment.[127]

Threat scenarios operate with methods of social sorting, creating populations at or of risk. Social sorting uses person-related data to locate a specific individual in a category of potentially dangerous (or endangered) persons. This kind of threat assessment involves probabilistic assumptions about causal processes, individual propensities or vulnerabilities, cultural and social attitudes, all merged into a typified actor. Starting from this model actor or avatar, databases can be screened to identify individuals matching the threat profile. Such dragnet operations create abstract collectives or groups that can receive special attention and can become the target of further surveillance measures. Whether an individual is assigned to such a group remains unknown, and although some effects may be felt (e.g. receiving special treatment at security checks, being refused access to services) the person is not informed about her being labelled. It seems that such profiles often are operating on faulty reasoning, assuming if a high percentage of terrorists are Muslims then a high percentage of Muslims are potential terrorists and hence should receive special attention of security agencies. (*For greater elaboration on the issuse of lebelling, false positives etc. see report D3.3*)

[126] Such as proposed by Schneier in his essay *Our Security Models Will Never Work — No Matter What We Do,* published on Wired.com March 14th 2013, http://www.wired.com/opinion/2013/03/security-when-the-bad-guys-have-technology-too-how-do-we-survive/

[127] For more detailed elaboration on the limits of PbD approaches in individual fields of SOSTs, see Schlehahn, Eva, SurPRISE project D3.1.

5. Societal impact and alternative concepts[128]

5.1 Social threats of surveillance and impact on human rights

Any use of information technology and all surveillance measures are collecting and generating sheer indefinite masses of information in the first place; once transferred into classified knowledge such as personal profiles stored in corporate databases, the access to this advanced information is one of the keys for asymmetrical power relations. Lyon, for instance, stresses the category is becoming more important than the individual[129] – which is, strictly speaking, no less than fundamentally inhuman.

Surveillance technologies like (smart) CCTV or behavioural pattern recognition are aiming at eliminating every *potential* threat. This is pointing towards a pre-emptive society where everyone has at first to be considered a potential perpetrator – until proven otherwise. A steady shift from "post-crime" to "pre-crime" situation management can be observed.[130] Latest attempts to observe the Internet to filter out the "dangerous ones" in advance are already going beyond screening for keywords, dataveillance or data mining. So it is e.g. hoped to identify psychopaths on micro blogging networks such as Twitter via conducting word-pattern analysis of the tweets.[131] However, it is already an issue, that algorithmic models come inherently with the assumption of zero tolerance and therefore incorrect categorization of persons, based on standardized routine procedures is not uncommon.[132]

Individuals get selectively confronted with differential options based on their personal profile and classification. A growing number of studies highlight that an automated sorting of personal data into categories can re-produce marginalizing effects and create negative discrimination.[133] Matching with a specific (suspicious) subgroup either willingly or accidentally, either as a positive or a false positive yield fundamental consequences for the individuals, therefore techno-centrism has – at least from a social perspective – to be understood as a slippery slope. The question remains whether the technological fix theorem has to be questioned in its ability to serve as a (key) narrative of late-modernity.

European states are increasingly becoming more and more judgemental and regulatory on what used to be "normal" or leastwise accepted behaviour in public space. Increasingly everyday-life actions (like e.g. drinking alcohol in public) become issues controlled within new regulatory frameworks. Flanked by a variety of surveillance measures, neoliberal ideologies are encoding neoliberal values into the system of institutional efficiency and commercial profit is often excluding the social good.[134] Also, since knowledge creates power and vice versa[135] m*ass* surveillance per definition remains an asymmetric instrument in the hands of those in charge and power of the data.

---

128 By IRKS

129 David Lyon, Surveillance Studies: An Overview. Polity, (2007).

130 Rosamunde van Brakel and Paul De Hert, 'Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies', *Journal of Police Studies*, (2011), Issue 20, Vol. 20, No. 3, pp. 163-192.

131 Kasmir Hill, 'Using Twitter to identify psychopath', *Forbes Magazine* (2012). http://www.forbes.com/sites/kashmirhill/2012/07/20/using-twitter-to-help-expose-psychopaths/

132 Lyon, David. Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination. Taylor & Francis Group (2003).

133 Comp. Monahan, Torin, David J. Phillips and David Murakami Wood, 'Editorial. Surveillance and Empowerment', *Surveillance & Society,* Vol. 8, No. 2), (2010) pp. 106-112.
Also: Oscar H. Gandy 'Consumer Protection in Cyberspace', *tripleC-Cognition, Communication, Co-operation* 9, Nr. 2 (2011): pp. 175–189. http://www.triplec.at/index.php/tripleC/article/view/267

134 Monahan, Torin, David J. Phillips and David Murakami Wood, 'Editorial. Surveillance and Empowerment', *Surveillance & Society,* Vol. 8, No. 2), (2010) pp. 106-112.

135 Michel Foucault and Paul Rabinow, The essential works of Michel Foucault, 1954-1984. Subjectivity and Truth Vol. 1, Ethics London: Penguin (2000).

If *every potentiality of any threat* has to be eliminated before anything happens, the presumption of innocence – not necessarily in the first place in strict legal terms (applied in court cases) but rather as an everyday practise of those authorities securing security – is consequently going to be negated on a regular basis. If citizens do increasingly consider exercising democratic rights such as participating in political discourse, civic engagement forms of public protest etc. as potentially disadvantageous[136] or even dangerous, it can be spoken of the civil society being at stake.

In most general terms the impact of surveillance measures on human rights resides in the enforced ignorance of citizens in the face of pervasive surveillance. It is a key feature of surveillance practices, creating the difference between the (few) watchers and the (many) watched, that citizens do not know what kind of information or data is stored about them and how this information is used and processed. Not knowing what others know about oneself can create a state of ontological insecurity. Surveillance, designed to increase transparency for the watchers creates in-transparency for the watched. This is the logic of the panopticon.[137] While one strategy or reaction may consist in surrendering to such a panoptical regime it is hard to conceive how an active exercise of democratic rights can flourish in a panoptical order.

5.2 Alternative concepts

The following paragraphs offer a brief depiction on the variety of societal (conceptual) ideas that have to be taken into account investigating non-technical options to maintain - or enhance – societal security.[138] These concepts range from 1950ies 'security communities' theory to contemporary debates grouping around the wide framework of what is termed 'community resilience'. *(For an elaborate discussion see D3.3.)*

Adequate responses to security threats can be developed in different ways. On one hand a distinction can be made between *prevention and mitigation:* A security threat can be tackled in order to prevent the damage to materialize. On the other a response can focus on the minimization of damage caused by an event; or – possibly most promising – measures are to be taken towards strengthening *resilience,* and a resilience-aware society. It should be noted though when looking at alternative concepts that security as a frame of reference produces a specific type of discourse narrowing down the range of what can legitimately be uttered. Contemporary societies are obsessed with a rather narrow set of security problems and this obsession can be reconstructed from a very abstract vantage point of social theory. It is difficult to come up with alternative solutions as long as one accepts the implicit assumptions of mainstream political and administrative security discourses, which are primarily discourses of fear and threat.[139] Nonetheless there are some conceptual and theoretical approaches providing alternatives to the type of surveillance regimes promoted by contemporary security policies.

Security Communities: Introduced in the late 1950s and 1960s, the (constructivist) concept of security communities[140] influenced in the following decades a number of scholars mainly in the field of peace research. In the late 1990s Adler and Barnett adopted and scientifically augmented the concept.[141]

---

136 BVerfGE 65, 1 (15.12.1983), comp.: Juristischer Informationsdienst Online: http://dejure.org/dienste/vernetzung/rechtsprechung?Text=BVerfGE%2065,%201
UK House of Lords, Select Committee on the Constitution, (2nd Report of Session 2008-2009, *Surveillance: Citizens and the State*, HL Paper 18-I, Volume I: Report, pp. 26-27.

137 Michel Foucault, *Discipline and Punish: The Birth of the Prison*, New York: Vintage Books (1995).

138 For an elaboration of these alternative concepts see: Reinhard Kreissl and Regina Berglez, *SurpRISE project D3.3,* chapter "5 Alternative concepts".

139 Jason Ditton, and Stephen Farrall, *The Fear of Crime*, Dartmouth: Ashgate (2000).

140 Karl W. Deutsch et al., *Political Community and the North Atlantic Area*, International Organization in the Light of Historical Experience, Princeton: Princeton University Press (1957).

141 Comp. Emanuel Adler and Michael Barnett, *Security Communities*, Cambridge University Press (1998).

Waever puts the beneficial potential of the concept into perspective, stating that "'*security communities" proved to be a fertile organizing question in that it produced a re-thinking of European politics in the complex field where the historic novelty of non-war meets a transformation of security from state monopoly to multiple units. (…) Without war, security becomes much more complex, and the identities built on this kind of security pose challenges not only to security but analysis but generally to international relations theory, unprepared as it still largely is for structuring thinking about post-sovereign politics.*'[142]

Restorative Justice as a framework is aiming at (fundamental) changes in the legal systems of democratic societies. Conceptual ideas elaborating the idea of "Restorative Justice**"** have been developed since 1970s.[143] Nils Christie claimed in 1977 that criminal justice systems in modern industrialized democratic states mainly followed logics of control rather than aiming at solving societal conflicts in the benefit of the citizen.[144] Restorative justice roots in a basic premise of active participation *by those who are concerned* in solving conflicts in society. Discussion about conflict and crime shall take place in local citizens' summits or victim-orientated neighbourhood courts and the like. In this process it is also concepts of compensation and reparation that are higher valued than penalization and punishment. Empowerment as a key factor is seen as bearing beneficial potential for the victims as well as the offenders and for society after all.

It is however obvious that these concepts rely on great trust in the capability of self-organisation and the acceptance of high responsibility from within the community. Such community action raises important questions regarding e.g. the application of informal control and the representation of the 'entire' community in the process.

Communitarianism and community crime prevention: The following statement from Amitai Etzioni emphasises the Communitarian logic on matters of accountability and responsibility for safety and security neatly: *"Order and autonomy are community needs; […] In short, the sociological protection for a regime of individual rights (of liberty) is to ensure that the basic needs of the community members are served. This in turn requires that community members live up to their social responsibilities - they must pay taxes, serve in neighbourhood crime watches, and attend to their children and their elders. We see here that there exists at the core of civil democratic societies a proud mutuality between individual rights and social responsibilities."*[145] This leads directly to community policing. This term is used for a number of different techniques but can on a general level be seen as a "creative" form of cooperation between the "civil society" and local police forces to raise awareness to and find solutions for local issues such as public disorder.

Putting the idea of citizens as informants to the police for surveillance in a broader context produces a sobering result. (1) It is difficult to determine and/or define what makes a behaviour or person suspicious. (2) Engaging citizens in this kind of surveillance is a complex task and often invites free riders (who then blame their neighbours for personal reasons). (3) The police are suffering from information overload. (4) Targeted activities in high-profile security cases such as terrorism are problematic because they create a substantial number of false positives.

Social resilience and community resilience: Focussing on resilience, security problems appear to be of a twofold nature. They comprise prevention and mitigation. Prevention from a resilience perspective does not translate into controlling individuals but rather into looking at (or redesigning) the very structures and processes of a system to avoid the emergence of security threats. This entails a subtle but nonetheless important semantic shift in the meaning of security, making it a property of the societal

---

142 Ole Waever, 'Insecurity, security and asecurity', (1998) p. 105f; In: Adler and Barnett, *Security Communities*.

143 Nils Christie, 'Conflict as property', in, *A Restorative Justice Reader.Texts, sources, context*, edited by Gerry Johnstone, Cullompton: Willan Publishing (2003) pp. 57-69.

144 Ibid.

145 Amitai Etzioni, 'The Responsive Community: A Communitarian Perspective' Presidential Address, American Sociological Association, August 20, 1995. *American Sociological Review,* (February 1996), pp. 1-11. http://www.gwu.edu/~ccps/etzioni/A243.html

system instead of a consequence of externally monitoring the inner workings (transactions, movements, interactions) of this very system to detect signs of future issues.

Bristow envisages three key factors of resilient regions[146], marking the close relationship these factors have to (balanced) ecosystems: (1) resilience is in need of local supplements for the globalized just-in-time chains of food and basic goods supplies. Basic /primary services need to be provided from within a local community in case these chains are happening to be cut off. (2) Also, local communities/places do need to be engaged with the "outside" world, not on a level of mutual dependency but rather in terms of what Bristow names ethic network and information sharing.[147] (3) An important characterization of resilient places is their emphasis on small-scale activities embedded in the local structures whilst not over depending on mono-cultural key sectors. Also, e.g. invasive bureaucracies are to be minimized.

For instance Edwards is describing community resilience as an elastic concept, stating: 'Community resilience is an everyday activity. It manifests itself in meetings and conversations, dialogue and training, skills and information and – when disaster occurs – action.'[148] He is placing strong emphasis on engagement, education, empowerment and encouragement.[149]

The problem of reducing resilience to a purely moralistic concept has to be considered, when discussing these alternative approaches to security. Nevertheless resilience does have a central advantage over the standard surveillance and prevention strategies: It acknowledges the risk of attacks, failures and malfunctions and focuses on the robustness of the system and the mitigating reactions in the ace of threats and damages. This refocuses the strategic approach and can help to curtail the unlimited logic of surveillance.

A great number of *further alternative approaches* trying to enhance security can be envisaged. Attempts to maintain and increase (feelings of) security are e.g. being made through urban planning. *Signing out crime approaches* can be followed from two opposite directions: by believing in a vital public space and the 'eyes of the street' or by believing in segmentation, fragmentation and control of public space.[150]

Lessons to be learned from the field of safety engineering can be adopted in various technological areas. Privacy protection can also be augmented through relatively novel approaches in privacy impact assessment; and furthermore by using privacy enhancing technologies and by implementing privacy by design *(see chapters 4.1 - 4.3*).

Also, Bennett reminds us that '*An important part of the political struggle over information is whether or not an issue is defined in technical terms and therefore only subject to discussion by self-appointed experts, or whether it concerns a broader public constituency.*'[151] The wide field of science communication (and/or public understanding of science) can thus be regarded as a key factor for an inclusion of the general public into the debate and ideally for policy-making. Science communication is therefore playing a significant role not only for a better public understanding of technologies but also for creating or even pushing an informed public debate about the impact technologies have for matters of security, surveillance and privacy in society.

---

[146] G. Bristow, 'Resilient regions: re-'placing regional competitiveness', *Cambridge Journal of Regions, Economy and Society* 3, Nr. 1 (2010) pp. 153–167, http://cjres.oxfordjournals.org/content/3/1/153.short.

[147] Ibid.

[148] Charlie Edwards, *Resilient Nation*, Demos, 2009. p.79.

[149] Ibid.

[150] Comp. Reinhard Kreissl and Regina Berglez, *SurPRISE project D3.3* (2013), chapter "5.2.1. Urban planning",

[151] Colin J. Bennett, *The privacy advocates: resisting the spread of surveillance*. Cambridge, MA: MIT Press, (2008). p. 98.

Conclusion: On the one hand many problems of technology cannot be solved by adopting a Luddite attitude. Solving problems in a technologically mediated world requires more and better technology – which does not come down to more of the same. It also requires a better public understanding of what technology is, how it operates and what effects it can have. Hence a strategy focusing on public awareness of science and technology can be considered to have a positive impact on security by providing the basis for a rational public discourse.

On the other hand it has to be taken into account that societal-based alternative approaches are encountered by two fundamental problems: (1) Revitalizing a communitarian spirit is not an easy task at all and as stated (2) community-based approaches can have detrimental effects on late-modern life styles and universalistic values. Social, non-technical alternatives to perceived security threats always encounter a series of standard counter arguments. Alternative societal approaches cannot pretend to be based on a crisp and superficially convincing logic as technological solutions since they operate in a larger, cultural, societal frame, and approach the problem often in a more indirect way when looking at so-called root causes.

Under the Fordist welfare regime of social policy, which is being emasculated by neo-liberalism in most Western societies, social justice and equality were objectives to be pursued in their own right. Governing through the social was a strategy aiming at inclusion, equality of life chances, and raising standards of health, education and general welfare. This political frame has lost much of its momentum. In order to get political approval for measures formerly conceived as social policy, they have to be reframed as contributing to improved security. Many social programmes e.g. addressing ethnic minorities in European societies, and pursuing old-school welfare objectives, have been justified in a discourse of countering radicalization and mitigating the threat potential presumably emerging from an excluded generation of young Muslims. Often euphemistically declared as strategies to address the 'root causes' of so-called home-grown terrorism, these programmes in fact contributed to an improvement of the social situation of marginalized groups. Providing support for disadvantaged groups is hard to justify as an end in itself as under the old welfare regime. But policies geared towards such ends can be declared as a means to an end in a society obsessed with security. So from a strategic perspective there is a need for policies addressing social inequality, at least to some extent. They simply have to claim to contribute to a more secure society. Such an approach can help to counter a reductionist exclusionary and surveillance-oriented strategy to address the highly politicized security challenges in modern societies.

Maintaining control rather than addressing the root causes of fundamental societal problems such as (rising) inequality and austerity has become the basic overarching approach of (Western) neoliberal politics. As already stated in D2.2: '*Security policies […] have increasingly adopted a conceptual approach to security problems that is strongly solution-driven and tends to neglect the variety and complexity of social, economic, technical and political factors that may have caused the emergence of those security problems in the first place.*'[152]

[152] Vincenzo Pavone, Sara Degli Eposti and Elvira Santiago, *SurPRISE project D2.2* (2013), p. 7.

6. Conclusion: Towards balanced risk awareness[153]

Acknowledging the fact of an indeterminable and uncertain number of risks and the fact that surveillance technologies produce significant social, cultural and political costs, while their positive effects are hard to substantiate, a rational approach to security could be summarized under the heading of balanced risk awareness. Having reviewed legal, technological, and social aspects of SOST and SOSS it becomes clear which parameters of the societal equation are available to solve the puzzle of security and which of these parameters are at the disposal of rational change under the given conditions of modern societies: what is a society willing to change (or give up) to reduce imbalances and injustices at different levels?

There are a number of admittedly abstract ideas such a perspective can contribute to the debate on security challenges. While a standard approach would step up security and surveillance measures (e.g. more police conducting more stop and search, more CCTV, more access controls, etc.) to prevent criminal activities, a risk balance and resilience-based policy would focus on involving members of the community in local politics, improving general living conditions, creating job opportunities for disadvantaged groups, providing social services, etc. assuming that crime emerges out of the inner processes of the community instead of being an evil force imposed from outside. Hence any effort at prevention will also primarily look at these inner processes as root causes for security problems while at the same time acknowledging that these problems cannot be solved completely. As can be demonstrated many security solutions, from the local to the global level, produce massive effects of social exclusion and erode traditional mechanisms of social integration.

As the dominant discourse has it, there is a trade-off between security and privacy: security threats require surveillance and surveillance entails infringements of privacy. Taking the broader perspective into account a different type of trade-off emerges: the life-style of Western societies is based on an exploitation of those countries where, according to dominant Western security discourse, some of the most pressing security threats emerge. Affluence in the "West" is traded in for poverty, dissatisfaction and threats in the Global South. This amounts to a tripartite relation between convenience and security, and security and privacy.

The security/convenience link can also be demonstrated with regard to consumer-related data collections used for surveillance purposes. Providing easy access to goods and services for a majority of citizens in a highly mobile society requires an elaborate infrastructure of data processing. From this abstract perspective, a tripartite trade-off between security, convenience and privacy can be construed: consumerist convenience can create security problems that are to a large extent caused by social inequality, which again is the consequence of an international regime of exploitation. Privacy seems to be traded in for the promise of higher security. Security in turn is jeopardized through processes and activities that are the consequence of exploitation. It should also consider the trade-off between security and convenience. Living in a global risk society, to borrow a term from Ulrich Beck,[154] one should be careful not to fall prey to the illusion of an emerging post-imperialist New World Order, striving for eternal peace, achievable when the few uncooperative groups or individuals are successfully targeted

[153] By IRKS

[154] Ulrich Beck, *Risk society: towards a new modernity*, London: Sage (2007).

and eliminated. Taking this global perspective on security, several critical issues immediately come to the forefront. First, the dominant new security risks, providing the basis for an ever more intrusive regime of surveillance can be traced back to a political and economic world order breeding dissatisfaction, protest and last not least violent resistance on a continuous basis. Secondly, when looking at the global market for surveillance and security technologies it becomes obvious how these technologies are marketed in countries lacking any form of democratic legitimacy and how they are used in these countries to fight emerging local movements. What is sold to the general public as a necessary (technological, political and legal) move to protect Western democracies of the Atlantic rim against enemies from the Global South is used in the countries of this regions to suppress political movements fighting regimes far beyond any modern democratic standards.

Many of the suggested alternative security enhancing solutions address social inequalities and social injustice. They also often require a reactivation of what could be called a "communitarian spirit". Substantial global inequalities are the basis of a culturally entrenched lifestyle of consumerism and for a communitarian spirit to flourish a number of the anomic individualistic freedoms of this middle-class lifestyle would have to be sacrificed for stronger civic engagement, enforcing communal values. Neither of these requirements will realistically be met in present day societies.

First of all, the dimensions of perceived threats should be put into a realistic perspective. As could be demonstrated, the politics of fear tend to exaggerate security threats for a number of obvious reasons. Second, the proposed administrative and technological solutions require close and critical scrutiny, since in most cases they do not live up to the promises brought forward by the security hawks. But downscaling perceived security threats and debunking surveillance-based security solutions as largely ineffective will not produce a world without risks. What is required is an informed public debate about what could be called 'acceptable' risks. Such a debate has to go beyond the standard reasoning of calculating statistical probabilities and multiplying them with a hypothetical damage. Rather it should start from the premise that in many cases the cure is worse than the disease in the field of security. It should also consider the "trade-off" between security and convenience and the role growing societal inequality is playing. Finally it should take for granted the premise that liberty and freedom are risky in many respects and that both are rooted in the fundamental right to privacy, however this concept is spelled out.

7. Executive Summary and Policy Recommendations

In this section the key findings from the different perspectives of law, technology and social science are summarized and a number of policy implications are presented for discussion. [155]

- The rights to privacy and data protection express crucial societal values. Privacy refers to the sphere of a person's life in which he or she can freely express his or her identity. As such, it puts normative limits to technological advances (notably in the field of ICTs) and related practices that enhance human possibilities but interfere with autonomy and freedom (of home, body and correspondence).

- Such values informed the legislative development of the right to privacy, from article 12 of the Universal Declaration of Human Rights of 1948, to articles 7 and 8 of the European Charter of Fundamental Rights, including a full acknowledgment of the right to personal data. The formulations of the right to privacy attest to its universal relevance. "Privacy" appears as an umbrella term encompassing several different dimensions, a versatile understanding upheld and fostered by Courts. Data protection appears as a more "procedural right" safeguarded by the mechanisms put in place by the legal instruments. Both rights, though, are defined as relative, in the meaning that they can be interfered with by means of permissible limitations, which must respect a number of criteria that have been interpreted and clarified through case law.

- The established meaning of the fundamental rights to privacy and data protection allowing for permissible limitations implies that, in principle, there is no opposition between their protection and the achievement of individual or public security, understood as a legitimate aim. In practice, however, after the terrorist attacks of 9/11, law enforcement activities driven by the collection of personal information have expanded, leading to the increased use of SOSTs and SOSSs.[156]

- This deliverable challenges the security vs. privacy approach, and proposes an analytical alternative: the core/periphery approach (based on a reinterpretation of Robert Alexy's theory of rights). The theory can be applied to explain how any fundamental right would have an inviolable core (often more than one such core) or "essence" sealed in a rule, and a periphery surrounding that core and subject to permissible limitations. Three different criteria have been preliminarily suggested as candidates to determine the scope of the core of the right to privacy: sensitive data as privileged content, information produced in the course of confidential personal relationships, and methods of intrusion. The inviolability of the essential core of any human right – in this case the right to privacy – is one of the steps in an analytically rigorous test for the permissibility of restrictions.

- The test for permissible limitations incorporating the core/periphery theory could provide a tool for evaluating the acceptability of SOSTs and SOSSs, whenever an interference with the right to privacy is the outcome.
- Surveillance-oriented security technologies often do not stand the test of functionality outside controlled laboratory settings. There is often an imbalance between intrusiveness and the security gain to be achieved by SOSTs.

---

[155] By IRKS, EUI, ULD

[156] The ensuing policies in the field of AFSJ, such as the Council Framework Decision 2008/977/JHA and the Data Retention Directive, framed the relationship between privacy (together with data protection) and security predominantly in terms of the need to "strike a balance", i.e. to weigh against each other security interests and privacy (and data protection) rights. Yet, such rhetoric de facto often results in introducing excessive limitations to these rights, questioning their significance in our society.

- Technological solutions to enhance privacy (mainly privacy by design) are difficult to implement for most surveillance technologies.

- SOSTs do entail a social definition of normal and deviant (or unusual, suspicious) behaviour. Since the underlying algorithms come with the inherent assumption of zero-tolerance, such definitions can create a substantial number of false positives when the technology is implemented.

- All SOSTs are prone to function creep and also abuse and may easily be used outside the narrowly defined realm justifying their implementation in the first place. It is difficult to control such proliferation once a given technology is put in place.

- Alternative concepts to enhance security typically target root causes of societal problems. Technological solutions focus on a narrow understanding of security and ignore the wider societal context.

- Security is a multi-dimensional concept and has to be understood in a comprehensive sense. Reducing security discourse to a narrow understanding of identifying potential perpetrators by means of pervasive surveillance ignores aspects of perceived security.

- Technology use in contemporary societies creates security problems and problems of privacy and data-protection at the same time.

- Falling back on alternative societal solutions to reduce security risks in modern societies is difficult since these alternatives often involve elements rooted in traditional social forms of community life which cannot be revitalized at will. Furthermore communitarian approaches to security tend to entail a limitation on individualistic life styles typical for modern societies.

Policy suggestions from a legal perspective

- Fast technological and technical innovations constantly put under test our understanding of the fundamental rights to privacy and data protection, sometimes to the effect of making the mechanisms of protection that we devised obsolete. A deterministic approach whereby the full enjoyment of the rights is inevitably sacrificed vis-à-vis technological innovation and its many applications is not compatible with a democratic society. We suggest:

- Promoting a political reflection as to how to harmonize the enjoyment of human rights with the technological innovation and its application in the field of Justice and Home Affairs.

- Including in these reflections a commitment to the idea that the essence of any fundamental right is inviolable (the core/periphery approach) and that in issues that do not fall within the essence (core), a proper proportionality assessment is required, including through demonstrating that the benefits actually delivered are greater than the intrusion into privacy and data protection.

- This requires introducing technology assessment at the earliest stage of policies in the AFSJ. As it is understood that law enforcement agencies will avail themselves of technologies, the discussions of which technologies are permissible (and acceptable) should be fully included in the decision-making processes.

- Such a process requires the involvement of data protection agencies, technology experts and civil society organizations.

- Excluding citizens from the decision-making process as to what technologies are permissible could affect the right to good governance. Citizens at the national level need to be fully involved in the process. National governments should address the democratic deficit in this field.

Policy suggestions from a technological perspective

- Policy-makers have to make important choices on the implementation of SOSTs. In order to do this in a rational way, compatible with principles of privacy and data-protection, they should be able to answer the following questions, using the proficiency of independent experts from the relevant fields of privacy impact and technology assessment. These criteria or questions also connect to the test of permissible limitations.

- How does a given technology work exactly?

- Which individuals or groups are affected primarily and in what way?

- What are the benefits for enhancing security this technology provides?

- Can the security gains be measured independently?

- Which risks are known or anticipated when implementing a given technology?

- Can Privacy by Design approaches be applied and are non-technological alternatives available to address the problem at hand?

- Do the criteria for technology impact assessment applied strike a balance between security and privacy?

- Does the technology stand the test of criteria from a legal point of view:

- Necessity, suitability, and proportionality? How are these criteria operationalized into technological requirements of design?

Policy suggestions from a social perspective

- Narrowly defined security problems should be deconstructed into more general problems of social justice and inequality. This can open the horizon for alternative solutions addressing root causes of security threats.

- Strengthening available societal resources can have preventive effects in the long run and increase social resilience, i.e. making societies more robust in the face of different types of threats.

- Security should not be perceived as the exclusive domain of law enforcement and intelligence experts. Security has to be taken back from the experts to the general public. Involving citizens and civil society organisations in an informed public debate about security can create a better and more comprehensive understanding of the different aspects of (perceived) security.

- Policy discourse on security issues should not fall prey to securitization. The broader the perspective adopted when analysing policy options the better the chances to develop a sustainable solution for security problems.

- Security should always be understood as a public good, a discursive object and an individual psychological state at the same time, taking into account the interrelation between these different kinds of security.

- Policy makers should refrain from strategies claiming the elimination of security risks but rather strive for balanced risk awareness as desirable public attitude.

8. Bibliography

ADDPRIV project, "Deliverable 2.1: Review of existing smart video surveillance systems capable of being integrated with ADDPRIV project", (Submission date July 31st 2011). http://www.addpriv.eu/uploads/public%20_deliverables/149--ADDPRIV_20113107_WP2_GDANSK_Scoreboard_R11.pdf

Adler, Emanuel and Michael Barnett, *Security Communities*, Cambridge: University Press (1998).

Alexy, Robert 'Constitutional Rights and Legal Systems', in Joakim Nergelius (ed.), *Constitutionalism - New Challenges: European Law from a Nordic Perspective* (2008).

Charles Arthur 'Internet remains unregulated after UN treaty blocked', *The Guardian,* (2012) http://www.guardian.co.uk/technology/2012/dec/14/telecoms-treaty-internet-unregulated

Article 29 Data Protection Working Party (2010), 'Report 01/2010 on the Second Joint Enforcement Action: Compliance at National Level of Telecom Providers and ISPs with the Obligations Required from National Traffic Data Retention Legislation on the Legal Basis of Articles 6 and 9 of the e-Privacy Directive 2002/58/EC and the Data Retention Directive 2006/24/EC Amending the e-Privacy Directive', (Brussels).

Ashworth, Andrew 'Security, Terrorism and the Value of Human Rights', in Benjamin Goold and Lazarus Liora (eds.), *Security and Human Rights*, Portland: Hart, (2007) pp. 203-226.

Badke-Schaub, Petra et al. (eds.) *Human Factors*, Heidelberg: Springer (2008).

Bankston, Kevin, 'Surveillance Shocker: Sprint Received 8 MILLION Law Enforcement Requests for GPS Location Data in the Past Year', *Electronic Frontier Foundation,* (Article of December 1st 2009). https://www.eff.org/deeplinks/2009/12/surveillance-shocker-sprint-received-8-million-law

Barak, Gregg, *Media, process, and the social construction of crime: studies in newsmaking criminology,* New York: Garland (1995).

Beck, Ulrich, *Risk society: towards a new modernity*, London: Sage (2007).

Bedner, Mark, 'Rechtmäßigkeit der Deep Packet Inspection', Analysis created for the 'Projektgruppe verfassungsverträgliche Technikgestaltung (provet)' at the Universität Kassel (2009). www.kobra.bibliothek.uni-kassel.de/bitstream/urn:nbn:de:hebis:34-2009113031192/5/BednerDeepPacketInspection.pdf

Bennett, Colin J., *The privacy advocates: resisting the spread of surveillance*. Cambridge, MA: MIT Press, 2008.

Blair, John, *The International Covenant on Civil and Political Rights and its (First) Optional Protocol. A short Commentary based on Views, General Comments and Concluding Observations by the Human Rights Committee* , Frankfurt: Peter Lang (2005).

Boers, Klaus, *Kriminalitätsfurcht*, Pfaffenweiler: Centaurus (1991).

Booth, Robert, 'Government plans increased email and social network surveillance', *The Guardian*, (April 1st 2012).
http://www.guardian.co.uk/world/2012/apr/01/government-email-social-network-surveillance

Bristow, G. 'Resilient regions: re-placing regional competitiveness', *Cambridge Journal of Regions, Economy and Society* 3, Nr. 1 (2010) pp. 153–167.
http://cjres.oxfordjournals.org/content/3/1/153.short.

Burke, Jason, *Al-Qaeda: The True Story of Radical Islam*, London: I.B. Tauris (2004).

Buttarelli, Giovanni (Assistant EDPS) (2011), 'What future for the Data Retention Directive. General remarks', in Discussion on the Commission Evaluation reportEU Council Working Party on Data Protection and Information Exchange (DAPIX – Data Protection) (ed.), (Brussels).

Buzan, Barry, Ole Waever and Jaap De Wilde, *Security: A New Framework for Analysis*, Lynne Rienner Publishers (1998).

BVerfGE 65, 1 (15.12.1983), *Juristischer Informationsdienst Online:*
http://dejure.org/dienste/vernetzung/rechtsprechung?Text=BVerfGE%2065,%201

'Charter of Fundamental Rights of the European Union', (2007) Official Journal C 303/1, 1–22.

Christie, Nils, 'Conflict as property', in, *A Restorative Justice Reader.Texts, sources, context*, edited by Gerry Johnstone, Cullompton: Willan Publishing (2003) pp. 57-69.

--- 1977. 'Conflicts as Property', *British Journal of Criminology* , Vol. 17, 1: 1-15.

Clarke, Roger, 'Person-Location and Person-Tracking: Technologies, Risks and Policy Impli-cations', *Technology & People* ,Vol. 14, No. 2 (2001) pp. 206-231.

'Consolidated versions of the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU)', Official Journal C 83/01.

Council (2008), 'Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters', (OJ L 350), 60 –71.

--- (2010), 'Draft Internal Security Strategy for the European Union: Towards a European Security Model', (5842/2/10; Brussels).

Council of Europe (2001), 'Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and trans-border data flows', (CETS No. 181; Strasbourg).

Council of Europe (1981), 'Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data', (CETS No. 108; Strasbourg).

Council of Europe (1950), 'Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols No 11 and 14', (CETS n° 005; Rome).

Court of Justice of the European Union (2012), 'Case C 360/10, Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV', Judgment of the Court (Third Chamber).

--- (1989), 'Case 5/88, Wachauf V Bundesamt Für Ernährung Und Forstwirtschaft', (Third Chamber).

Craig, Paul and Gráinne de Búrca, *European Union Law: Text, Cases and Materials* Oxford, 1320 (2011).

Deibert, Ronald J. 'Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace', *Millenium - Journal of International Studies,* 32 (2), (2003) pp. 501-530.

Deutsch, Karl W. et al., *Political Community and the North Atlantic Area*, International Organization in the Light of Historical Experience, Princeton: Princeton University Press (1957).

Ditton, Jason, and Stephen Farrall, *The Fear of Crime*, Dartmouth: Ashgate (2000).

Drafting Committee on an International Bill of Human Rights (1st session) (1947), 'International Bill of Rights Documented Outline '.

Dumortier, Frank, et al. 'La Protection des Données dans l'Espace Européen de Liberté, de Sécurité et de Justice', *Journal de Droit Européen,* 166, 23 (2010).

Edwards, Charlie, *Resilient Nation*, Demos, (2009).

ENISA-Website: http://www.enisa.europa.eu/media/press-releases/new-report-on-top-trends-in-the-first-cyber-threat-landscape-by-eu2019s-cyber-agency-enisa

ENISA: Website: *Threat Landscape Report,* (for download on the ENISA-website), (2013).

ENISA Threat Landscape Published.pdf

Ericson, Richard Victor and Kevin D. Haggerty, *Policing the Risk Society*, Oxford: University Press (1997).

Etzioni, Amitai, 'The Responsive Community: A Communitarian Perspective', Presidential Address, American Sociological Association, (August 20, 1995) *American Sociological Review,* (February 1996), pp. 1-11. http://www.gwu.edu/~ccps/etzioni/A243.html

European Commission (2010), 'Communication. The EU Internal Security Strategy in Action; Five steps towards a more secure Europe, COM (2010) 673 final', (Brussels).

--- (2011), 'COM (2011) 225 final, Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC)', (Brussels).

--- (2012), 'COM(2012) 254 final, Amended proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the establishment of 'EURODAC' for the comparison of fin g erprints for the effective application of Regulation (EU) No [.../...] (establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person) and to request comparisons with EURODAC data by Member States' law enforcement authorities and Europol for law enforcement purposes and amending Regulation (EU) No 1077/2011 establishing a European Agency for the operational management of large-scale IT systems in the area of freedom, security and justice (Recast version)', (Brussels).

European Court of Human Rights (2009), *Opuz v. Turkey* (Application No. 33401/02)), Judgment of 9 June 2009.

European Data Protection Supervisor (EDPS), (2011) 'Opinion of the European Data Protection Supervisor on net neutrality, traffic management and the protection of privacy and personal data' (OJ C 34/01).

--- (2010), 'Opinion of the European Data Protection Supervisor on the proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse, sexual exploitation of children and child pornography, repealing Framework Decision 2004/68/JHA'.

European Parliament, Council, and Commission (2007), 'Explanations Relating to the Charter of Fundamental Rights'.

European Parliament and Council (2006), 'Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (Data Retention Directive)', (Brussels), 54–63.

--- (2008), 'Regulation 2008/767/EC of 9 July 2008 concerning the Visa Information System (VIS) and the Exchange of Data between Member States on Short-stay Visas', (Brussels).

European Parliament and European Council 'Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA', (OJ L335/1).

F-Secure Blog, '440,783 '"Silent SMS" Used to Track German Suspects in 2010', (December 29th 2011). https://www.f-secure.com/weblog/archives/00002294.html

Florencio, Dinei and Cormac Herley, 'The cybercrime wave that wasn't', *The New York Times Sunday Review* (2012). http://www.nytimes.com/2012/04/15/opinion/sunday/the-cybercrime-wave-that-wasnt.html?_r=0

Foucault, Michel, *Discipline and Punish: The Birth of the Prison*, New York: Vintage Books (1995).

Foucault, Michel and Paul Rabinow, *The essential works of Michel Foucault, 1954-1984. Subjectivity and truth, Vol. 1, Ethics,* London: Penguin (2000).

Freudiger, Julien, 'When Whereabouts is No Longer Thereabouts: Location Privacy in Wireless Networks', *École Polytechnique Féderale de Lausanne* (2011).

Fuchs, Christian, 'Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society", *The Privacy & Security Research Paper Series*, Issue #1 (July 2012). http://www.projectpact.eu/documents-1/%231_Privacy_and_Security_Research_Paper_Series.pdf

Gandy, Oscar. H., 'Consumer Protection in Cyberspace', *tripleC-Cognition, Communication, Co-operation* 9, Nr. 2 (2011) pp. 175–189. http://www.triplec.at/index.php/tripleC/article/view/267.

General Assembly (3rd session) (1948), 'Universal Declaration of Human Rights. Resolution 217', in United Nations (ed.).

Goldberg, Jeffrey, 'The things he carried', *The Atlantic* (2008). http://www.theatlantic.com/magazine/archive/2008/11/the-things-he-carried/307057/

Goold, Benjamin J., University of British Columbia, in 'CCTV and Human Rights', published in the 'Citizens, Cities and Video-Surveillance' paper of the *European Forum for Urban Security publication* (of June 2010), titled 'Citizens, Cities and Video Surveillance – Towards a democratic and responsible use of CCTV', www.cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Publication/CCTV_publication_EN.pdf

Gray, Jim, Microsoft Research San Francisco, in the foreword of *Location-Based Services*, published by Jochen Schiller & Agnés Voisard (2004).

Hayes, Ben, 'NeoConOpticon. The EU-Security Industrial Complex', Transnational Institute in association with Statewatch (2009). Statewatch ISSN 1756-851X.

Hill, Kashmir, 'Using Twitter to identify psychopaths', *Forbes Magazine* (2012). http://www.forbes.com/sites/kashmirhill/2012/07/20/using-twitter-to-help-expose-psychopaths/

Hilty, Lorenz, Britta Oertel, Michaela Wölk and Kurt Pärli, 'Lokalisiert und identifiziert – wie Ortungstechnologien unser Leben verändern', *Zentrum für Technologiefolgen-Abschätzung (TA-Swiss)*, (2012). http://www.ta-swiss.ch/ortungstechnologien/

Human Rights Committee (1990), *William Eduardo Delgado Paez v. Colombia* (Communication No. 195/1985), Final Views by the Human Rights Committee 12 July 1990.

Hustinx, Peter, European Data Protection Supervisor, '*Video surveillance guidelines'*, (March 17th 2010). http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf

Kranzberg, Melvin 'Technology and History: "Kranzberg's Laws"', *Technology and Culture* 27, Nr. 3 (July 1986).

Kreissl, Reinhard and Regina Berglez, *SurPRISE project D3.3* (2013).

Lewis, Dan A. and Greta W. Salem, *Fear of Crime: Incivility and the Production of a Social Problem*, New Brunswick: Transaction Publishers (1986).

Lichtblau, Eric, 'Wireless Firms Are Flooded by Requests to Aid Surveillance', *The New York Times*, (July 8th 2012).
http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?_r=2&ref=surveillanceofcitizensbygovernment

Loader, Ian and Neil Walker, *Civilizing Security*, Cambridge: Cambridge University Press (2007).

Lyon, David, *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. Taylor & Francis Group (2003).

Lyon, David, *Surveillance Studies: An Overview*. Polity, (2007).

Marx, G.T. "Thoughts on a Neglected Category of Social Movement Participant: The Agent Provocateur and the Informant." *American Journal of Sociology*. vol. 80, pp. 402-442. (1974).

Mattelart, Armand, *The Globalization of Surveillance* Cambridge, Malden: Polity (2010).

Mautz, Rainer, Washington Ochieng, David Walsh, Gary Brodin, Andy Kemp, John Cooper and Thanh Son Le 'Low Cost Intelligent Pervasive Location Tracking (iPLOT) in All Environments for the Management of Crime', *Journal of Navigation*, 59, pp. 263-279.

Meléndez-Juarbe, Hiram A., University of Puerto Rico Law School, 'Intermediaries and Freedom of Expression', essay translated by University students Edgardo Canales and Marini Rodriguez, (no date). http://www.palermo.edu/cele/pdf/english/Internet-Free-of-Censorship/04-Intermediaries_Freedom_of_Expression_Hiram_Melendez_Juarbe.pdf

Minch, Robert P., 'Privacy Issues in Location-Aware Mobile Devices', *Proceedings of the 37th Hawaii International Conference on Systems Sciences* (2004) pp. 10-19.

Monahan, Torin, David J. Phillips and David Murakami Wood, 'Editorial. Surveillance and Empowerment', *Surveillance & Society,* Vol. 8, No. 2), (2010) pp. 106-112.

Morsink, Johannes, *The Universal Declaration of Human Rights: Origins, Drafting and Intent*, Philadelphia: University of Pennsylvania Press (1999).

Newman, Abraham L., *Protectors of Privacy. Regulating Personal Data in the Global Economy*, Ithaca: Cornell University Press (2008).

Norris, Clive, Mike McCahill and David Wood, "The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space', titled 'The Politics of CCTV in Europe and Beyond', *Surveillance & Society*, Vol. 2, no. 2/3 (2004).

Nowak, Manfred 'Chapter on Article 17', in Manfred Nowak and Felix Ermacora (ed.), *UN Covenant on Civil and Political Rights, CCPR Commentary* Kehl: N.P. Engel, (2005 (2nd edition)), pp. 377-405.

O'Malley, Pat, *Crime and Risk*, London et al, Sage (2010).

Organization for the Economic Cooperation and Development (1980), 'Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data', in Council of the Organization for the Economic Cooperation and Development (ed.).

Pavone, Vincenzo, Sara Degli Eposti and Elvira Santiago, *SurPRISE project D2.2* (2013).

Perusco, Laura and Katina Michael, 'Location-Based Services and the Privacy-Security Dichotomy', *Proceedings of the 3rd International Conference on Mobile Computing and Ubiquitous Networking*, London (2006) pp. 91-98.

Porcedda, Maria Grazia, Mathias Vermeulen and Martin Scheinin, 'Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy. *Deliverable 3.2,* SurPRISE Project. Forthcoming', Florence: European University Institute (2013).

Poullet, Yves and Rouvroy, Antoinette, 'The right to informational self-determination and the value of self-development. Reassessing the importance of privacy for democracy', in Serge Gutwirth, et al. (eds.), *Reinventing Data Protection?* (2009).

Rehof, Lars Adam, 'Universal Declaration of Human Rights – Common Standard of Achievement', in Asbjorn Eide and Gudmundur Alfredsson (ed.), Norway: Scandinavian University Press, (1995) pp. 251-64.

Richtel, Matt, 'The mystery of the flying laptop', *The New York Times* (2012). http://travel.nytimes.com/2012/04/08/travel/the-mystery-of-the-flying-laptop.html?pagewanted=1&src=dayp

Robertson, Adi, 'Military-backed surveillance prototype can read people's actions on video', *theverge.com,* (October 28th 2012). www.theverge.com/2012/10/28/3567048/carnegie-mellon-video-surveillance-action-recognition

Rodotà, Stefano, *Elaboratori Elettronici e Controllo Sociale* , Bologna: Mulino (1973).

--- 'Data Protection as a Fundamental Right', in Yves Poullet Serge Gutwirth, Paul De Hert, Sjaak Nouwt and Cécile de Terwangne (ed.), *In Reinventing Data Protection?* Springer (2009).

--- *Il diritto ad avere diritti*, Bari: Editori Laterza (2012).

Sartor, Giovanni, *L'informatica Giuridica e le Tecnologie dell'Informazione. Corso di Informatica Giuridica,* Torino: Giappichelli Editore (2010).

Scheinin, Martin, 'Terrorism and the Pull of 'Balancing' in the Name of Security', in Martin Scheinin (ed.), *Law and Security, Facing the Dilemmas,* 11; Florence: European University Instite (2009a).

--- 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism', Geneva: General Assembly (2009b).

Schlehahn, Eva, *SurPRISE project D3.1* (2013).

Schneier, Bruce, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, New York: Springer (2003).

Schneier, Bruce, *Psychology of security,* Own Website, *(*January 18th 2008). http://www.schneier.com/essay-155.html

Schneier, Bruce, 'Our Security Models Will Never Work — No Matter What We Do', Essay for *Wired.com* (March 14th 2013). http://www.wired.com/opinion/2013/03/security-when-the-bad-guys-have-technology-too-how-do-we-survive/

Schoen, Seth, 'Legal Struggles Over Interception Rules in the United States', *Electronic Frontier Foundation* (no date).
https://www.eff.org/pages/legal-struggles-over-interception-rules-united-states

Sennett, Richard, *The fall of public man,* New York, London: W.W. Norton (1996) [1977].

Solove, Daniel J., *Understanding Privacy*, Harvard: University Press (2008).

Squires, Peter, 'Evaluating CCTV: Lessons from a Surveillance Culture', published on pp. 39 ff. in the 'Citizens, Cities and Video-Surveillance' paper of the *European Forum for Urban Security* publication (of June 2010), titled 'Citizens, Cities and Video Surveillance – Towards a democratic and responsible use of CCTV'.

SURVEILLE Project Consortium (2011), 'Document of Works of the SURVEILLE Project. Surveillance: ethical issues, legal limitations and efficiency', (Seventh Framework Programme, European Union).

Taleb, Nassim, *The black swan : the impact of the highly improbable*, London, Penguin (2008).

Taylor, Nick, 'State Surveillance and the Right to Privacy', *Surveillance & Society*, Vol. 1, no. 1 (2002). http://www.surveillance-and-society.org/articles1/statesurv.pdf

UK House of Lords, Select Committee on the Constitution, (2nd Report of Session 2008-2009), *Surveillance: Citizens and the State*, HL Paper 18-I, Volume I: Report, pp. 26-27.

United Nations (1966), 'International Covenant on Civil and Political Rights', (New York).

United Nations High Commissioner for Human Rights (OHCHR) (2012), 'Human Rights Indicators. A guide to Measurement and Implementation', (New York and Geneva: United Nations Human Rights Office of the High Commissioner).

van Brakel, Rosamunde and Paul De Hert, 'Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies', *Journal of Police Studies*, (2011), Issue 20, Vol. 20, No. 3, pp. 163-192.

Vann, Irvin B. and G. David Garson, 'Crime Mapping and Its Extension to Social Science Analysis, *Social Science Computer Review*', Vol. 19. No.4 (2001) pp. 471-479.

Waever, Ole 'Insecurity, security and asecurity', In: Adler, Emanuel and Michael Barnett, *Security Communities*, Cambridge: Cambridge University Press (1998).

Walters, Reece, *Deviant knowledge : criminology, politics, and policy,* Cullompton, Portland, OR, Willan (2003).

Wacquant, Loic 'Suitable enemies', *Punishment and Society*, Vol 1(2), (1999) p.215–222.

Warren, Samuel D. and Brandeis, Louis D., 'The right to privacy', *Harvard Law Review,* 4 (6) (1890).

Westin, Alan, *Privacy and Freedom*, Atheneum Press (1967).

Younger (Hon.), Kenneth (Chairman) (1972), 'Report of the Committee on Privacy', in Home Office (ed.), London: H. M. Stationery Office.