"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 3.3 Report on security enhancing options that are not based on surveillance technologies

Lead Beneficiary: IRKS

Authors: Regina Berglez (IRKS), Reinhard Kreissl (IRKS)

Due Date: March 2013

Submission Date: March 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

BPR	Behavioral Pattern Recognition
CCTV	Closed-circuit Television
DHS	U.S. Department for Homeland Security
DPI	Deep Packet Inspection
ECHR	European Court of Human Rights
GPS	Global Positioning System
HCI	Human-Computer Interaction
ICT	Information and Communication Technology
PAwS	Public Awareness of Science
PbD	Privacy by Design
PET	Privacy-enhancing Technology
PIA	Privacy Impact Assessment
PUS	Public Understanding of Science
RFID	Radio-frequency Identification
RJ	Restorative Justice
SbD	Security by Design
SIA	Surveillance Impact Assessment
SOSS	Surveillance-oriented Security Solution
SOST	Surveillance-oriented Security Technology
WWI	First World War
WWII	Second World War

Abstract

Investments in surveillance-based security technology are justified with the need to counter existing or emerging security threats. From a social science perspective this raises four questions. (1) Is the presented threat substantiated? (2) Do the proposed solutions improve security? (3) Which negative side effects on (the cohesion of) society are to be observed and have to be considered? (4) Can alternative options for understanding and handling security problems be envisaged? This report discusses available evidence from theory and research in sociology, criminology and security studies to answer these questions. Non-technical solutions to security problems can be identified the more so when security is understood in a comprehensive way. By investigating these alternative solutions from a broader social theory perspective, their limitations and costs can be analysed. Finally, by weighing pros and cons of technical and non-technical strategies, the complex relations between privacy and security can be assessed from a different angle.

Executive Summary

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.

Securing security

The most general definition of security as a "dynamic non-event"[1] demonstrates the problem of pinning down the concept with a precise definition. 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. Perceived security refers to an individual's subjective perception of feeling secure or insecure. A number of studies in criminology[2] have demonstrated the so-called "security paradox": individuals may feel insecure despite the fact of low victimisation risks and vice versa.

Security as a discursive object has been elaborated in security studies.[3] 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.

Precisely identifying causes and designing adequate counter measures is a difficult and bold venture: the absence of evidence is not the evidence of absence. The logic of security policies requires these measures to be applied comprehensively to each and every individual in order to sort out the potential predators. Taking highly dramatized security threats as a justification the different practices 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 of such an event.

Additionally it is also very difficult to assess the seriousness or magnitude of security threats. 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.

The states' 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. The security discourse appears to be highly contested and used in strategic contexts. Loader and Walker state that security has become *the* political vernacular of our times.[4] Since the practice of government is becoming increasingly one of risk management[5] and risk management has become – especially under neo-conservative political ideologies – a growing industry[6]

---

1 Petra Badke-Schaub et al. (eds.) *Human Factors*, Springer Heidelberg (2008), p. 21.
2 Klaus Boers, *Kriminalitätsfurcht*, Pfaffenweiler, Centaurus (1991).
3 Barry Buzan, Ole Waever, and Jaap De Wilde, *Security: A New Framework for Analysis*, Lynne Rienner Publishers (1998).
4 Ian Loader and Neil Walker, *Civilizing Security*, Cambridge: Cambridge University Press, (2007), p. 9.
5 Reece Walters, *Deviant knowledge : criminology, politics, and policy*, Cullompton; Portland, OR: Willan (2003) p. 139ff.
6 Pat O'Malley, *Crime and Risk*, London et al. SAGE (2010).

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.

The threat debate

Looking at the security threats with the highest public and political priority we find a similar situation as with the surveillance practices: it is very difficult to draw a precise line to define them. Terrorism 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 September 11th 2001 attacks in the USA an empowered Islamist network provided the new "suitable enemy" 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.[7]

Additionally large parts of the popular media (“crime sells”) actively propagate the idea that significant new threats exist. Under these circumstances 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.[8] Mattelart observed that *“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.”* [9]

On technology

Technology is neither good nor bad nor is it neutral.[10] Technological systems like mobile phones, credit cards, GPS, etc. are not explicitly designed as surveillance measures but can be used for surveillance purposes. For instance smart meter technologies bear on the one hand a great potential e.g. for cost and energy saving and thus for the environmental good but on the other they can also be used for surveillance purposes or social sorting.

However, it is often technologies, which are regarded as trivial to both consumers and businesses that can cause serious issues through relatively minor discrepancies in their functionality, for instance misrepresentation of places on electronic maps.[11] Technological – or respectively an inextricably mixture between technological and human – failures and malfunctions are creating an alarming number and variety of serious incidents. For instance DNA-testing is one of the areas where techno centrism and technology fix are not meeting with practice resp. reality. E. g. in the US ten thousands of cases based on DNA-testing/hair matching had to be questioned since they may have relied on exaggerated testimony

---

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

8 Florencio and Herley (2012), ‘The cybercrime wave that wasn’t’ http://www.nytimes.com/2012/04/15/opinion/sunday/the-cybercrime-wave-that-wasnt.html?_r=0

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

10 Melvin Kranzberg, ‘Technology and History: “Kranzberg’s Laws”’, *Technology and Culture* 27, Nr. 3 (July 1986): pp. 544–560.

11 Arthur (2012), ‘Apple redraws maps after Australian drivers led astray in the bush’ http://www.guardian.co.uk/technology/2012/dec/10/apple-maps-life-threatening-australian-police

or false forensic evidence.[12] Greater parts of surveillance technologies in use seem far from being 100% accurate and reliable, and, especially when combined with human error, are simply dangerous.

On privacy

The concept of a (off-line) private sphere, defined in spatial terms of the private home (reaching back to the Greek notion of Oikos) is of no avail in the age of the Homo Electronicus and hence a redefinition of privacy is becoming inevitable. The boundaries between public and private domains – and alongside with it the 'old' concept of privacy – seem blurred already. It cannot be neglected that, concerning personal privacy, the rise of social networks such as Facebook is steadily changing the perceptions of privacy for greater parts of the population.

However, three main arguments can be envisaged for our perspective concerning privacy: We stress that: (1) It is the potential future consequences of present behaviour where "privacy problems often lie in.[13] (2) Privacy is less about the content but rather about the functional relevance of multiple identities. (3) Citizens need to be better informed about (novel) technologies, and the impact these technologies have on rights such as the right to privacy. These three points do indicate once more the need for an informed public debate.

Impact on human rights

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 threat. A steady shift from 'post-crime' to 'pre-crime' situation management can be observed.[14] 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 writings.[15] 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.[16]

Individuals get selectively confronted with differential options based on their personal profile and classification. A growing number of studies highlight, that automated sorting by categories of personal data can re-produce marginalizing effects and create negative discrimination.[17] 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

---

12 Spencer (2012), 'FBI lab woes cast a growing shadow' http://www.independent.co.uk/news/world/americas/fbi-labs-woes-cast-a-growing-shadow-8430348.html
Porter (2009), 'The rising odds of DNA false matches' http://www.guardian.co.uk/commentisfree/henryporter/2009/may/25/dna-database-false-positive
Spencer (2012) 'Review of FBI forensics does not extend to federally trained state, local examiners' http://articles.washingtonpost.com/2012-12-22/local/36016999_1_crime-lab-arnold-melnikoff-fbi

13 Mark S. Ackerman and Scott D. Mainwaring, 'Privacy issues and human-computer-interaction' (2005) pp. 381–400. p. .383. In: Cranor, Lorrie, and Simson Garfinkel (Ed.) *Security and Usability: Designing Secure Systems That People Can Use*, O'Reilly Media, Inc. (2007).

14 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.

15 Hill (2012), „Using Twitter to identify psychopaths" http://www.forbes.com/sites/kashmirhill/2012/07/20/using-twitter-to-help-expose-psychopaths/

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

17 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: O. 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.

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.

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.[18] If citizens do increasingly consider exercising democratic rights such as participating in political discourse, civic engagement forms of public protest and alike as potentially disadvantageous or even dangerous, it can be spoken of the civil society being at stake.

Alternative concepts

Chapter 5 offers an overview of theories, concepts and approaches that can be taken into account as alternatives to (technological) surveillance-oriented security solutions. Societal concepts are investigated on the basis of their potential to function as alternatives; advantages and disadvantages are identified and critically assessed. These in detail investigated concepts are:

Security Communities

Restorative Justice

Communitarianism and community crime prevention

Social resilience and community resilience

Further alternative approaches trying to enhance security can as well be envisaged. Attempts to maintain and increase (feelings of) security are e.g. being made through urban planning. 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. Also, the wide field of science communication (and/or public understanding of science) can be regarded as a key factor for an inclusion of the general public into the debate and ideally for policy-making.

It can be stated that adequate responses to security threats can be developed in different ways. 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 hand a response can focus on the minimization of damage caused by an event; or – possibly most important – measures are to be taken towards strengthening *resilience,* and a resilience-aware society.

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. They cannot present the crisp and superficially convincing logic of technological solutions often. They operate in a larger, cultural, societal frame, and they approach the problem often in a more indirect way when looking at so-called root causes.

Conclusion

While a standard approach would step up security and surveillance measures to prevent criminal activities, a 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

[18] 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.

instead of being an evil force imposed from outside. Hence any effort at prevention will dominantly look at these inner processes as root causes for security problems.

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 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.

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. 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.

1. Introduction

In recent decades there has been a great deal of interest in scientific research on the rise of globalization, neoliberalism and terrorism. Major schools of thought have been built up and established providing the scientific community as well as the interested lay public with ground-breaking studies and elaborate theoretical frameworks on the powerful impact these developments have on the accelerating transformation of contemporary societies. It is possible to gain the impression that we live in more diverse societies than have possibly simultaneously ever emerged before in the history of mankind. Risk societies, surveillance societies, network societies, late-modern or optionally postmodern societies, multicultural societies, clash of civilizations – what all of these 'societies' have in common though are strong effects of augmentations of societal destabilization and fragmentation on one hand and the growing societal need for security in a somewhat insecure disintegrating world on the other hand.

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. Neither can it be overlooked that many nation states – most often in the name of the fight against crime and terrorism – are excessively extending their military and security industrial complexes. Furthermore, this process is accompanied by an ongoing 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, raising all sorts of questions about the destructive potential it has and will have on fundamental civil rights such as the right to privacy.

But while there is a broad range of scientific research on security versus privacy, so far astonishingly little attention seems to have been paid to conducting research for alternative strategies that go beyond surveillance-oriented security solutions (SOSSs) and furthermore comparatively little attempt seems to have been made to introduce existing strategies from other fields and disciplines into this debate. There are promising societal approaches – whether it be some problem solving on a micro-scale from within local communities or some middle-range theories – which will be conducive for the continuing debate around SOSSs versus (societal-rooted) alternative security solutions.

The current state of critical security studies with regard to these topics, where policy initiatives have called for increased surveillance measures to step up security, will be reviewed and paradoxes of security and privacy will be pointed out. 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. Assuming that in a greater part of the public debates the *visibility of security threats* seems to be more important than the *presumed threat levels*, we will scrutinize the evidence brought forward to make the case for surveillance: what kinds of threats are presented and what kind of reasoning unfolds in policy discourse to justify surveillance measures.

From a legal perspective surveillance and infringements on privacy are justified with the perceived security threats. We will investigate to what extent the claims brought forward in political discourse with regard to security threats can be substantiated through independent evidence (i.e. data not produced by those agents who then are the – political and economical – beneficiaries of new surveillance practices). It also can be investigated how decisions about the introduction of new surveillance systems and technological measures are made. Having done this, we will be able to identify those security problems that stand the test of seriousness.

The objectives of this task are in brief:

- Deconstructing security threats into their constituent parts;
- Elaborating on the concept of security;
- Analysing the side effects of security and surveillance practices for various stakeholders and;
- Collecting ideas and concepts for alternative security solutions.

A main object of this task is to offer some overview of the variety of alternative theories, concepts and methods. Alternative strategies that go beyond surveillance oriented security solutions (SOSSs) are to be investigated. The analysis of alternatives will take up the security discourse and demonstrate how and where security can be maintained with less (technology-based) surveillance. It will be examined if, or to what extent, these approaches bear the potential to function as alternatives to SOSSs. As the leading requirement therefore is to maintain or even enhance security without infringing democratic rights and undermining privacy, the findings will be measured against these standards.

1.1 Interdependencies within the SurPRISE project

This report represents one part (deliverable 3.3) of the Work Package 3 – Exploring the Challenges – within the SurPRISE project. The main aim of Work Package 3 is 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. Therefore this task 3.3 (societal developments/alternatives) is tightly connected to the task 3.1 (technological developments) and the task 3.2 (legal developments).

Task 3.3 also interacts with the results of Work Package 2 (Framing the Assessment), which focuses on assessing surveillance-oriented security solutions; task 3.3 has some impact on Work Package 4 (Questionnaire and Information Material) and it will furthermore provide basic background for Work Package 6 on the analysis and synthesis report within the whole project.

The identified alternative 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; some alternative security solution approaches will probably be used as (test case) examples in the multi-national participatory citizens' events to follow in the further SurPRISE Work Packages 5 to 7.

Since in task 3.4 the individual findings of the tasks 3.1–3.3 are to be integrated into one synthesis report, the deliverable D 3.4 will thereafter put 'Exploring the Challenges' into a broad context, compiling expertise in the fields of technological, legal and social sciences.

1.2 Outline

The report consists of six chapters. This introduction is followed by Chapter 2 (Research Approach), which offers – besides a brief methodological explication of the approach to the task – necessary elaborations on the main operational terms. Chapter 3 (Challenges) elaborates on how various challenges and threat potentials are perceived and exerted on a societal basis. Problems like calculations based on non-events, black swans, bounded rationality or function creep are discussed. Chapter 4 (Implications) merely examines existing security technology investments, focusing on the implications they have for (the cohesion of) society. Aspects like social profiling and social sorting, discrimination and human rights are debated. Chapter 5 (Alternative concepts) offers an overview of theories, concepts and approaches that can be taken into account as alternatives to (technological) surveillance-oriented security solutions. Their potential to function as alternatives, advantages and disadvantages is identified and critically assessed. Finally, Chapter 6 (Conclusion) argues for an alternative perception of (European) societal threat potentialities and recognition of security in a societal context rather than primarily as an

issue in need of a mere technological fix, and advocates a balanced view of the risks of living in late modernity.

2. Research approach

2.1 Methodology

The research approach of this task is primarily sociological and criminological. A theoretically informed empirical approach will be taken and thus be completed with a literature review. Methodologically, this task will use the tool kits developed in Science and Technology Studies (STS) and different strains of contemporary social theories such as Surveillance Studies and others. The key concepts of security, surveillance, risk, threat, and resilience will be elaborated and put into perspective for the work in this task. Various theories and scholars will be taken into account for the discourses about privacy and security and SOSSs versus non-technological alternatives. A range of theories, concepts and methods will be collected to serve as possible alternatives to the propagation and implementation of (technology-based) surveillance. The social processes underlying surveillance and security will be investigated and also the effects these processes have, taking into account the wider social context often neglected in security experts' discourse. In doing this, we will enter into what has been termed a 'replacement discourse', i.e. reframing specific phenomena presented as security problems.

As Lederer explains: '*When sociologists look at privacy, they see social nuances that engineers overlook. When cryptologists consider privacy, they see technical measures that everyday people ignore. When the European Union looks at privacy, it sees moral expectations that American policymakers do not.*'[19] This task is looking at privacy, security and surveillance from a social science perspective.

2.2 Security, surveillance and privacy as terms and concepts

As we are going to excessively use 'security', 'surveillance' and 'privacy' as operational terms, a digression on the manifold character of these terms is required to clarify our connotations of security, surveillance and privacy.

2.2.1 Security

Security has been defined in different ways by different academic disciplines. The most general definition of security as a 'dynamic non-event'[20] demonstrates the problem of pinning down the concept with a precise definition. In trying to achieve a more detailed definition of 'security', an initial step can be taken by examining the dictionary definition, notably the German 'Wörterbuch der Soziologie' (=Dictionary of Sociology). Since in the German language no distinction is made between 'security' and 'safety' (both translate as 'Sicherheit'), and this is furthermore the case in the majority of European languages[21], this approach illuminates the equivocal use of the term 'Sicherheit/security'. '*Security is a social, ambiguous term for social objectives and programmes, as well as valuable social symbols in terms of security, reliability and the absence of risk, certainty. Security enfolds the security of individual societal status as well as the protection of the social conditions of the individual or of society as a whole through increasing social service/benefits, legal certainty, (societal) order through the institutionalization of conflict and the*

[19] Scott Lederer u. a., "Five pitfalls in the design for privacy" (2005); p. 422.
In: Lorrie Cranor and Simson Garfinkel (Ed.), *Security and Usability: Designing Secure Systems That People Can Use* O'Reilly Media, Inc. (2007).

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

[21] Compare e.g. Italian (=sicurezza), Spanish (=seguridad), Hungarian (=biztonság), Danish (=sikkerhed), Finnish (=turvallisuus), French (=sécurité), Dutch (=veiligheid) etc.

transparency and predictability of social relationships. Objective social security must be distinguished from the subjective feeling of social security. […]. ' [22]

As revealing as this definition is, the use of the term 'absence of risk' is highly contentious. (*We will be coming back to that in the chapters 'Challenges' and 'Conclusion: Towards balanced risk awareness'.*) Since being at risk is a somewhat ambivalent condition of being alive, we prefer to follow Beck's rationale: '*Risk is ambivalence. Being at risk is the way of being and ruling in the world of modernity; being at global risk is the human condition at the beginning of the twenty-first century.*'[23] Global economic, social, environmental and military conditions make the absence of risk and therefore absolute security/safety per se impossible.

Besides this minor critique, the definition provided above exemplifies well why any idea of a common (European) view on the 'concept of security' must fail in the first place. When e.g. German speakers debate 'Sicherheit' – if the discussion isn't clearly limited to special aspects as in 'security regarding the functionality of technical devices' – they presumably create a different mindset than e.g. English speakers do.

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). Perceived security refers to an individual's subjective perception of feeling secure or insecure. A number of studies in criminology[24] have demonstrated the so-called 'security paradox': individuals may feel insecure despite the fact of low victimization risks and vice versa.

On an individual basis, security can be approached in either a subjective or an objective way, which might mark the difference between a real threat and a perceived threat. Whether a threat is in an objective sense real or not, does, however, not matter for the further course of action: '*If men define situations as real, they are real in their consequences.*'[25] In the face of ubiquitous threats and a tremendous decrease of social security measures in the course of neoliberal policies, one's 'need' for security will aim probably at first at the individual life-design, but also contextualize e.g. in the fear of austerity, fear of nuclear power or, on an even broader scale, as 'national security', translating neatly into 'fear of terrorism'.

In addition, yet another ambiguity complicates attempts to conceptually frame security. Multiple aims of security have to be taken into account: '*Security is revealed as an objective policy goal, as subjective perception, as pursuit and practise, as symbolic assurance, and as a public good at the heart of the modern state.*'[26] Owen[27] suggests a methodological division into four categories of human security: human security as a policy tool, as a means of issue appropriation, as an exercise in measurement and as a critical tool. Debating human security, a number of questions have to be taken into account: Who are the actors taking part in *securing security*? What are their particular interests? Who is securing whom? Being secured by the state (as in 'national security') or being secured from the state (as in 'protection of privacy') draws another demarcation line. It does, though, make a difference whether the state, organizations, industries, individuals or civil society are to be secured. In the case of fighting terrorism all of the above are subject to being secured by all means – but not in the case of e.g. law enforcement agencies clashing with civil society demonstrators protesting against austerity. In the latter case it is also the state securing itself from its very own citizens.

---

22 Translation from German into English by Regina Berglez. Karl-Heinz Hillmann, *Wörterbuch der Soziologie,* Stuttgart: Kröner (2007). p. 778.

23 Ulrich Beck, *Risk society : towards a new modernity*, London u. a.: Sage (2007). p. 330.

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

25 Robert K. Merton, 'The Thomas Theorem and The Matthew Effect', *Special Forces* 74 (2) (1995): pp. 379–424.

26 Lucia Zedner, *Security*, London; New York: Routledge (2009).

27 Taylor Owen, 'Human Security. A Contested Contempt', In: *New Security Studies* (2010), pp. 39–49.

An individual can either get in the focus as a 'security threat' owing to a particular situation or for being member of a group, subject to racial, ethnic or political negative social profiling. The fundamental demarcation line is drawn between those *who have to be protected* and those *'society' has to be protected from*. The catchwords here are terrorism and deviancy.

It can be stated that different readings of security are socially contextual and ambiguous, even equivocal. Security varies through time and space, relates to threats and risk as well as to basic social conditions, holds different levels of abstractness, is symbolic or 'real' (or both), and highly dependent on perception. In this sense, human security is first and last and always a social construct.

Security as a discursive object has been elaborated in security studies.[28] Any social field can be 'securitized', i.e. talking about a social object or process in terms of security changes the dominant discourse, mindset 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[29] and can therefore be (re-)created as an entity of security matters.

2.2.2 Surveillance

Within the SurPRISE project, we are referring to a basic joint definition of surveillance in the security context as follows: 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 risk and to enable, typically, a preventive, protective or reactive response, or the collection of data for preparing such a response in the future.

We are stating, furthermore, *that the major aim of surveillance is to name, identify, monitor and track individuals and their actions*, and to aggregate and analyse these collected data in a next step to figuring out individual as well as group patterns; whether this is done for statistical measures or national security reasons by governmental authorities or whether this is done by commercial enterprises for consumer relations or customer pattern recognitions is not of interest for a basic definition of surveillance in the first place. In Bennett's and Regan's words, that basic definition is: '*Surveillance is a means of determining who is where and what they are doing, either in the physical or virtual world, at a particular point in time. This is the basic purpose of surveillance and the most common goal of surveillance systems. These systems help answer the question of who is where, at what point in time, and what are they doing.*'[30]

For capturing the logic of surveillance measures, it has to be added that surveillance is not fixed to either a physical appearance and/or electronic data traces, nor is security static in time and space. Surveillance can be understood as: '*Monitoring of the physical, mental, economic, cultural, social or other activities of identified or identifiable individuals, irrespective of the means and methods applied, whether automated or human interaction-based, mass or individually targeted, continuous, repetitive or ad hoc, perceptible or imperceptible, done physically or from a distance by means of electronic equipment, done in real-time or retrospectively, based on the activities of the individual him/herself or on the analysis of the personal data of the individuals concerned.*'[31]

---

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

[29] Ibid.

[30] Colin J. Bennett and Priscilla M. Regan, 'Surveillance and Mobilities', *Surveillance & Society* 1, Nr. 4 (2002) http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/3330.

[31] ETICA-project (2011), 'Glossary, DEL 5.3.' p.119 . http://ethics.ccsr.cse.dmu.ac.uk/etica/deliverables

2.2.3 Privacy

Attempts to capture the exact meaning of privacy have been made by a considerable number of scholars from various disciplines.[32] Definitions of the term privacy are controversial and in flux; privacy was even referred to as a conceptual jungle.[33] There is no consistent or distinct definition or conceptual framework on privacy yet. We will refer to privacy in a broad sense, taking into account that it is well possible to infringe one's privacy without processing data; privacy can '*be understood* […] *as contextual integrity where the core problem is sharing of information outside of socially agreed contextual boundaries.*'[34] [35]

We follow Bennett's elaboration on privacy: '*As most of the literature notes, privacy is an elusive and multidimensional concept whose meaning is culturally and historically contingent. Yet, it is still the concept that tends to define the policy issue in advanced industrial societies, and it is still the concept around which challenges to excessive surveillance get framed. At root, it has tended to mean the extent to which individuals have control over the circulation of their personal information. Surveillance, broadly defined, challenges that right or interest.*'[36]

The right to privacy is stated in article 12 of the Universal Declaration of Human Rights: '*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, or to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.*'[37] The EU Charter of Fundamental Rights also states in article 8 a number of protection measures for personal data and data processing.[38] Following the definition provided in D 3.1, from a legal perspective, privacy has to be understood 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.*'[39]

In the context of surveillance, data protection is *a core element of privacy*. Data protection shall hereby be perceived in a broad sense as well. Following the definition provided by the ETICA-project, data protection is understood as '*the complex of principles, norms, procedures, data processing devices, means and methods restricting the collection, processing and use of personal data, and protecting the persons concerned.*'[40]

It is a crucial fact that the possibility of violations of data protection cannot be ruled out, since wherever data is collected, stored and processed, data can be lost, stolen and leak out.

'*Personal data do tend to leak out of organizations in an uncontrolled way, often owing to negligence of the data processors, and stored data are rarely encrypted and are thus easy to read.*'[41] Once data has leaked out

---

32 Comp. e.g. Daniel J. Solove, *Understanding Privacy*, Harvard University Press (2008); Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy*, Univ. of North Carolina Press (1995); Barrington Moore, *Privacy: Studies in Social and Cultural History*, M. E. Sharpe (1984).

33 Solove, *Understanding Privacy*.

34 IRISS-project (2012), 'DEL. 1, Surveillance, fighting crime and violence report' p. 19. http://irissproject.eu/?page_id=9

35 L. Hansen and H. Nissenbaum, 'Digital disaster, cyber security, and the Copenhagen School', *International Studies Quarterly* 53, Nr. 4 (2009): 1155–1175, http://onlinelibrary.wiley.com

36 Colin J. Bennett, *The privacy advocates: resisting the spread of surveillance*. Cambridge, MA: MIT Press (2008). p. xi (Introduction)

37 Universal Declaration of Human Rights: http://www.un.org/en/documents/udhr/index.shtml#a12

38 Charter of Fundamental Rights: http://europa.eu/legislation_summaries/justice_freedom_security/combating_discrimination/l33501_en.htm

39 Scheinin (2009), Rodotà (2009) cited in SurPRISE task 3.2. p. 4

40 ETICA-project (2011), 'Glossary, DEL 5.3.' p. 13. http://ethics.ccsr.cse.dmu.ac.uk/etica/deliverables

41 John Borking, 'The use and value of privacy-enhancing technologies' (2005) 69–95, p.76. In: Susanne Lace (Ed.), *The Glass Consumer: Life in a Surveillance Society*, The Policy Press (2005).

little can be done, more so if the information is floating in cyberspace. 'Information' cannot be taken back.

What was pointed out about security above is partly true for privacy as well: Any comprehension of privacy is individually subjective, socially contextual and ambiguous. From the legal perspective it is argued that core elements of the human condition are always to be seen as private. This points towards a basic *concept* of privacy as elaborated in D 3.2. From a social science perspective, *practices* of privacy can be seen as varying through time and space, holding different levels of abstractness and depending strongly on perception and in this sense can be understood and examined as socially constructed. To gain common ground within Work Package 3, we follow the division between the *concept* and the *practice*: '*Privacy as a whole can be described as a triangle of the concepts of privacy, privacy practice and the accountability principle as a measure to influence the practice according to the spirit of the concept.*'[42]

[42] Daniel Guagnin, Leon Hempel and Carla Ilten, 'Privacy Practices and the Claim for Accountability', p. 101. In: Schomberg, Rene, *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, Luxembourg: Publication Office of the European Union (2011).

3. Challenges

3.1 Security, securitization and risk perception

As mentioned, security problems – ranging from terrorist threats to petty crime and from vulnerable infrastructures to volatile financial markets – are perceived as major challenges to modern societies, perpetually producing risk. Acknowledging these threat potentials is a first step, which requires the acceptance of a number of risks emerging in globalized, networked societies with hitherto unknown mobility of material and symbolic goods, persons and information.[43] 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 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.*'[44]

First, precisely identifying causes and designing adequate countermeasures is a difficult and bold venture: the absence of evidence is not the evidence of absence, as one of the security hawks in the Bush administration would repeatedly remark, quoting a key phrase of the black swan theorem.[45] This nicely brings the logic of security discourse to the point. From a strictly logical point of view, the fact that no major incident has occurred (aeroplanes crashing into high-rise buildings, bombs being exploded in metropolitan areas etc.) 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. The logic of security policies requires these measures to be applied comprehensively to each and every individual in order to sort out the potential predators. Taking the highly dramatized security threats as a justification (or pretext), the different practices 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 of such an event. This process of narrowing down the focus of policy debate to one single dimension – security – has been termed 'securitization'.[46]

Second, securitization creates a mind-set focusing on prevention, and once the logic of prevention gains momentum there are no stop rules or internal limits to preventative strategies. However, some legal scholars attempt to implement what is termed the 'permissible limitations theory' to lay down a constitutional provision for such permissible limitations. *(Comp. D 3.2, especially Chapter 4: 'A core-periphery approach? The fundamental norm of the right to privacy and permissible limitations'.)* The logic of prevention maintains that in the perceived causal chain leading to an event, an early intervention should take place to interrupt the future course of action. When a bottle of liquid explosive can be taken aboard an aeroplane, prevention requires banning liquids from being transported in aeroplanes. The empirically substantiated observation that out of several millions of bottles carried by passengers not a single one may contain an explosive is irrelevant for securitized prevention. Besides that, e.g. securing (passengers from) liquids may just be seen as a placeholder, as Schneier puts into perspective: '*If we concentrate airport security on screening shoes and confiscating liquids, and the terrorists hide explosives in their brassieres and use solids, we've wasted our money. Terrorists don't care what they blow up and it shouldn't be our goal merely to force the terrorists to make a minor change in their tactics or targets. Our*

---

43 John Urry, *Mobilities*., Cambridge, UK; Malden, MA: Polity (2007).
44 Charlie Edwards, *Resilient Nation*. Demos, (2009) p. 16.
45 Nassim Taleb, *The black swan : the impact of the highly improbable*. London: Penguin (2008).
46 Buzan, Waever, and Wilde, *Security*.

penchant for movie plots blinds us to the broader threats. And security theatre consumes resources that could better be spent elsewhere.'[47]

The fact that modern communication technologies may be used by potential perpetrators coordinating their actions justifies a comprehensive screening of Internet traffic to detect suspicious conversations. Ample evidence suggests that only a tiny fraction of Internet traffic can be linked to criminals; nonetheless, from prevention logic this is considered as irrelevant. Proportionality is not considered in the mindset of a security expert focusing on prevention.

The frame of reference based on the logic of securitization and 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. Furthermore this logic is irrefutable since it is based on non-events. Implementing a preventive measure (banning liquids on airplanes, intercepting electronic communication) can be said to be successful when nothing happens. Should something happen, despite the assumed preventative effects of the security measures implemented, the next turn of the screw is due and surveillance and control will be stepped up. Public policy takes threats, risks and security as key drivers for the implementation of surveillance and control regimes.

Third, it is very difficult to assess the seriousness or magnitude of security threats. This is owing to their very nature: security threats are projections of future events, typically perceived from a perspective of risk logic or risk-based reasoning. A risk-based reasoning assesses alternative options for present action to avoid future damages. This forward-looking approach is similar to neo-classical economic reasoning: the price paid for a commodity (or the investment made today) cannot be read off the commodified object but is valued based on assumptions about future development of prices (or returns). In a way, risk-based reasoning displays a kind of negative economical thinking: present actions are valued based on assumptions about the probability of future damages, triggered by these actions. Comparing the field of security threats with the field of economics can help to better understand the underlying problem that can be analysed as a problem of temporal order. It is not the present state of affairs that matters, but the projected course of events.

That also points to the fourth problem: *how to measure security threats?* Typically the formula for the assessment of risks is applied to solve the problem: multiplying the calculated probability with the expected damage. '*Security historically dominates privacy in crises such as attacks, but the current security threat is cast as ongoing, with no near-term conclusion possible.*'[48] This indefinite nature of the conflict seems thus to create novel circumstances. Is the reasoning done in a rational and responsible way, data about past events has to be taken into consideration. This can be done as long as historical data is available, which is not always the case, since often security threats are introduced as 'novel' and hitherto unknown.

3.2 Crime and terrorism

Looking at the security threats with the highest public and political priority, we find a similar situation as with the surveillance practices: it is very difficult to draw a precise line to define them. Terrorism is a catch-all category, applicable to almost all situations. For surveillance technologies this means that all forms of surveillance may be justified in preventing and combating terrorism.

John Urry, *Mobilities*, Cambridge, UK; Malden, MA: Polity (2007).

47 Bruce Schneier 'Beyond security theatre', *New Internationalist,* (2009) http://www.schneier.com/essay-292.html

48 Chris C. Demchak and Kurt D. Fenstermacher, 'Institutionalizing Behavior-Based Privacy', *Administration & Society* 41: (7) (2009): 783–814, p.790.

3.2.1 A few notes on terrorism

Terrorism in the post-Second World War context is a term applied by politicians and media to attacks on civilian, state and military targets that are conducted outside of a war zone recognized by the same politicians and media. The word terrorism has been emotive for 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 and Madrid. In the period between and including World War I and World War II, weapons now regarded as weapons of terror were considered for use among civilian targets to cause demoralization. Winston Churchill, for instance, held the following opinion: '*I do not understand this squeamishness about the use of gas. We have definitely adopted the position at the Peace Conference of arguing in favour of the retention of gas as a permanent method of warfare.* […] *I am strongly in favour of using poisoned gas against uncivilized tribes. The moral effect should be so good that the loss of life should be reduced to a minimum.*'[49]

In the initial post-WWII period, terrorism became identified with the type of attacks such as those made by the Jewish Resistance Movement in trying to force the British out of Palestine and the formation of the Israeli state. Although many attacks were directed at infrastructure such as railways and bridges, the attack that crystallises the modern perception and interpretation of a terrorist act by the public was the bombing of the King David Hotel by the Irgun group.[50] This attack was aimed at the British military base in the hotel but resulted in the death of 91 civilians.

Although history may have recognized the causes terrorists support as just and proper, despite the means being vilified, many individuals identified as terrorists find that their labelling as such by governments and media continues beyond the legitimization of their cause. As a member of Irgun, Menachem Begin was labelled a terrorist and this label was maintained despite him becoming Prime Minister of Israel and receiving a Nobel Peace Prize.[51] Similarly, despite being released from prison in 1990 and becoming South Africa's first president following the collapse of the apartheid regime, Nelson Mandela only had restrictions born of his terrorist status lifted by the U.S. in 2008.[52]

For the most part until the 1990s terrorism was divided into two categories for Europe; international and domestic. International terrorism, with a few exceptions, occurred outside European boundaries and was executed by non-residents of Europe. These attacks again varied, from attacks on infrastructure through to the taking and killing of hostages. Domestic terrorism in Europe was largely committed by European citizens and reflected conflicts relevant to the countries involved. This included groups such as the Red Army Faction in Germany, Euskadi Ta Askatasuna (ETA), who want independence for a particular region of Spain, and both the Loyalist and Republican groups in Northern Ireland, who disputed the sovereignty of the territory. Despite these terrorist activities, security measures that caused comparatively minimal disruption were put in place to counter these threats. Such measures included e.g. the removal of refuse receptacles in central London and the so-called 'Ring of Steel' around the City district of London.[53]

---

[49] Martin Gilbert and Randolph S Churchill, *Winston S. Churchill. Vol. 4. Companion volume. Part 1, January 1917–June 1919*. Boston: Houghton Mifflin (1978).

[50] No author or date, Princeton Edu, 'King David Hotel bombing' http://www.princeton.edu/~achaney/tmve/wiki100k/docs/King_David_Hotel_bombing.html

[51] No author (1992), Deseret News 'Menachem Begin' http://www.deseretnews.com/article/214526/MENACHEM-BEGIN.html?pg=all

[52] No author (2008), BBC 'Mandela taken off U.S. terror list' http://news.bbc.co.uk/2/hi/7484517.stm

[53] Bain (1996), 'London's ring of steel' http://www.independent.co.uk/news/londons-ring-of-steel-to-expand-1313139.html

The unexpected collapse of the Soviet Union and opening of the Warsaw Pact nations at the end of the 1980s suddenly left the U.S. and large parts of Europe without a 'suitable enemy'[54] both to justify the military industrial economy and to unite the nation against. In the 1990s the colonial concept of 'gunboat diplomacy' was expanded beyond the use of naval bombardment and attack aircraft to using the Tomahawk cruise missile giving rise to the term 'cruise missile diplomacy'.[55] However these were frequently disproportionate responses (if not totally erroneous in the choice of targets) to attacks or alleged involvement in attacks[56] or even allegedly plotting attacks.[57] It has even been suggested that the 1998 Tomahawk attacks on camps in Afghanistan, which had connections to Osama bin Laden, provided the catalyst to closer relations between the Taliban regime and al-Qaeda owing to the deaths of Afghan citizens.[58]

With the September 11th 2001 attacks in the U.S. this empowered Islamist network provided the new 'suitable enemy' that the U.S. 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 relatively passive 'Reds under the beds' Cold War spying fear to an active fear of neighbours with 'guns, gas, germs or grenades under their pillows'. Failed raids[59] and the media's attention to Islamic converts such as the 'Shoe Bomber' and the 'American Taliban'[60] further served to increase the public's paranoia.

Despite arguably providing no greater threat than the historic domestic terrorism (the Provisional IRA almost succeeded in killing the sitting Prime Minister of the UK in 1984)[61], this new hybrid international/domestic terrorism has been used to justify increasingly pervasive and intrusive new security measures. As Demchak puts it: '*The possibility of unknown and uncontrollable actors beyond national boundaries in millions of small decisions changing the internal dynamics of our nation is hugely problematical in practical and theoretical terms.*'[62]

Groups that are dedicated to domestic political change are finding themselves increasingly labelled as terrorist organizations, justifying draconian measures to be taken against these groups. Additionally, some governments and justice systems are trying to identify merely criminal acts as terrorist.[63] Despite these attempts to misuse the term 'terrorist' by governments and justice systems to investigate, curtail

---

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

55 Sparks (1997), 'The Dawn of Cruise Missile Diplomacy' http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA333251

56 Zill (no date), 'The controversial U.S. retaliatory missile strikes' http://www.pbs.org/wgbh/pages/frontline/shows/binladen/bombings/retaliation.html

57 Drehle and Smith (1993), 'U.S. strikes Iraq for plot to kill Bush' http://www.washingtonpost.com/wp-srv/inatl/longterm/iraq/timeline/062793.htm

58 U.S. National Security Archive (2008), '1998 missile strikes on Bin Laden may have backfired' http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB253/index.htm

59 Walker and Fickling (2006), 'Police apologise to east London raid family' http://www.guardian.co.uk/world/2006/jun/13/terrorism.uk

60 Tyrangial (2001), 'The Taliban next door' http://www.time.com/time/nation/article/0,8599,187564,00.html

61 No author (1984), BBC 'Tory Cabinet in Brighton bomb blast' http://news.bbc.co.uk/onthisday/hi/dates/stories/october/12/newsid_2531000/2531583.stm
Additionally Wilson (2000), 'Brighton bomber thinks again' http://www.guardian.co.uk/uk/2000/aug/28/northernireland.jamiewilsonv

62 Demchak and Fenstermacher, 'Institutionalizing Behaviour-based Privacy', p.784.

63 Comp. E.g. Okan (2012), 'Hacker group accused of being an armed terrorist organization' http://sosyalmedya.co/en/redhack-accusation/
Lemieux (2012), 'UK's Gary McKinnon extradiction call reflects scepticism about US justice' http://www.guardian.co.uk/commentisfree/2012/oct/17/gary-mckinnon-extradition-scepticism-us-justice
Schmidt (2012), 'F.B.I. Counterterrorism agents monitored occupy movement, records show' http://www.nytimes.com/2012/12/25/nyregion/occupy-movement-was-investigated-by-fbi-counterterrorism-agents-records-show.html?_r=0

and punish undesirable groups, there still is a prejudice in media to assume that terror attacks are Islamist as e.g. the Breivik attacks in Norway demonstrated.[64]

The use of disproportionate gunboat and cruise missile diplomacy, particularly against Islamic organizations or populations, coupled with increased military presence in Islamic countries caused an increase in Islamic groups willing to use violence and terror tactics in response. Attacks by these Islamic groups on domestic territories gave a justification for continued military expenditure for defending against international targets and also massive increases in domestic securitization using the emotive threat of terrorism as a justification.[65] Additionally large parts of the popular media actively propagate the idea that significant new threats exist and securitization is justified despite the fact that domestic terrorism has been a fact of life – at least since the inter-bellum period or arguably even before WWI – for many European and NATO nations.

3.2.2 Fear of crime

Although sociological research on deviant behaviour and crime etc. dates back to the 'Chicago School' of a century ago, it became re-recognized on a large scale in the 1970s. Consequently 'fear of crime' came into focus as a research subject.[66] By contrast, within the following decades crime started to become in the political debate – slowly but steadily – perceived as an issue to be overcome either by technological solutions and/or by securitization.

A number of studies conducted in the 1980s created substantial knowledge on these subjects. For instance, Lewis and Salem published an innovative study on the connections between crime and broader social aspects in 1986.[67] On the basis of an excessive data collection carried out from 1975 to 1980, they indicated that concepts or feelings of safety are closely linked with the social control perspective – i.e. fear of crime and fear of victimization – but also correlate strongly to neighbourhood characteristics and detection, which they could primarily narrow down to the lack of control people feel to have over their (social) environment.[68]

The political outcome on the basis of such findings (back then as well as in present times) leads to various lines of political action: to programmes such as 'zero tolerance' at one end of the scale or to *social* neighbourhood programmes and the like at the other. (The latter will be elaborated on in the chapter 'Alternative concepts'.) While these programmes indeed share a common ground in endeavouring to increase (feelings of) safety – and control – in local vicinities, 'zero tolerance' is to a greater extent connected to technological security solutions and thus not addressing root causes whereas social programmes do aim at grasping a wider perspective.

Hence, a broader perspective on the character of fear is advisable, as Vanderveen indicates: '*Fear of crime is an umbrella concept that embraces all kinds of indicators and concepts and is not even so much about "fear" and "crime"*,'[69] and elaborates furthermore: '*In many studies "fear of crime" means the fear for one's safety and the experience of safety, which is perceived to be threatened by an expected, perceived or encountered "dangerous" other person. "Fear of crime" then interacts with the perception of risk, an*

---

64 Teller (2011), 'The Norway terrorist attacks: News without facts' http://www.globalresearch.ca/the-norway-terrorist-attack-news-without-facts-experts-on-jihad-and-muslim-terrorism/25761
Brooker (2011), 'The news coverage of the Norway mass-killing was fact-free conjecture' http://www.guardian.co.uk/commentisfree/2011/jul/24/charlie-brooker-norway-mass-killings

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

66 For an extensive overview, see Jason Ditton and Stephen Farrall, *The Fear of Crime*. Ashgate/Dartmouth (2000).

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

68 Ibid.

69 Gabry Vanderveen, *Interpreting Fear, Crime, Risk, and Unsafety: Conceptualisation and Measurement*. Boom Juridische Uitgevers (2006). p. 4.

estimation that an undesirable or dangerous event will occur and the subjective assessment of one's own ability to deal with the possible threat, the imminent danger.'[70]

Also, perceptions of personal risk in everyday situations frequently do not equate to the mathematically predictable risk. Risks, taken on an individual basis, from smoking to engaging in hazardous sports, drunk driving or investing in stocks are judged on an entirely separated level of individual perception.[71] Risks are reactively calculated and compensated in everyday life.[72] '*Risk is not "'objective"' but produced, negotiated and manipulated within social interaction, for example, sometimes taking specific risk is socially legitimated.*' [73] In other words: Risk as such is not neutral and neither is the framework surrounding it.[74]

Scheingold, besides others, noted in the 1980s that calls for law and order got integrally linked not only to direct crime rates but also to rapid and unwelcome social change.[75] Beckett states for the U.S. that as early as the 1960s Conservatives began to use the crime issue in their critique of the welfare state.[76] She also notes that public fears about the social order were translating into social inequality (like protest against racial injustice or poverty which got channelled by a symbolism on 'fear of crime'). This is suggesting some interesting parallels to contemporary conditions in Europe and its citizens' anti-austerity protests and the like. Beckett frames her findings with the democracy-at-work thesis[77], elaborating also on the impact of political and media discourse on popular attitudes. The thesis theorizes that approaches to crime control are reflecting the worsening of the crime problem and the public sentiment about it[78], and that these are presented cursorily in no need for further elaboration,[79] coming to the conclusion that '*the ascendance of the rhetoric of policies of law and order is not an expression of democracy in action. Rather* […] *the effort to replace social welfare with social control as the principle of state policy.*'[80]

Fear of crime and terrorism trigger hitherto unprecedented efforts by state authorities to gather data in order to combat the perceived threats emanating from these 'social evils'. In the following pages we will address the different forms of data collection, and their intended and unintended effects.

3.3 Data collections

3.3.1 Data flow

One of the central strategies of increasing security is the control of individuals to identify potential attackers. This typically entails the collection, storage and processing of person-related data.[81] These data can be used to selectively exclude individuals or have them undergo further scrutiny. This process of social sorting[82] creates a social practice that has been termed 'dangerization'[83], where the default

---

70 Ibid. p. 222.
71 Amos Tversky; Daniel Kahneman, 'The Framing of Decisions and the Psychology of Choice', *Science*, New Series, Vol. 211, No. 4481. (Jan. 30, 1981), pp. 453–458.
72 Alex Howard, 'Insecurity: philosophy and psychology', pp. 58–72.
In: John Vail, Jane Wheelock, and Michael J. Hill, *Insecure times: living with insecurity in contemporary society*. London; New York: Routledge (1999).
73 Ibid. p. 149.
74 Michaelis Lianos and Mary Douglas, 'Dangerization and the End of Deviance: The Institutional Environment', *British Journal of Criminology* 40, Nr. 2 (March 1) (2000).
75 Stuart A. Scheingold, *The Politics of Law and Order: Street Crime and Public Policy*. New York: Longman (1984).
76 Katherine Beckett, *Making Crime Pay: Law & Order in Contemporary American Politics*. New York: Oxford University Press (1999). p. 35.
77 Ibid.
78 Ibid. p. 4.
79 Ibid. p. 15ff.
80 Ibid. p. 106ff.
81 Comp. e.g. Gary T. Marx, *Undercover: Police Surveillance in America*. University of California Press (1990).
82 David Lyon, *Surveillance As Social Sorting: Privacy, Risk, and Digital Discrimination*. Taylor&Francis Group (2003).
83 Lianos and Douglas, '*Dangerization and the End of Deviance*'.

attitude in every social situation is suspicion: an actor has to prove s/he is entitled to enter into a transaction with an institution. The prototypical constellation is a person in front of an ATM: the machine does not differentiate on the basis of age, race, class or gender; all people are equal and anonymous when approaching this machine. But in order to enter into an exchange with the technical system (and e.g. draw money from an account), identification based on information controlled and provided by this technical system is required. The next levels are fingerprint required to gain permission to access files on a computer or an iris scan required to gain access to a certain area in a building. The logic of security policies requires these measures to be applied comprehensively to each and every individual in order to sort out the potential predators. Some form of identification code is stored in a database and the person who produces this code is granted permission to utilize the services this system offers. *'Knowledge of the population is now manifest in discrete bits of information which break the individual down into flows for purposes of management, profit and entertainment. While such efforts were originally a footnote to the historical rise of urban anonymity, they now constitute an important force in their own right.'*[84] Getting access to controlled spaces, services or information requires such procedures of proving one's innocence (or eligibility).

Two types of problems emerge here: (1) the information stored in the database for purposes of identification and granting access to service may be linked to other information without the person being indentified in front of the machine knowing about this; (2) the person producing the identification code may not be identical to the person whose data is stored in the database. Both problems can be solved in principle: the first by disclosing all information to the individual and the second by introducing multiple security checks and using e.g. additional biometric data for cross-checking identification. For security policies, the second type of problem seems to be more pressing: how to prevent an individual who is not entitled to gain access to a secured space or individualized service from overcoming the controls in place to protect this space or service? The solution to this problem typically entails a tightening and extension of control measures and links directly to the contemporary rise of biometric measures.

3.3.2 For example Biometrics

Biometrics can be seen as a form of identification and surveillance that operates on information gathered from the human body. The general logic of this form of surveillance is to link information, taken from the physical body, to a database containing other information about the person. The prototype is the fingerprint, used to identify an individual using a dactyloscopic database. In order to work effectively, a database containing information about a large number of individuals has to be established. From a surveillance perspective, the ideal solution would be to have some sort of bio-data from all persons (e.g. a national comprehensive DNA register or fingerprint register, etc.), so that every individual claiming an identity with a proper name can be checked against the bio-data stored in such a database. The problem that is supposed to be solved by this type of practice is the identification of an individual as being the person s/he claims to be, based on his/her biological existence.[85]

For instance, the state of India is currently creating the largest biometric database worldwide. By 2017, India aims to identify each of its roughly 1.2 billion inhabitants through a unique personal 12-digit number. Without any cost-ratio analysis done, a total of 36,000 registration offices have started to take three biometric measurements of all individuals: facial images, fingerprints and iris scans. The estimated

---

[84] Richard Victor Ericson and Kevin D. Haggerty (Ed.), *The New Politics of Surveillance And Visibility*. University of Toronto Press (2006), p. 619. Also: Richard Victor Ericson and Kevin D. Haggerty, *Policing the Risk Society*. Oxford University Press (1997).

[85] N. Rose and C. Novas, *Biological citizenship*. Blackwell Publishing (2004). http://webfirstlive.lse.ac.uk/sociology/pdf/RoseandNovasBiologicalCitizenship2002.pdf.

cost lies between 2.6 billion and 21.7 billion Euros. Civic advantages are supposed to be the simplification of access to bank accounts, social benefits and such like, but also a strong improvement in national security.[86]

Taking on Foucault, but analysing recent dynamics that go beyond Foucault, Haggerty and Ericson use the term 'surveillance assemblages'[87] to describe such forms of late-modern dataveillance. Through the process of assemblage, human bodies are abstracted and separated into a series of discrete (data) flows. In a second step, these flows are reassembled into distinct 'data doubles' for the purpose of scrutiny, targeting, sorting etc. They also state: '*In the process, we are witnessing a rhizomatic levelling of the hierarchy of surveillance, such that groups which were previously exempt from routine surveillance are now increasingly being monitored*.'[88]

The creation of biometric databases of whole populations might well be seen as the aim for ubiquitous identification of every single individual claiming an (institutionally certified) identity.

Collecting data on the population is seen as a dominant strategy to improve security in the face of perceived ubiquitous threats. Beyond the active collection of person-related data, surveillance-oriented security solutions also work on data sets originally produced for non-security related purposes. Since modern technologies continuously create machine-readable data sets of different transactions, it is easy to access person-related information under the pretext of fighting crime and terrorism. A major field of this form of surveillance-oriented security practice is electronic communication, producing large data sets stored in what has been termed 'the cloud'.

3.3.3 For example Cloud computing

Cloud computing is becoming more and more common, and (European) institutions are moving data as well as ICT operations into the cloud. Third-party states and other actors do have legal access to the data in the cloud; these include the U.S. government (mainly according to its 2001 Patriot Act) as well as government agencies across the EU, as Hoboken, Arnbak and Eijk stress.[89] They claim that '*the U.S. legal state of affairs implies that the transition towards the cloud has important negative consequences for the possibility to manage information confidentiality, information security and the privacy of European end users in relation to foreign governments*.'[90] Under the treaty of the Foreign Intelligence Surveillance Amendments Act, governmental organizations can arrange direct access to data of non-U.S. citizens living abroad, with no commitment even to transparency.[91] Hoboken et al. also remind all parties collecting and storing data that data is never secure. Data in the cloud is at greater risk of 'leaking', and of not being removed after deletion by the end user. Microsoft already stated in 2011 that EU citizens would not be informed in cases where the U.S. government accessed the personal data stored by Microsoft. Gordon Frazer, Microsoft Managing Director U.K., stated: *'Microsoft cannot provide those guarantees. Neither can any other company*.'[92]

---

86 Meister (2012), 'Die Mutter aller E-government-Projekte' https://netzpolitik.org/2012/die-mutter-aller-e-government-projekte-indien-baut-die-groste-biometrische-datenbank-der-welt/ and also: No author (2012), *The Economist*, 'India's UID scheme. Reform by numbers'. http://www.economist.com/node/21542814

87 Kevin D. Haggerty and S. Ericson, 'The surveillant assemblage', *The British Journal of Sociology*, 51,Nr. 4 (2000), pp. 701–717.

88 Ibid. p. 706.
David Brin(2004), 'Three cheers for the Surveillance Society!' http://www.salon.com/2004/08/04/mortal_gods/.

89 See Hoboken et al. (2012), 'Cloud Computing in higher education and research institutions and the US Patriot Act'. Abstract to be found at : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2181534

90 Ibid.

91 Whittacker citing Arback (2012), 'Patriot Act can "obtain" data in Europe, researchers say' http://www.cbsnews.com/8301-205_162-57556674/patriot-act-can-obtain-data-in-europe-researchers-say/

92 Whittacker interviewing Frazer (2011), 'Microsoft admits Patriot Act can access EU cloud data' http://www.zdnet.com/blog/igeneration/microsoft-admits-patriot-act-can-access-eu-based-cloud-data/11225

These concerns are highlighted in a recent study carried out on behalf of the European Parliament.[93] Bigo at al. stress that indeed the greatest challenges arising from cloud computing are not the possibilities for cyber fraud but the loss of control over individual identity and data.[94] They criticize that the legal ground is highly unclear: '*the set of relations currently defining cloud computing technologies encompasses negotiations and tension between public authorities, private entities and public and private authorities. In this set of relationships, data protection and privacy are often objects of negotiations to the detriments of the individuals' rights.*'[95]

Cloud computing can thus serve as a good example to demonstrate the presumed trade-off late-modern societies are supposedly facing between a desirable level of consumer convenience on one hand and an increasing risk of data violations accompanying this very convenience on the other. While public attention is focusing on cybercrime as the new threat emerging with the spread of ICT, creating the image of criminals moving into a new sphere, the rather mundane problems of data security, surveillance and privacy infringement are played down. An informed public debate about the functionality, advantages and disadvantages of such technologies is necessary for balanced risk awareness on an everyday level. This entails a better understanding of the magnitude of the new challenges flowing from so-called cyber criminals.

3.4 Cybercrime

Cybercrime is a comparatively new threat, and from a critical perspective it is far from clear whether it really creates a lot of damage. Nonetheless, all sorts of surveillance measures are justified with reference to this threat.[96]

Mattelart observed that '*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.*'[97]

DPI is at this juncture the core technology for Internet surveillance. As they can be used for a great variety of purposes, ranging from pure network management to content filtering, rerouting and blocking of websites as far as manipulation of websites and full users profiling, DPI technologies can be seen as some of the most powerful surveillance tools of late modernity. The high potential DPI holds for censorship, infringement and repression is obvious. (*Since D3.1 and D 3.2 elaborate excessively on cyber security and DPI technologies, there are only a few additional observations on contemporary European approaches on the issues of cybercrime to be added here.*)

In the beginning of 2013 EUROPOL launched its European Cybercrime Centre (EC^3), claiming on the website that '*in fact, about one million people worldwide fall victim to some form of cybercrime every day*' and furthermore that '*investigations into online fraud, online child abuse and other cybercrimes regularly involve hundreds of victims at a time*'[98]. Besides, placing 'child abuse' literally and prominently next to

---

93 Didier Bigo et al. 'Fighting Cyber crime and protecting privacy in the cloud', European Parliament (2012), http://www.europarl.europa.eu/studies.

94 Ibid.

95 Ibid. p. 10.

96 Florencio and Herley (2012), 'The cybercrime wave that wasn't' http://www.nytimes.com/2012/04/15/opinion/sunday/the-cybercrime-wave-that-wasnt.html?_r=0

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

98 EUROPOL Website (2013), Media invitation to the opening of the European Cyber Crime Centre (EC^3) at: https://www.europol.europa.eu/content/press/media-invitation-opening-european-cybercrime-centre-ec3-europol-1977
See also: main webpage of EUROPOL EC^3: https://www.europol.europa.eu/ec3

general online fraud, followed by claiming hundreds of victims at a time, is a rather interesting approach.

International European dataveillance collaborations to be initiated and pushed by EC³ – to a greater extent between law enforcement and industries – will include the following: '*EC³ will fuse information from open sources, private industry, police and academia. The new Centre will also serve as a knowledge base for national police in EU Member States pooling European cybercrime expertise and training efforts, and responding to queries from partners on specific technical and forensic issues. It will also reach out to industry and other important non-law enforcement players to put in practice public-private partnerships and develop general and more specialized threat assessments on the nature of cybercrime*.'[99]

ENISA published in 2013 the 'Threat Landscape Report'[100] 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, cyber criminals, hacktivists, corporations and also employees.[101] That demonstrates once more that almost everything and everyone is perceived as a potential threat to security – at least in cyberspace.

In contrast Brin[102] and others emphasize the heterogeneity, flexibility or even fragility of surveillance systems and argue that contemporary surveillance is not – like Bentham's Panopticon or Orwell's 1984 – a one-sided instrument of sovereigns, tycoons or national authorities used to control the masses. Surveillance can work both directions, which is bottom-up as well. Surveillance could even stabilize democracy. Fuchs marks the fact the Internet can help to watch the watchers and to raise public awareness.[103]

Social movements within transnational publics endeavour to influence national public spheres;[104] the resonance they are able to gain to a great extent depends on visibility. The Internet plays without doubt an important role in this process. Web-based movements like Avaaz[105] demonstrate indeed that online-based social movements can establish global information and activist chains on crucial social and environmental issues, thus putting pressure on governments and pushing towards the social and environmental good. (In the case of Avaaz, that is e.g. educational programmes for children in Pakistan, some protection of the Amazon rainforest in Brazil and the Coral Sea in Australia etc.[106])

---

99 EUROPOL Website (2013), Media invitation to the opening of the European Cyber Crime Centre (EC³) at: https://www.europol.europa.eu/content/press/media-invitation-opening-european-cybercrime-centre-ec3-europol-1977

100 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

101 ENISA; Ibid; 'Threat Landscape Report' p. 24ff, for download, on ENISA-website: ENISA Threat Landscape Published.pdf

102 David Brin(2004), 'Three cheers for the Surveillance Society!' http://www.salon.com/2004/08/04/mortal_gods/.

103 Christian Fuchs et al., (Ed.), *Internet and Surveillance–The Challenges of Web 2.0 and Social Media*. London: Routledge (2011), p. 306.
He is also providing examples for corporate watch organizations, e.g.: CorpWatch Reporting (http://www.corpwatch.org), Transnationale Ethical Rating (http://www.transnationale.org), The Corporate Watch Project (http://www.corporatewatch.org), Corporate Europe Observatory (http://www.corporateeurope.org)

104 Thomas Olesen, 'Transnational Publics: New Spaces of Social Movement Activism and the Problem of Global Long-Sightedness', *Current Sociology* 53, Nr. 3 (January 5, 2005).

105 AVAAZ: Website: http://www.avaaz.org/en/
Avaaz is in their own words '*the global web movement campaigning community bringing people-powered politics to decision-making worldwide*.' (ibid) The Avaaz 'movement' on the level of people being registered with their e-mail-address signing petitions consists of almost 17.5 million from all over the world. Besides petitions, Avaaz '*is funding media campaigns and direct actions, emailing, calling and lobbying governments, and organizing "offline" protests and events*.' Avaaz launched in 2007 with the idea of starting a democratic grassroots movement to organize citizens worldwide for social justice and is now campaigning in up to 15 languages worldwide.

106 Ibid.

Morozov, for instance, argues quite the opposite, providing evidence for the conclusion that the Internet is inhibiting rather than encouraging democracy.[107] (*See also the chapter 'Information control on the Internet'.*)

A tentative conclusion at this point would be that the rise of the World Wide Web can 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 (for increasing parts of the world's population, thus by a long term not for all), or as a curse, opening up sheer indefinite possibilities for violation of intellectual property rights, copy rights and privacy rights, furthermore accompanied by extremely dangerous cyber criminals and cyber terrorists. 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) did fail.[108]

3.5 Function creep

Technical systems can be put to many different uses and, as Kranzberg reminds us, technology is neither good nor bad nor is it neutral.[109] Technological systems like mobile phones, credit cards, GPS etc. are not explicitly designed as surveillance measures but can be used for surveillance purposes. It can be stated that function creep can never be ruled out as a possibility in any field of technology, and that consumer convenience orientated technologies are especially prone to function creep.

An extremely interesting contemporary example can be found in the field of smart grid technologies. On the one hand, smart grid technologies help by pushing towards a much better and more efficient use of finite energy resources, thus promoting sustainability; on the other, the implementation of smart grid technologies stands quite often in opposition to lessons learned from fields such as safety engineering and creates legal uncertainty for the end users.[110] Grid systems are vulnerable to outsmarting on a small scale and cascade failures on a larger scale, and moreover more vulnerable to cyber attacks than decentralized systems.[111] This vulnerability triggers the demand for specific – technological – security measures to protect the complex architecture of the smart grids. Such 'technology fix circles' will be criticized in the following chapter.

However, smart meter systems in particular are steadily finding their way into households all over the world and hence into 'trivial' but core parts of everyday life, and might possibly be perceived as normal in greater parts of Europe within the next decade,[112] although they as yet remain highly controversial.

For instance, in the Australian state of Victoria consumers were forced to accept the roll-out of smart meters in their households at the end of 2011. Although 10% of the households in the poll so far had

---

[107] Evgeny Morozov, *The net delusion: how not to liberate the world*. London: Allen Lane (2011).
Comp. also: Evgeny Morozov, 'You Can't Say That on the Internet', *The New York Times*, November 16 (2012), Opinion/Sunday Review, http://www.nytimes.com/2012/11/18/opinion/sunday/you-cant-say-that-on-the-internet.html.

[108] Arthur (2012), 'Internet remains unregulated after UN treaty blocked' http://www.guardian.co.uk/technology/2012/dec/14/telecoms-treaty-internet-unregulated

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

[110] Comp. S. Massoud Amin and B. F. Wollenberg, 'Toward a smart grid: power delivery for the 21st century', *Power and Energy Magazine, IEEE* 3, Nr. 5 (2005): pp. 34–41. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1507024.

[111] Comp. Gorman (2009), 'Electricity grid in U.S. penetrated by spies', *Wallstreet Journal* http://online.wsj.com/article/SB123914805204099085.html#

[112] Smart Grids European Technology Platform Website, missions and objectives for the implementation of smart grid in Europe: http://www.smartgrids.eu/

refused the installation of the devices in the first place, the government released an (cost) audit and presented a privacy impact assessment. Although the review revealed wrangling over legal liability, suspected restricted supply to appliances, non-transparent cost schemes and further issues, the government claimed to have no financial choice while the power companies reserved the right to cut people off the supply in 'extreme cases'. (At the end of 2013 when all of the 2.6 million homes and businesses are planned to be connected, the estimated net cost will be 319 Australian dollars – to the customers.)[113]

The debate about the pros and cons of these technologies is mainly down to exactly the dilemma touched on by Kranzberg above. On the one hand, smart meter technologies offer a great deal of potential, e.g. for cost and energy saving and thus for the environmental good in the long term. But on the other hand, they are also inherently prone to intransparency and can be misused for customer rip-offs. They also can be used for surveillance purposes, social sorting, discrimination and the like. What might be faced here is a somewhat slippery slope towards highly likely function creep (attempts). The availability of data from smart metering systems is opening up a number of new possibilities for data gathering and cross-system enforcement for companies, state agencies, law enforcement etc., and also the means of a general dataveillance of the whole population. As stated thoroughly in D3.1 and mentioned in the chapter 'Privacy by Design', a variety of PbD measures – on the organizational as well as on the technological level – can be applied comparatively easily to smart meter technologies, allowing for a relatively simple approach to protecting end users' data.

Yet, smart grid technologies raise a long list of concerns: power relation concerns over governmental control on all energy-using activities and the 'kill-switch' function; health concerns over emissions; social concerns over fair and/or equal availability to the end users; and last but not least concerns over privacy according to the usage of data by law enforcement and other agencies.

3.6 Technology investments and technology fix

Nuclear disasters like Chernobyl and Fukushima constitute some of the most threatening and frightening major events of technological failure in the history of mankind. The protection of critical infrastructures in the face of global terrorist threats is a relatively new challenge, emerging with the increasing complexity of information and communication technology-based control structures of critical infrastructures. Applying safety engineering measures to critical infrastructure, conducting hazard analysis and establishing reliability centred maintenance are to create fault-tolerant systems to enhance security in critical systems.

However, it is often technologies that are regarded as trivial to both consumers and businesses that can cause serious issues through relatively minor discrepancies in their functionality. Technological – or an inextricable mixture of technological and human – failures and malfunctions are also creating an alarming number and variety of serious incidents that can turn out to be not just inconvenient but also life threatening. The examples provided in this chapter offer some insight into the spectrum of events and the issue of implicit reliance on technology.

December 2012: When Apple moved to its iOS 6 software, the town of Mildura, Australia (population 30,000) got misplaced by about 70 kilometres on Apple maps. At least four individuals got lost in that area, which has poor mobile network coverage, little water and temperatures of up to 46 °C. Local police had to go on rescue missions.[114]

---

[113] Collier (2011), 'Tough talk on Victoria's smart meters' http://www.heraldsun.com.au/news/victoria/victorias-electricity-smart-meters-here-to-stay/story-fn7x8me2-1226222296707

[114] Arthur (2012), 'Apple redraws maps after Australian drivers led astray in the bush' http://www.guardian.co.uk/technology/2012/dec/10/apple-maps-life-threatening-australian-police

March 2009: The 'Phantom of Heilbronn', Germany, was one of the most bizarre European murder mysteries of recent decades. After 15 years of police investigations for a phantom leaving DNA traces in various unrelated (murder) crime scenes in Austria, France and Germany, all turned out to be a blunder: the DNA belonged to an employee of the company providing state police departments with the cotton swabs the DNA traces were recovered with.[115]

In this context, the general public's trust in the infallibility of DNA testing methods is another crucial issue that should be addressed. Also, popular culture does play an important role in creating everyday life 'knowledge' about technology: The need to use DNA testing in solving crime cases is sold to the lay public through highly popular global TV crime series such as CSI[116].

However, Frumkin et al. demonstrated in a groundbreaking study the possibility of counterfeiting human DNA: '*Standard molecular biology techniques* […] *enable anyone with basic equipment and know-how to produce practically unlimited amounts of in-vitro synthesized (artificial) DNA with any desired genetic profile.*'[117] Furthermore, they also found that *current forensic procedure fails to distinguish between* 'real' and faked DNA. Yet, another fundamental problem arises in addition to the possibility of deliberately counterfeiting DNA traces: once DNA databases reach a certain size, meeting the limits of standard sampling methods seems ineluctable: '*it is mathematically predicted an innocent person will be matched to a crime they did not commit.*'[118]

Not necessarily rooted in the fallibility of DNA testing as such, but rather in a mixed scenario of techno-centrism accompanied by human failure, there are a number of documented cases where innocent individuals were matched to crimes they did not commit.[119]

July 2012: The U.S. Justice Department announced a nationwide review of all cases handled by the FBI Laboratory's hair and fibres unit before 2000 […] to determine whether improper lab reports or testimony might have contributed to wrongful convictions. This is at least according to a minimum number of 21,000 cases. *'Thousands of criminal cases at the state and local level may have relied on exaggerated testimony or false forensic evidence to convict defendants of murder, rape and other felonies.*'[120]

Hair matches in particular are often contested. The 2012 review follows a series of scandals dating as far back as the 1970s. In 2001, more than 1,400 cases of Oklahoma City police crime lab supervisor Joyce Gilchrist had to be questioned once a review found that her claims on hair matching were '*beyond the acceptable limits of science*'. Another case is that of the Montana crime lab director Arnold Melnikoff, who was fired in 2004 over the questioning of more than 700 cases when reviewers called enormous scientific errors, mainly on the accuracy of hair matches dating back even to the 1970s.[121] The problem

---

[115] No author (2009), BBC 'DNA bungle haunts German police' http://news.bbc.co.uk/2/hi/europe/7966641.stm
Also, the popular American TV series *CSI* fictionalized these events in their 6th season episode, 'Dead Reckoning'.

[116] *CSI* held the record for the most successful TV crime series on a global basis. It had over 73 million viewers in 2009 and in 2012 it was stated to be the most watched TV series worldwide for the fifth time in total.
See here: http://tvbythenumbers.zap2it.com/2012/06/14/csi-crime-scene-investigation-is-the-most-watched-show-in-the-world-2/138212/

[117] D. Frumkin, A. Wasserstrom, A. Davidson and A. Grafit, 'Authentication of forensic DNA samples', *Forensic science international. Genetics* (2010), 4 (2), pp. 95–103.
http://www.ncbi.nlm.nih.gov/pubmed/20129467
Pinar Bilgin, 'Identity/Security', *The Routledge Handbook of New Security Studies* (2010), pp. 81–89.

[118] Porter (2009), 'The rising odds of DNA false matches'
http://www.guardian.co.uk/commentisfree/henryporter/2009/may/25/dna-database-false-positive

[119] Spencer (2012), 'FBI lab woes cast a growing shadow' http://www.independent.co.uk/news/world/americas/fbi-labs-woes-cast-a-growing-shadow-8430348.html

[120] ibid.

[121] See also: Spencer (2012), 'Review of FBI forensics does not extend to federally trained state, local examiners' http://articles.washingtonpost.com/2012-12-22/local/36016999_1_crime-lab-arnold-melnikoff-fbi

here is that proving one's innocence in the face of supposedly infallible high-tech evidence can be difficult for the layperson and the defence lawyer.

These examples demonstrate that the greater part of surveillance technologies in use are far from being 100% accurate and reliable, and, especially when combined with human error, are simply dangerous. Surveillance technologies presented by the industrial security complex as being 'the next ground-breaking' invention most often do not stand the test for practicality.

For instance, in the case of public CCTV combined with face recognition technology, even the UK Parliamentary Office of Science and Technology stated: '*In controlled conditions these systems can achieve accuracy of 96%, but covert face recognition is likely to be less effective. Obtaining clear facial images is difficult owing to factors such as lighting, movement and accessories such as hats or glasses that obscure the face. Chances of a false match increase with the size of the photograph database.*'[122]

Practical implementation of surveillance measures – whether technological or procedural – frequently cannot replicate the effectiveness in the field that was suggested by controlled laboratory pretesting or ring-fenced pilot schemes. Malfunctions, false matches and other issues are not uncommon and the ability to outsmart the systems cannot be excluded either.

Since false matches and other failures yield fundamental consequences for the mismatched individuals, techno-centrism has – at least from a social perspective – to be understood as a slippery slope. The complex of problems arising from these issues will be reasoned at greater length in the chapter 'Implications'. Rather than stepping up surveillance technology measures to cure frequent issues with a more-of-the-same approach, possibly causing further – more elaborate – problems, solutions found for instance in the field of safety engineering could be taken into account for potential adaptation. Moreover, the technological fix theorem has to be questioned in its ability to serve as a (key) narrative of late modernity.

3.7 Conclusion: Replacement discourse

The ambiguity of the term security (see the chapter 'Security, surveillance and privacy as terms and concepts'), accompanied by a broad spectrum of possible security threats – the more so in an era of global risks – facilitates political malpractice. '*Conventional accounts that take identity as pre-given cannot imagine a way out of the security dilemma, for they fail to capture the role politics plays in the (re)construction of those very identities*'[123] Because of the multi-layered nature of the definition(s) of security, it holds emotional weight for the general public; therefore it is easy to alter the direction of security discourse in order to manipulate the public response to conclusions, which might not necessarily be the result, were the situation subject to an objective analysis. Since the states' attempts to *secure national security* are flanked by an enormous increase of the national and international industrial security complex, ringled by the global players in the security sector and shadowed by lobbyist groups, the security discourse appears to be highly contested and used in strategic contexts. Loader and Walker state that security has become *the* political vernacular of our times.[124] Politicians and lobby groups but also the media ('crime sells') are distending possible threats, as highlighted in the chapter on 'Crime and terrorism'.

Whereas 'public opinion' is an important factor for stepping up security measures, another problematic aspect can be envisaged: '*Researchers and governmental organizations have not only used statistics to understand social phenomena but mainly to prove their points and use it as a tool in policy and for decisions in financial matters, like cutting back costs.* […] *Neither a systematic theory-driven (hypothetical–deductive)*

[122] UK Parliamentary Office of Science and Technology (2002), Post note from April 2002; to be found at: http://www.parliament.uk/post/nfr/pn175.pdf
[123] Pinar Bilgin, 'Identity/Security', *The Routledge Handbook of New Security Studies* (2010), p. 81–89.
[124] Ian Loader and Neil Walker, *Civilizing Security*. Cambridge: Cambridge University Press (2007), p. 9.

approach nor a systematic data-driven (inductive) approach has been used to develop the concept [of fear of crime in e.g. public opinion polls] *and its operationalisation*.'[125]

Taking the findings of this chapter into account, it can well be stated that there is evidence for security solutions not standing the test for effectiveness. 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'[126] are to be observed as well. 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'[127].

In other words, since the practice of government is becoming increasingly one of risk management[128] and risk management has become – especially under neo-conservative political ideologies – a growing industry[129], the public visibility of some action taken against this threat seems to be increasingly more important than an actual threat level. The international industrial–security complex[130] on the global scale is one of the fastest-growing industries. National authorities and a variety of other actors are spending money on ill-conceived surveillance technologies. These technologies do not primarily increase security, they increase the profits of an industry that is flourishing on high levels of public fears.

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*',[131] with a market value of between €26 billion and €36.5 billion.[132] Pointing to positive economic effects, i.e. creating employment, is a rhetorical move that is hard to question in political discourse. And since the security industry is promising to create new jobs, the proposed course of action in the near future seems obvious. The most recent security concern, fighting cybercrime activities, is seen as *the key for the EU Internet-based economy*, according to EU commissioner Malmström.[133]

---

125 Vanderveen, *Interpreting Fear, Crime, Risk, and Unsafety*. p. 105ff. (Note in brackets by Regina Berglez.)

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

127 Comp. also Richtel (2012), 'The mystery of the flying laptop' http://travel.nytimes.com/2012/04/08/travel/the-mystery-of-the-flying-laptop.html?pagewanted=1&src=dayp
Goldberg (2008), 'The things he carried'
http://www.theatlantic.com/magazine/archive/2008/11/the-things-he-carried/307057/

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

129 Pat O'Malley, *Crime and Risk*. London et al: SAGE (2010).
J. Donahue, N. Whittemore, and A. Heerman, *Ethical Issues of Data Surveillance*. Ethica Publishing.
http://www. ethicapublishing. com/ethical/3CH20. pdf),

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

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

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

133 Comp. EUROPOL-Website: https://www.europol.europa.eu/content/press/media-invitation-opening-european-cybercrime-centre-ec3-europol-1977

4. Implications

4.1 Privacy

Citizenship in late modernity is marked by a host of identity documents. Our everyday lives have turned into a gigantic paper trail[134] – or increasingly into electronic data traces. A few decades ago identity documents consisted of printed papers, kept in folders on shelves, and information exchange among different organisations required an active effort (e.g. sending letters with photocopies).

It is a truism that this has changed fundamentally. Whereas comprehensive biometric databases of whole populations might well be achieved in the near future, allowing for ubiquitous identification of the individual, data protection and privacy protection are becoming more important and at the same time increasingly difficult. '*The notion of data privacy, while it has held a consistent core for about 40 years, is not static. New principles continue to emerge and become absorbed in new or amended data privacy legislation, the most notable recent example being 'data breach notification'. Other emergent principles include data tracking restrictions, the anonymous transactions right, and the 'right to be forgotten', though they can usually be seen as specific implications of already existing general principles.*'[135]

The concept of a (off-line) private sphere, defined in spatial terms of the private home (reaching back to the Greek notion of *oikos*), is of no avail in the age of the 'Homo electronicus', and hence a redefinition of privacy is becoming inevitable. The boundaries between public and private domains – and along with it the 'old' concept of privacy – seem blurred already (see also D3.2.). It cannot be neglected that, concerning personal privacy, the rise of social networks such as Facebook is steadily changing the perceptions of privacy for greater parts of the population and especially the younger generations. Advanced positions held within the 'digital natives' web community' claim that the very basic idea of private sphere is nothing more than an outdated concept from the last century, and thus even '*our children may find the word "anonymous" impossibly quaint, perhaps even incomprehensible*,' [136] which is not only perceived as negative.[137] (This view will be challenged in the chapter 'Social profiling'.)

But it is also the potential future consequences of present behaviour where 'privacy problems often lie'.[138] Since awareness is the basis of and the key to one's privacy (enhancing) behaviour – in the non-virtual world as well as in cyberspace – knowledge and awareness of one's behavioural patterns and potential threats to privacy have to be gained by the individual in the first place. This requires reconnaissance as well as educational training. To clarify, this is by no means arguing for putting top-down pressure on individuals to get back offline or back onto the trees, but rather to push for an informed open debate. At the end, concerning one's privacy it is also one's optional attitude towards privacy that matters.[139]

---

[134] J. Donahue, N. Whittemore, and A. Heerman, *Ethical Issues of Data Surveillance*. Ethica Publishing (2013), http://www.ethicapublishing.com/ethical/3CH20.pdf.

[135] Graham Greenleaf, 'Global data privacy in a networked world', p.3. For publication in: *Research Handbook on Governance of the Internet*. Cheltenham: Edward Elgar (2011),

[136] David Brin (2004), 'Three cheers for the Surveillance Society!' http://www.salon.com/2004/08/04/mortal_gods/;

[137] Ibid.
and also: Christian Heller, *Post Privacy: prima leben ohne Privatsphäre*. München: Beck (2011).

[138] Mark S. Ackerman and Scott D. Mainwaring, 'Privacy issues and human-computer-interaction' (2005) p. 383.

[139] Comp. also: M. Farinosi, 'Deconstructing Bentham's Panopticon: The New Metaphors of Surveillance in the Web 2.0 Environment', *tripleC-Cognition, Communication, Co-operation* 9, Nr. 1 (2011): pp. 62–76, http://www.triplec.at/index.php/tripleC/article/view/249

As Allmer states, critical privacy movements do need to develop what he calls counter-hegemonic power for and to raise awareness of privacy threats.[140] According to Lyon, awareness should furthermore be raised by professional groups, especially those practitioners directly concerned with information management.[141] Bennett also notes that privacy advocacy can be expressed in many ways, whether that be traditional activism, scholarly research, consultancy, IT development, journalism or even art.[142]

Three main arguments can be envisaged for our perspective concerning privacy in the context of this task. We stress that (1) the consequences of present behavior might potentially only arise in the future, but it is still today's attitude towards privacy that matters; (2) privacy is less about the content but rather about the functional relevance; (3) citizens need to be better informed about (novel) technologies and the impact these technologies have on rights such as the right to privacy. These three points do indicate once more the need for an informed public debate, changes in the general educational systems and various approaches of Public Understanding of Science (PUS).

4.2 Information control on the Internet

As Evgeny Morozov, castigator of the perception of the web as a democratic freedom- of-speech space, points out sharply: '*Silicon Valley imagines itself as the un-Chick-fil-A. But its hyper-tolerant facade often masks deeply conservative, outdated norms that digital culture discreetly imposes on billions of technology users worldwide.* […] *Silicon Valley does not engage in direct censorship. What it does, though, is present ideas and terms that have gained public acceptance as something to be ashamed of. Silicon Valley doesn't just reflect social norms – it actively shapes them in ways that are, for the most part, imperceptible.*'[143]

There are two key issues here, one of which is that of the effects according to the zero-tolerance nature of algorithms not 'only' on matters of dataveillance, cross-system enforcement technologies and alike but also relating to all sorts of content on the worldwide web. (Copyright) warning interruptions in live-streamed events owing to copyright protection means are one example of possible interferences.
A recent prominent example of a malfunction of copyright protection enforcement technology occurred in the live stream from the Hugo Awards in September 2012, where the acceptance speech of author Neil Gaiman was cut off with some cryptic copyright warning.[144] Since Neil Gaiman is not only a popular author but also a popular and incredibly active 'netizen' and blogger, with additionally almost 1.8 million followers on Twitter and over 500,000 fans reading his Facebook updates, this was a big deal in the 'net world'.
While this incident illustrates the power of algorithms, it was nevertheless only annoying for fans and rather harmless in the big picture.

The second and crucial problem is that of the many opportunities for exertion of influence and censorship, concerning not only but especially the main global players Google, Facebook etc. Morozov's critical view of contemporary communication strategies in the current web environment is indeed accompanied by numerous examples of what can basically be termed as (indirect) censorship or exertion of influence. This is working both ways – from within the web service providers themselves and

[140] T. Allmer, 'A critical contribution to theoretical foundations of privacy studies', *Journal of Information, Communication and Ethics in Society* 9, Nr. 2 (2011): pp. 83–101 http://www.emeraldinsight.com/journals.htm?articleid=1931176&show=abstract

[141] Lyon, *Surveillance As Social Sorting*; David Lyon, *Surveillance Studies: An Overview*. Polity (2007).

[142] Bennett, *The privacy advocates*. p. 94.

[143] Morozov (2012), 'You can't say that on the internet' http://www.nytimes.com/2012/11/18/opinion/sunday/you-cant-say-that-on-the-internet.html

[144] Newitz (2012), 'How copyright enforcement robots killed the Hugo Award' http://io9.com/5940036/how-copyright-enforcement-robots-killed-the-hugo-awards
also: Knight (2012), 'Copyright enforcement boots seek and destroy Hugo Award' http://www.techdirt.com/articles/20120903/18505820259/copyright-enforcement-bots-seek-destroy-hugo-awards.shtml

through pressure placed on them from the outside by corporations concerned about copyright infringements etc.

In 2012 Google, for instance, was asked to remove over 51 million links to infringing web pages, mostly owing to copyright violations. Currently, Google has to process half a million infringing links per day, while major record labels and other global companies want Google to increase its anti-piracy efforts intensively.[145] Even Google itself is raising concerns about these dramatic figures. As Google's Legal Director Fred Von Lohmann stated in 2012, '*As policymakers evaluate how effective copyright laws are, they need to consider the collateral impact copyright regulation has on the flow of information online.* […] *By making our copyright data available in detail, we hope policymakers will be able to see whether or not laws are serving their intended purpose and being enforced in the public interest*.'[146]

Arbitrarily, Google itself does play an important role in shaping perception.

How powerful Google rankings are can be illustrated with the example of a German online company, 'Holzspielzeug-Discount' (Wooden Toys), which was victim to cyber fraud at the end of 2011. The company was being blackmailed but refused to pay and was soon afterwards facing a massive decrease in business, up to 75%. Expert testimony on search engine optimization (SEO) proved that the company's webpage showed a massive back linking to sites in Eastern Europe, Asia etc., creating cross-over bad links with negative spam wordings such as Viagra, sex, porno, which seemed to have had serious impact on the Google ranking.[147] The process of removing these linkages is intricate since Google doesn't have a serial interface for those matters yet.[148]

Besides the power of Google rankings, functions like Google's auto completion play an important role. The blacklisting of such words as 'bisexual' on Google's auto completion is just one example of the many possibilities to influence the kind of results offered in the first place – which translates into visibility and therefore perception, knowledge and power.

This is particularly interesting, since what is perceived as acceptable or inacceptable is often rather highly non-transparent and lacking balance (even within the same 'standards' applying for a particular country). Once Facebook pages of reputable online magazines are being blocked within 24 hours for violating e.g. sex standards through rather harmless cartoons[149] or even pictures of breastfeeding[150] are taken down while pages on Facebook which are clearly to be seen as appealing for sexual harassment (or racist content) are having to be reported by a large number of Facebook users over a period of weeks or longer (or even petitions started, for that matter)[151] until eventually action is taken by Facebook, solid standard policies cannot be spoken of at all. As long as (sexual) hate speech pages on Facebook like

---

145 Ernesto (2012), 'Google removed 50 million "pirate" search results this year' http://torrentfreak.com/google-removed-50-million-pirate-search-results-this-year-121228/

146 Ernesto (2012), 'Hollywood and Google square off over pirate search results' http://torrentfreak.com/hollywood-and-google-square-off-over-pirate-search-results-121214/

147 Klaß (2012), 'Wie ein Erpresser einem Online-Shop schadete' http://www.golem.de/news/google-ranking-wie-ein-erpresser-einem-onlineshop-schadete-1202-89548.html

148 Ibid.

149 Wells (2012), 'The New Yorker magazine's Facebook page temporarily shut down for showing too much nipple' http://www.nydailynews.com/news/national/new-yorker-magazine-Facebook-page-temporarily-shut-showing-nipple-article-1.1157053
Mankov (2012), 'Nipplegate' http://www.newyorker.com/online/blogs/cartoonists/2012/09/nipplegate-why-the-new-yorker-cartoon-department-is-about-to-be-banned-from-Facebook.html

150 Protalinski (2012), 'Facebook clarifies breastfeeding photo policy' http://www.zdnet.com/blog/Facebook/Facebook-clarifies-breastfeeding-photo-policy/8791

151 No author (2012), 'Facebook removes racist page in Australia' http://www.bbc.co.uk/news/world-asia-19191595
Comp. also Petition (2011): 'Petition Facebook to remove material that promotes rape culture': http://www.gopetition.com/petitions/petition-Facebook-to-remove-material-that-promotes-rape.html

'*teach sluts to run faster to avoid becoming victims*'[152] are simply termed as controversial humour and stay online,[153] accessible to all users hitting the respective national age limit for such content, these standards are not sufficient.

Serious incidents with greater impact on the freedom of speech are also to be observed and seemingly with increasing frequency.

One showcase example is that of the WikiLeaks/Amazon incident at the end of 2010. Amazon.com – as the host of the cloud computing services of WikiLeaks – chucked the main WikiLeaks website and also some subsites devoted to U.S. diplomatic documents soon after the site hosted leaked U.S. embassy cables. Amazon announced it had been contacted by the Chairman of U.S. Homeland Security.[154] Also, a few days later, the WikiLeaks domain name was withdrawn as well. While the provider claimed that cyber attacks on WikiLeaks endangered other customers' services, the WikiLeaks lawyer stated that '*pressure appears to have been applied to close the WikiLeaks domain name*', and also reputable newspapers such as *The Guardian* were quoting that U.S. companies '*have also come under intense political pressure to remove any connection to, or support for, WikiLeaks*.'[155]

Fundamentally, partly invisible and highly problematic attempts towards influence and censorship are working in the contested world of cyberspace and more so underneath web-algorithms (as well as underneath e.g. behavioural pattern recognition systems). Algorithms have the power to determine cultural acceptability of standards on the web, and current developments do show some resistance against liberal opinions or even a push towards conservative mainstream attitude estimating social norms and values.[156]

4.3 Smart surveillance and behavioural pattern recognition

As demonstrated in D3.2, in the chapter 'Smart CCTV surveillance', there is currently neither a legal definition to distinguish smart surveillance from any other form of surveillance, nor a consistent technical terminology available to describe what makes a surveillance system 'smart'. Definitions of smart surveillance on the technical level vary distinctively and range from terminologies like 'automated respectively automatic video surveillance' to surveillance systems being *'capable to extract specific information* […] *in order to generate high-level event descriptions that can ultimately be used to make automated or semi-automated decisions*'.[157] However, it can clearly be asserted that the rapid increase of smart surveillance technologies is pushing towards mass-surveillance measures.

Besides the critique on the potential negative impact of mass surveillance on society, there are also counter-arguments to be found. In theory it could be presumed that mass surveillance measures can yield the quite opposite effect and enhance security without interfering with privacy. For instance,

---

[152] Facebook Page to be found at: http://www.facebook.com/the.rape.alleyway

[153] This is particularly interesting since there are even different standards applied by Facebook within the very same countries according the options given for reporting Facebook pages. Sometimes the list for reporting pages contains options as 'hate speech', 'violence' and 'sexual explicit', sometimes it doesn't. In the case of the page mentioned above '*teach sluts to run faster …'*, there are no such options. The reporting list is limited to options such as 'I don't like it', 'I or someone I know feels molested', 'it doesn't fit on Facebook', 'it is spam', 'it is wrongly categorised'. (Status checked with a German Facebook account in January 2013.)

[154] MacAskill (2010), 'WikiLeaks website pulled by Amazon after US political pressure' http://www.guardian.co.uk/media/2010/dec/01/wikileaks-website-cables-servers-amazon

[155] Arthur and Halliday (2010), 'WikiLeaks fights to stay online after US company withdraws domain name' http://www.guardian.co.uk/media/blog/2010/dec/03/wikileaks-knocked-off-net-dns-everydns
O. 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.

[156] Morozov, *The net delusion*.

[157] Bellanova, Rocco, and Michael Friedewald (eds.), Deliverable 1.1: Smart Surveillance – State of the Art, FP7 SAPIENT Project, Brussels (2011) http://www.sapientproject.eu/

automated (video-) surveillance without any (stored) recordings and even without any real-time watching in the first place could be assessed as more proportionate for a balance between privacy and security than conventional forms of CCTV. If any further action to be taken (like watching, recording, storage, processing of data) was only started once a problematic situation or an incident occurred (comp. D3.1.), the right to privacy of anyone else would remain unaffected.

From a social perspective, lots of assumptions about human perception are made and remain unquestioned once it is spoken of 'incidents' and the like. Simon Davies pointed out on the rise of smart CCTV systems*: 'For one thing, somebody has to decide what "normal behaviour" is, and that somebody is likely to represent a narrow, authoritarian viewpoint. The system reflects the views of those using it* […] *Anyone who does act out of the ordinary will be more likely than now to be approached by security guards, which will put pressure on them to avoid standing out.* […] *The push to conformity will be extraordinary.*'[158]

Behavioural pattern recognition for instance aims at eliminating every potential threat in advance; that is pointing towards a pre-emptive society where everyone has at first to be considered a potential threat. A steady shift from 'post-crime' to 'pre-crime' situation management can be observed for at least two decades; van Brakel and de Hert even talk about a shift towards a pre-crime *society* with proactive and predictive characteristics.[159]

Also, how to teach the idea of 'fair use' to an algorithm remains an unsolved question for the time being since algorithms come naturally with the inherent assumption of zero-tolerance.[160] Since knowledge creates power and vice versa[161], mass surveillance per definition remains an asymmetric instrument in the hands of those in charge and in power of the data – whether that is governments or the industrial complex – over the 'masses' of ordinary citizens.

4.4 Social profiling

4.4.1 Dataveillance

Mass dataveillance aims at (specific) groups of people while personal dataveillance aims at pinning down the particular individual for profiling and targeting reasons. Profiling in terms of dataveillance becomes problematic once assumptions or rather chains of assumption are being created rooting in and based on categories such as religion, race or social class.

Personal data surveillance used for simple front-end verification (e.g. a bank searching for inconsistencies in past payment records of someone applying for a credit card) is common practice[162] and can possibly be perceived as widely socially accepted despite privacy issues involved in such a procedure. But contemporary technological advances in cross-system enforcement and the like opened up a whole range of privacy-threatening options to cross-check, compare, classify and scrutinize (actions and characteristics of) individuals. Clarke defines cross-system enforcement as the relationship of one

158 (No author), BBC/*New Scientist* feature, 'Warning! Strange behaviour' http://architecture.mit.edu/house_n/web/resources/articles/lifeinthefuture/New%20Scientist%20Feature%20Warning!%20Strange%20behaviour.htm

159 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.

160 Morozov, 'You Can't Say That on the Internet'.

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

162 Donahue, Whittemore and Heerman, *Ethical Issues of Data Surveillance*.

individual to one organization depending on the relationship of that individual to another organisation.[163]

Once students cannot re-enrol for their next term without having returned their outstanding books to the university's library,; or once one cannot get a marriage licence while having outstanding parking tickets[164], cross-system mechanisms show their impact on everyday life.

Additionally, surveillance practices like data mining are aiming at social sorting by classifying information about individuals available in different databases. The bulk of this information emerges from the myriad of data traces left in electronically mediated exchanges of consumer society. The key question here is: in what category or group should you properly be placed?

First, the possibility of someone being counterfeit, accidentally mismatched or blacklisted cannot be ruled out. '*Although no official statistics exist on false positives, the existence of "collateral damages" related to blacklists and no-fly lists is acknowledged at the EU and UN level.*'[165] This might become an even larger problem if a blacklisted person doesn't know about the underlying mechanisms and therefore has fewer options to protest against it. After all, companies often use the most cost-effective insecure and inaccurate solutions.[166] Algorithms also have no 'fair use' mechanism, so that incorrect categorization of a person, based on standardized routine procedures, is not uncommon.[167]

Even if the data is 'correct' and the cross-system enforcement is functioning properly, and data-mining exercises are carried out within the legal framework, the questions remain about what impact this technology has on an individual and what power it exerts on society.

4.4.2 Cyberveillance

Since for instance U.S. defence companies are screening social network sites on behalf of the U.S. Department for Homeland Security (DHS)[168], it seems obvious that through cross-system enforcement individual profiles of the users are being created. Moreover, social networks like Facebook and micro-blogging services like Twitter are under automated DHS surveillance and are routinely screened for keywords. The list of approximately 500 keywords (which was made public in a DHS report)[169] contains words such as *security*, *response*, *cloud*, *wave*, *resistant*, *sick*, *power*, *smart*, *pirates*, *recruitment*, *home grown*, *emergency*, *ice*, *storm*, *snow*, *warning*, *aid*, *china*, *airport*, *subway and communication*, which makes it obviously almost impossible for users of any of these social network services to stay off the radar of these screening and filtering processes.

Additionally, cases like that of the Irish citizen Leigh van Bryan and his girlfriend (who were barred from entering the U.S. because of his tweet '*I go and destroy America*')[170]; or that of Paul Chambers in the UK

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

163 Clarke, Roger (no date), his own website: http://www.rogerclarke.com/DV/

164 Donahue, Whittemore and Heerman, *Ethical Issues of Data Surveillance*.

165 Comp. IRISS-project, (2012), DEL 1, 'Surveillance, fighting crime and violence report' p. 273. http://irissproject.eu/?page_id=9

166 Donahue, Whittemore, and Heerman, *Ethical Issues of Data Surveillance*.

167 Lyon, *Surveillance As Social Sorting*.

168 Krick (2012), 'Fluggastdatenabkommen mit den USA: Europäischer Offenbarungseid' http://www.spiegel.de/reise/aktuell/fluggastdaten-pnr-der-eu-abkommen-mit-der-usa-in-der-kritik-a-828814.html

169 US Department of Homeland Security Analyst's Desktop Binder' (2011), Document for download Compare list of keywords p. 20ff http://epic.org/foia/epic-v-dhs-media-monitoring/Analyst-Desktop-Binder-REDACTED.pdf

170 Nelson (2012), 'Leigh van Brian and Emily Bunting banned from entering U.S. after Twitter joke about "destroying America"' http://www.huffingtonpost.co.uk/2012/01/30/leigh-van-bryan-and-emily-bunting-banned-from-entering-us-after-Twitter-joke-about-destroying-america_n_1241104.html

(who was arrested and subsequently charged and convicted of causing a menace under the UK Communications Act a week after his tweet '*Crap! Robin Hood airport is closed* […] *I'm blowing the airport sky high*')[171]; or that of the arrest taking place under the UK Malicious Communication Act in Aylesham, UK (for posting a picture of a poppy burning on Twitter)[172], show how impetuous and overwrought these security surveillance scenarios have got already, and what serious implications spontaneous demonstrations of anger, 'bad jokes' or even inconclusive formulations can have for the individual.

D3.1 states in the chapter Social network surveillance: '*However, the current state of the art in classical social network surveillance combines the techniques of* […] *DPI network monitoring with new technologies of data mining. In doing so, filtering algorithms tuned in for atypical behavioural patterns and the automated removal of inappropriate and illegal content. But the effectiveness regarding security enhancement in social networks remains doubtful since the predefinition of typical user behaviour does not always lead to satisfying results*.'[173]

Moreover, attempts are already going far beyond a 'simple' screening of tweets and the like. Not only are psychologists increasingly examining social media as a rich and easily accessible source of all possible sorts of data, recent pilot studies on e.g. personal profiling of Twitter-users for the purpose of character (pattern) recognition. On the one hand, some scientists claim that such algorithmic models could be used for comparing character traits between countries, but on the other hand, security authorities also hope to identify psychopaths, using algorithmic models. Since Cornell University researchers[174] conducted a word-pattern analysis of the writings of psychopaths, claiming to have found similarities and patterns, this method is hoped to be adopted for an analysis of the writings of individuals in social and especially micro blogging networks to be able to filter out the 'dangerous ones'.[175]

This points also to very interesting future scenario on the evolvement of privacy rights and/or challenges for the legal systems, which can hardly yet be fully envisaged. Even if the data is on the basis of consent of a particular individual lawfully accessible to everyone, character recognition carried out on the single individual and 'results' possibly made public does go beyond 'customary' kinds of social media analytics or customer targeting.

Since dataveillance and related industries play an important role in the global economy, the supply of services in this sector is getting increasingly pushed and contested. Global corporations such as IBM offer highly targeted and specialized customized predictive analysis services to companies and other stakeholders. IBM, for instance, supplies the complete range of dataveillance practices: '*advanced analytics, data mining, text mining, social media analytics and statistical analysis including regression analysis, cluster analysis and correlation analysis, data collection and online survey research, data modelling and predictive modelling*.'[176]

---

171 Booth (2012), 'Judgement reserved in Twitter airport threat appeal'
http://www.guardian.co.uk/law/2012/feb/08/judgment-reserved-Twitter-threat-appeal?intcmp=239

172 Fogg (2012), 'Arrested for poppy burning? Beware the tyranny of decency'
http://www.guardian.co.uk/commentisfree/2012/nov/12/arrested-poppy-burning-beware-tyranny-decency?INTCMP=SRCH

173 Eva Schlehahn (2013), SurPRISE, D3.1.
And also: Menn (2012), 'Social networks scan for sexual predators, with uneven results'
http://www.reuters.com/article/2012/07/12/us-usa-internet-predators-idUSBRE86B05G20120712

174 Comp. Hancock, Woodword and Porter (2011), Abstract of 'Hungry like the wolf: A word-pattern analysis of the language of psychopaths'
http://onlinelibrary.wiley.com/doi/10.1111/j.2044-8333.2011.02025.x/abstract

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

176 IBM-Website on Predictive Analysis (2013),
http://www-142.ibm.com/software/products/us/en/category/SWQ50

Haggerty and Ericson remind us also that democracy is not an operative principle of corporations.[177] It should not be ignored that '*with more netizens flaunting their actions and thoughts in the open, social media has become a mainstay in police work*'[178] and often helps to uncover and identify criminals. It has been recognized that '*Facebook-posting crooks are making life much easier for cops*'[179] since '*you have guys who are bragging about their crimes online.*'[180] What might – in such cases – be perceived as straightforward lawful cyber investigation thus becomes blurry on the matters of access to individual accounts and the course of further investigations and the 'leaking out' of information.

In the case of the Boston Craigslist Killer in 2009, the lawfully executed Facebook subpoena of the suspect (and convicted killer) was – besides other sensitive documents – made widely public by the Boston Police Department as part of the case file, *including the full names of all of his Facebook friends plus their Facebook IDs* and more information on these unrelated third parties.[181]

How similar incidents can be prevented in the future remains an open question yet. As intelligible and crucial as it is for law enforcement to investigate such serious violent felonies and murders by accessing all information available and taking all action necessary, there is obviously a need for social-media policy for law enforcement and furthermore for sound legal protection of these unrelated third parties and their core privacy rights.

4.4.3 Social sorting

Once surveillance practices are combined with risk analysis – carried out in the name of (national) security – the sorting of whole populations into groups and clusters seems inevitable. '*Risk analysis treats the "at-risk" human being as a passive agent in the path of potentially disastrous events. In an effort to produce policy-relevant assessments, human populations are often classified into groups.*'[182] '*One's value or risk is assigned in advance based on statistical probabilities.*'[183] Tendencies pointing towards techno-centrism are to be observed, and discriminatory mechanisms following on as main or side effects might seem therefore somewhat admissible and unchallenged.

Individuals get increasingly confronted with individual advantages or disadvantages based on their personal profiling, i.e. being classified as wealthy or poor, middle-class or underclass, healthy or unhealthy etc. This might lead to social exclusion, since individuals do experience serious discrimination based on such profiling.[184] Thus, since we are not living in a perfect world of freedom, equality and justice, one most crucial reasoning for perpetuating (some) of our personal privacy should be kept in

---

177 Ericson and Haggerty, *The New Politics of Surveillance And Visibility*.

178 Yu (2012), 'Facebook's role in police investigations is growing' http://www.policeone.com/investigations/articles/5270796-Facebooks-role-in-police-investigations-is-growing/

179 Comp. exemplarily: No author: The Week editorial (2012); 'Suspected criminals who got themselves caught via Facebook' http://theweek.com/article/index/227257/7-suspected-criminals-who-got-themselves-caught-via-facebook

180 Yu (2012), 'Facebook's role in police investigations is growing' http://www.policeone.com/investigations/articles/5270796-Facebooks-role-in-police-investigations-is-growing/

181 No author (2012), The Phoenix Phlog: 'When the cops subpoena your Facebook information, here's what Facebook sends the cops' Comprehensive documentation: http://blog.thephoenix.com/blogs/phlog/archive/2012/04/06/when-police-subpoena-your-facebook-information-heres-what-facebook-sends-cops.aspx
Comp. also: No author, Phoenix (2012), 'The Craigslist killer files ' http://thephoenix.com/Boston/news/136761-slideshow-the-craiglist-killer-files/?page=8#TOPCONTENT

182 S. Jasanoff, 'Technologies of humility: citizen participation in governing science', *Minerva* 41, Nr. 3 (2003): 223–244, p. 241f http://www.springerlink.com/index/qv3vj6548kn55h25.pdf.

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

184 Comp. also: O. 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.

mind, as Baghai reminds us vividly: '*The contention here is that privacy conflicts arise when an event in one social system becomes relevant, arguably without justification, to selection of communication in another system, e.g. when love affairs become thematic in evaluating professional competence; health conditions become relevant to securing a bank loan; or sexual orientations become relevant to employment. The public or private nature of communication is not determined by its content, i.e. whether it involves secrets, embarrassing or confidential information, or merely trivial daily transactions, rather, by its functional relevance to the social system in question. Thus, if the love affair involves one's subordinate, the health condition undermines one's ability to be party to a contract, and the employer happens to be the Catholic Church, the system reference and functional relevance of communication change and so do the legal contours of privacy.*'[185] This matter of fact can yet be seen as one of the core problems of personal profiling and cross-enforcement technologies.

For instance Amoore and De Goede investigate how dataveillance promotes a culture of suspicion; and how risk classification designed to trace terrorist financing tends to focus on e.g. migrants, students or the unemployed, promoting financial exclusion of certain groups, criminalizing whole sectors of society and influencing individuals' ability to lead normal lives.[186] If automated sorting of customers by their postal code into the group 'marginalised neighbourhood' is the basis of consumption detriment (such as denying credit cards or special services), it can be spoken of discrimination on the basis of consumer social sorting. The next steps are, for instance, forcing the unemployed to stop smoking[187] or implementing pedometer measuring for the sake of their health and for their own good – as it was put – as is currently being pilot tested in Germany's state of Brandenburg.[188]

A recent example of discrimination on the basis of the grouping of people into dangerous classes is the cancellation of Iranian students' bank accounts in Germany at the end of 2012. '*Over the course of one week, several hundred Iranian students in Germany have reported that their German bank accounts were terminated; the only explanation for the closings appears to be that Iranians are a risk for German banks due to "Iran's* diplomatic relationship with the United States*."" According to Omid Nouripour, a member of the German parliament, German banks do not want the U.S. to 'hold them in contempt for doing business with Iranians.*'[189] Human Rights organizations got actively involved, a petition was started, etc. Investigations and exploratory talks among the various stakeholders are ongoing.[190]

'*Moreover, practices of profiling and social categorization can also result in "rational discrimination" that hides stereotypes and categories that would be declared illegal in other settings, but that attract less attention when these assumptions are embedded in algorithms.*'[191]

A growing number of studies highlight that the automated sorting by categories of personal data can reproduce marginalizing effects and negative discrimination.[192]

---

185 Katayoun Baghai, 'Privacy as a Human Right: A Sociological Theory', *Sociology* 46, nr. 5 (October 1), (2012): 951–965, p. 956.

186 Louise Amoore and Marieke Goede, 'Governance, risk and dataveillance in the war on terror', *Crime, Law and Social Change* 43, Nr. 2–3 (April 2005): pp. 149–173

187 HarzIV Nachrichten, Website (2012), 'Jobcenter zwingt zur Rauchentwöhnung' http://www.gegen-hartz.de/nachrichtenueberhartziv/hartz-iv-jobcenter-zwingt-zur-rauchentwoehnung-9001219.php

188 No author (2012), der Freitag 'Schritte zählen für das Jobcenter' http://www.freitag.de/autoren/gebe/schritte-zaehlen-fuer-das-jobcenter

189 No author, Blog (2012), '100 students' bank accounts close because their owners have the "wrong ethnicity"' http://armedwithknowledge.blogspot.co.at/2012_12_01_archive.html

190 Flüchtlingshilfe Iran e.V: Website: Collected Information about the case: 'Zwischenstand 11. Januar: 2013' http://fluechtlingshilfeiranev2010.wordpress.com/2013/01/11/in-sachen-bankkonto-fur-iraner-zwischenbericht-stand-11-01-2012/

191 IRISS-project (2012), DEL 1, 'Surveillance, fighting crime and violence report', p. 276, citing Solove, http://irissproject.eu/?page_id=9

4.5 Regulation and normalization

4.5.1 Public space

The impact (smart) CCTV surveillance in public space has on citizens' ordinary everyday life is crucial as well. Frehsee reminds us that those righteous citizens, who would claim to have nothing to hide, could quickly become targeted and punished for just minor and/or even accidental 'misbehaviour'.[193] As European states become more and more judgemental and regulatory on what used to be 'normal' or leastwise accepted behaviour some years ago, everyday-life actions become issues within new regulatory frameworks. Cleaning a car outside the house or burning garden rubbish in the backyard? Being a smoker and throwing the butt on the street? Riding on the tube with a pet dog without a muzzle? Sitting in the park, enjoying a summer evening, drinking a beer? In a (growing) number of European countries, these actions are considered as breaking local ordinances and thus can be punished with administrative fines.

To stretch the leastwise example a bit further: Once a person can be penalized for the public consumption of alcohol on a park bench, while a few meters away people are consuming alcohol in the outdoor facilities of a bar unchallenged, it is apposite to talk about structural discrimination on the basis of a consumer society. (Smart) CCTV surveillance facilitates this discrimination. Arguments by local authorities on the necessity of surveillance measures like CCTV to stop incidents and criminal acts are then also – and arguably in some cases mainly – directed towards all sorts of 'inappropriate' behaviour. '*Surveillance is never value-neutral. Surveillance is an observation, and information collection, mechanism, which can be seen as an extension of an apparatus of directed control from which it cannot be separated. The state's role ceases to be neutral adjudicator and infrastructure provider, but becomes increasingly judgemental – imposing its own normative values through a feedback of surveillance and action.*'[194] Those not acting within the boundaries of a capitalist–consumerist approach to everyday life and consumption are not only the lesser appreciated in a consumer society, it becomes furthermore possible to turn them into delinquents while an underlying neoliberal approach is partly hiding behind security discourses or respectively securitization.

The enforcement of a greater number of such new regulations would be unequally more difficult if it wasn't for the implementation of elaborate technologies to support and push these processes. Developments aiming at the regulation of all sorts of individual behaviours in public space are already becoming ubiquitous in European countries.

4.5.2 Policing

One could argue that the legislative systems in European countries are already well prepared to deal with imminent (terrorist) danger. For instance, Germany covers pre-emptive means through the controversial §129a StGB (=Criminal Code) 'Bildung krimineller Vereinigungen' (=Anti-terrorism-law)[195], which is supposed to be applied when significant and considerable danger is to be expected in the course of terrorist activities, and in the codes of criminal procedure (StPO) through 'Gefahr im Verzug (GiV)' (= Exigent circumstances). Once the basic premise of GiV is emphasized, a large number of lawful investigative tools are at the hand of police and law enforcement agencies.

---

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

[193] Detlev Frehsee, 'Zur Abweichung der Angepassten', *Kriminologisches Journal 23* (1991): pp. 25–45.

[194] IRISS-project (2012), DEL 1, 'Surveillance, fighting crime and violence report', p. 267. http://irissproject.eu/?page_id=9

[195] Juristischer Informationsdienst Online: Strafgesetzbuch/Germany: '§129a STGB'; http://dejure.org/gesetze/StGB/129.html

A prominent case is that of a German sociologist who was imprisoned in 2007 under the premises of §129a StGB. The commonly so-called terrorist paragraph §129a allows for many measures of targeted surveillance.[196] The arrest had followed years of inconclusive all-over surveillance including data mining, dataveillance, CCTV, tracking and (electronic) eavesdropping and later also DNA testing. The arrest, however, took place primarily on the basis of the 'evidence' that his scientific writing and also his extensive usage of the term 'gentrification' had been in the intellectual and sophisticated style used in written claims of responsibility from a militant organization (search warrant issued for arson attacks with material damage on German armed forces vehicles). Following a worldwide wave of protest against his detention, he was released three weeks later; the trial, however, was finally set three years later with acquittal.[197]

As long as interceptions are done within the legal framework by national authorities in democratic states, the targeting of individual suspects meets with wide acceptance in civil society. However, as it was just exemplified, lawful interception is entirely possible without necessarily meeting principles of proportionality or suitability.

Not only the UK's Occupy London protests in 2011 and further protests were accompanied but also followed by the usage of extensive and excessive technological surveillance measures.[198] Also for instance in the UK anti-terrorism laws were used for tackling minor misdemeanours.[199]

In the case of the U.S., revelations at the end of 2012 and in the beginning of 2013 about F.B.I. surveillance of the Occupy Wall Street Movement do place very serious concerns on what is yet to be expected to come to light in terms of peaceful citizens' protests labelled[200] as a terrorist/extremist threat by U.S. authorities to justify ubiquitous surveillance.[201]

'[…] *Scepticism about state power – a scepticism apparent in the long-standing preoccupation of police studies with the (arbitrary, violent) operation of police powers and discretion* […] *– indicates the importance of forms of constitutional and political regulation within any schema that seeks to defend the proper place of*

---

196 For a general overview on §129a comp.: Reinhard Kreissl, *Mob oder Souverän: Diskurse über die rechtliche Regulierung kollektiver Protestformen*. Leske + Budrich (2000).

197 Connolly (2007), 'Protests over terror arrest of German academic'
http://www.guardian.co.uk/world/2007/aug/21/highereducation.internationaleducationnews
http://delete129a.blogsport.de/2007/08/16/international-scholars-demand-suspension-of-the-a-129a-proceedings-against-all-parties-concerned/
Mikkelsen (2007), 'Guilty by Association' http://www.lewrockwell.com/orig3/mikkelsen4.html

198 Comp. e.g. Evans and Lewis (2011), 'Protester to sue police over secret surveillance'
http://www.guardian.co.uk/uk/2011/may/03/protester-sue-police-secret-surveillance
Gallagher and Syal (2011), 'Met police using surveillance system to monitor mobile phones'
http://www.guardian.co.uk/uk/2011/oct/30/metropolitan-police-mobile-phone-surveillance
Gallagher and Syal (2011), 'Police buy software to map suspects' digital movements'
http://www.guardian.co.uk/uk/2011/may/11/police-software-maps-digital-movements

199 Hastings (2008), 'Anti-terrorism laws used to spy on noisy children'
http://www.telegraph.co.uk/news/uknews/2696031/Anti-terrorism-laws-used-to-spy-on-noisy-children.html

200 P. MacNaughton-Smith, 'Der zweite Code', o. J.
In Klaus Lüderssen and Fritz Sack, *Seminar abweichendes Verhalten II Die gesellschaftliche Reaktion auf Kriminalität*. Frankfurt/Main: Suhrkamp (1975).

201 Schmidt (2012), 'F.B.I. Counterterrorism agents monitored occupy movement, records show'
http://www.nytimes.com/2012/12/25/nyregion/occupy-movement-was-investigated-by-fbi-counterterrorism-agents-records-show.html?_r=0
Cherkis and Carter (2013), 'FBI Surveillance of Occupy Wall Street detailed'
http://www.huffingtonpost.com/2013/01/05/fbi-occupy-wall-street_n_2410783.html
Hedges (2013), 'New documents on activist surveillance might be just the tip of the iceberg' http://truth-out.org/opinion/item/13739-new-documents-on-activist-surveillance-may-be-just-the-tip-of-the-iceberg
Wolf (2012), 'Revealed: How the FBI coordinated the crackdown on Occupy'
http://www.guardian.co.uk/commentisfree/2012/dec/29/fbi-coordinated-crackdown-occupy

the state in the just and democratic production of internal security, and even here it is rightly concerned with the bluntness and fragility of such protective instruments.'[202]

Surveillance technologies and practices become more and more ubiquitous in policing as well as in everyday life practices and it can be observed that (surveillance) technologies which are available will eventually be used. That leads – besides other problematic aspects – to the dilemma of democratic oversight on surveillance measures.

4.6 Conclusion: Human rights at stake

Foucault reminds us that it is analytically impossible to divide power and knowledge: power creates knowledge and vice versa.[203] 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. The problematic aspects of technological approaches such as behavioural pattern recognition are crucial: whoever is in the position to define 'normal behaviour' is establishing a power relation.

As it was elaborated mainly in the chapter 'Information control on the Internet', algorithmic gatekeepers of security and smart surveillance technologies play a crucial role in shaping our cultural perception. Automated technological systems can be used to make inconvenient opinions or even evidence less visible in the virtual public of the Internet or uncommon behaviour less acceptable. This is typically not the result of an intentional moral crusade but rather a side effect of enforcing local cultural or ethical standards. The problem though is that such decisions about decent behaviour or language based on local standards are enforced globally through the Internet.

Additionally, 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.[204]

Practices of dataveillance, cyberveillance, etc. are to become ubiquitous and '*in the surveillance society social sorting is endemic.*'[205] Gandy refers to practices of social sorting as panoptic sort, emphasizing very distinctively: '*The panoptic sort is a screen that excludes, a filter that blocks, a magnet that ignores fine wood in preference for base metals. The sorting process works primarily by eliminating those who are too much, too little, too late … too bad!*'[206] These mechanisms are fundamentally pushing the perpetuation of social inequality. To put that into perspective, matching with a specific (suspicious) subgroup either willingly or accidentally, either as a positive or a false positive, cannot only lead to discrimination quickly, it might also show serious impact on the well being and the whole life course of an individual. While 'mistakes' with impact on individuals and their lives are seen as regrettable, they are also seen as inevitable, as acceptable collateral damage in order to maintain what is perceived the overriding security theorem. Lyon stresses the category is becoming more important than the individual[207] – which is, strictly speaking, no less than fundamentally inhuman.

Accompanied by the fact that the data collected by the private sector for customer relations and targeting and also all data floating in social networks in cyberspace can eventually be used by national

---

202 Loader and Walker, *Civilizing Security*, p. 68f.

203 Foucault and Rabinow, *The essential works of Michel Foucault, 1954–1984. Subjectivity and Truth, Vol. 1, Ethics*.

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

205 Murakami Wood, D. (Ed.), Ball, K., Lyon, D., Norris, C. and Raab, C. (2006). *A Report on the Surveillance Society*. Wilmslow: Office of the Information Commissioner.

206 Oscar H. Gandy, *The Panoptic Sort: a Political Economy of Personal Information*. Boulder, CO: Westview (1993). p. 18.

207 Lyon, *Surveillance Studies*.

security agencies for further extensive dataveillance profiling shows the two sides of the coin once more. *(For problematic aspects of the lawfulness of interception measures, see D 3.2.)*

How seriously the privacy rights of unrelated third parties – who, for instance, happen to be somewhat loosely connected to (perilous) criminals – can be violated was exemplified in the chapter on '*Cyberveillance*'. The fact that law enforcement agencies are to hand criminal case files and similar documents including most sensitive data on unrelated third parties to the media shows that mandatory social-media policies are not only for these authorities a necessity on the one hand while there is also an increasing need for sound legal protection on the other. As Borking remarks, '*Lawyers and technologists should proactively try to solve privacy problems instead of reactively responding to complaints when harm already has been done.*'[208]

The examples of e.g. the Twitter incidents demonstrate how impetuous, overwrought and a somewhat fast-selling item governmental surveillance has already become, creating on the basis of excerpts serious aftermaths for the citizens involved. Since these incidents and scenarios are rapidly increasing, the developments should be observed with concern.
European states do become increasingly regulatory on e.g. behaviour in public space. When taking into consideration possible next steps to be taken by the authorities to prohibit what can be perceived as 'inappropriate behaviour', there is no less than the public civil society at stake.

A further fundamental problem is emerging: 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 practice of those authorities securing security – is consequently going to be negated on a regular basis.

Also the ability to transform external constraints into self-constraints[209] should not be underestimated. Once individuals are facing the possibility of drawbacks, they can easily be restrained from public statements or civic engagement – which was termed the chilling effect.[210] This effect might lead consequentially to the negation of exercising democratic rights. This peril was acknowledged e.g. in Germany in 1983 through a cornerstone decision of the Federal Constitutional Court of Germany, on the foundations of the concept of informational self-determination.[211] In the UK the 2009 report of the British House of Lords recognized this peril as well, stating that the surveillance may disturb some of the preconditions that underpin the relationship between the individual and the state.[212]

If citizens do increasingly consider exercising democratic rights such as participating in political discourse, civic engagement, forms of public protest and the like as potentially disadvantageous or even dangerous, it can be spoken of the civil society being at stake.

---

208 Borking, 'The use and value of privacy-enhancing technologies', in Lace, *The Glass Consumer*.
209 Norbert Elias, *On Civilization, Power, and Knowledge: Selected Writings*. Chicago: University of Chicago Press (1998).
210 Newton N. Minow, *Safeguarding Privacy in the Fight Against Terrorism Report of the Technology and Privacy Advisory Committee* (DIANE Publishing, o. J.).
211 BVerfGE 65, 1 (15.12.1983), comp.: Juristischer Informationsdienst Online: http://dejure.org/dienste/vernetzung/rechtsprechung?Text=BVerfGE%2065,%201
212 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.

5. Alternative concepts

In this chapter, various approaches to maintaining and enhancing security in different domains will be discussed and evaluated. The focus will be on alternative security-enhancing strategies applicable in late modern societies. In comparing strategies to enhance security, their merits will be assessed against the background of an overall theoretical framework.

Adequate responses to security threats can be developed in different ways. A distinction can be made between *prevention* and *mitigation:* A security threat can be tackled in order to prevent the damage materializing. On the other hand, a response can focus on the minimization of damage caused by an event or – possibly most importantly – measures can be taken towards strengthening *resilience,* and a resilience-aware society.

Society-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 lifestyles and universalistic values. We will get back to these problems in the final chapter 'Conclusion'. Social, non-technical alternatives to perceived security threats always encounter a series of standard counter-arguments. They often cannot present the crisp and superficially convincing logic of technological solutions. They operate in a larger, cultural, societal frame, and they approach the problem often in a more indirect and also long-term way when looking at so-called root causes.

5.1 Alternative societal concepts

5.1.1 Security communities

Introduced by Karl Deutsch et al. in the late 1950s and 1960s, the (constructivist) concept of security communities[213] 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, editing an anthology on security communities.[214] This modernized concept gained some new recognition.

According to Deutsch et al., '*a **security community** is a group of people which has become "integrated". By **integration** we mean the attainment, within a territory, of a "**sense of community**" and of institutions and practices strong enough and widespread enough to assure, for a "long" time, dependable expectations of "peaceful change" among its population. By "sense of community" we mean a belief on the part of individuals in a group that they have come to agreement on at least this one point: that common social problems must and can be resolved by processes of "peaceful change". By **peaceful change** we mean the resolution of social problems, normally by institutionalized procedures without resort to large-scale physical force.*'[215]

Two types of security communities are differentiated: amalgamated and pluralistic; the former are units which have merged into some type of common government (e.g. the U.S.), and in the latter the independence of the (national) units remains, nevertheless some common perception of an entity exists (e.g. Canada and the U.S. constituting North America). Based on an extensive study of historical developments of nations worldwide, Deutsch et al. highlight conditions of special importance for security communities: mutual compatibility of main values, a certain way of life, geographic and especially social mobility, processes of open communication, a balance of transactions, interchange in group roles and broadening of the political elite, and also high political and administrative capabilities.

---

[213] 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).

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

[215] Deutsch et al., *Political Community and the North Atlantic Area*. p. 2.

They noted furthermore that certain conditions such as administrative union, ethnic or linguistic assimilation, strong economic ties or foreign military threats were indeed helpful but less essential for a successful amalgamation of a security community than had been assumed before.[216] Hence, a sense of community within a certain territory (or even state) does rather develop bottom-up from within the local societies rather than top-down. Interaction and communication on the societal level are stated key factors for a process of integration.

Adler and Barnett[217] took these factors into account, but supplemented e.g. identities, values and meanings as important factors into the general framework. They define community by three main characteristics: common meanings as the very basis, direct relations and some degree of long-term interest. They observed that many (personal) relations have to exist and/or build up over time between the citizens of such communities, so reciprocity or perhaps even altruism will eventually exhibit over time (= trust and collective identity formations).[218] Adler and Barnett described the development of a security community in three steps: from nascent to ascendant to mature. The first step is herewith to perform change peacefully. The level of mature security communities is characterized by some collective security mechanisms – perhaps also perceptions – and contains also transnational elements.
However, some of their findings are challenged by a study conducted by Tusicisny.[219] He stresses empirical evidence that shared liberal values are not a necessary condition of security community building on the societal level and highlights that security communities showed a greater tolerance of out-groups and, partially, greater trust compared to other societies. He distinguished in his study interstate security communities – where war between states is becoming increasingly unlikely – and comprehensive security communities – where interstate conflicts and also civil war have become unthinkable.[220]
Waever, verifying on the concept(s) of security communities analyzing Europe and Scandinavia, comes to an interesting conclusion: '*"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 and generally to international relations theory, unprepared as it still largely is for structuring thinking about post-sovereign politics.*'[221]

5.1.2 Restorative justice

The conceptual idea of contemporary strains of 'Restorative Justice' dates back to the 1970s. Christie's article 'Conflict as property',[222] originally published in the *British Journal of Criminology* in 1977, initiated an intense debate on the general concept of criminal justice. Although Christie himself never used the term 'Restorative Justice', his findings and critiques of the justice system yet remain key points in the debates around these conceptual frameworks.

Christie claimed that criminal justice systems in modern industrialized democratic states mainly followed logics of control rather than aiming at solving societal conflicts for the benefit of the citizen. The parties in a criminal conflict are represented by specialists within a highly organizational and

---

216 Ibid. p. 24ff.
217 Adler and Barnett, *Security Communities*.
218 Emanuel Adler and Michael Barnett, 'A framework for the study of security communities', 1998, p. 31ff.
Adler and Barnett, *Security Communities*.
219 Andrej Tusicisny, 'Security Communities and Their Values: Taking Masses Seriously', *International Political Science Review* 28, Nr. 4 (January 9, 2007): pp. 425–449
220 Ibid.
221 Ole Waever, 'Insecurity, security and asecurity', 1998, p. 105f; Adler and Barnett, *Security Communities*.
222 Nils Christie, '*Conflict as Property*' (2003), p. 57–69.

specialized legal system and therefore the citizens' conflicts – their very own capability of dealing with conflict – is taken or in fact 'stolen' from them.[223] For Christie, active participation *by those who are concerned* in solving conflict bears a great beneficial potential for the victims as well as the offenders and for society overall.

By bringing the discussion about conflict back into the communities, to e.g. local citizens' summits or victim-orientated neighbourhood courts, taking it off the distant and highly inaccessible bureaucratic criminal court acts, victims are turned from 'nonentities' into important stakeholders.[224] The offenders are not only allowed but even expected to take part in the 'hearings' and are furthermore encouraged to actively do 'reparation work'. A procedure likewise not only aims for *understanding* the underlying reasons for wrongdoing and criminal acts rather than *denouncing* the wrongdoing, but stands also for a social concept of compensation and reparation instead of penalization and punishment. One major principle of restorative justice is, in short: public policy in criminal justice should serve public interests.

Some of the underlying principles are – to a certain extent – realized in European juridical systems, e.g. in criminal law relating to young offenders, e.g. once (re-) integration of these offenders through social community work is the preferred option rather than an imprisonment of these offenders. Such conventions can be found in most European countries' legal frameworks.

Within the variety of contemporary concepts grouping around restorative justice, one of the basic principles is to value and strengthen citizens' participation and empowerment.[225] Abstract juridical processes are seen as beyond the matters of the community. Active participation of those who are concerned is understood as a very core of societal cohesion and also to bear a great potential for further civic engagement. '*Highly industrialised societies face major problems in organizing their members in ways such that a decent quota takes part in any activity at all. Segmentation according to age and sex can be seen as a shrewd method of segregation. Participation is such a scarcity that insiders create monopolies against outsiders, particularly with regard to work. In this perspective, it will easily be seen that conflicts represent a potential for activity, for participation. Modern criminal control systems represent one of the many cases of lost opportunities for involving citizens in tasks that are of immediate importance to them.*'[226]

The contemporary debates on restorative justice[227] can serve in equal measures as a theoretical framework and a practical guideline for an integrated approach to conflict, crime and criminality – and as an alternative to an exceeding and excluding concept of punishment and imprisonment.[228]

Karp and Clear e.g. elaborate on a conceptualization of community justice, identifying five key aspects for successful community justice: (1) operating at the neighbourhood level (2) problem solving (3) decentralizing authority and accountability (4) giving priority to the community's quality of life and (5) involving citizens in the justice process. These should ideally be guided by democratic and egalitarian principles. '*In addition to a community's institutional strength, community capacity may also be evident in the ability of community members to enforce local normative standards. Do bystanders intervene when trouble starts on a street corner? Do neighbours admonish inappropriate behaviour by youths? A community that can effectively exercise informal social control may be less reliant on the formal controls of the police to*

---

223 Ibid.

224 Ibid.

225 K. Richards, 'Restorative Justice and "Empowerment": Producing and Governing Active Subjects through "Empowering' Practices", *Critical Criminology* 19, Nr. 2 (2011): pp. 91–105. http://www.springerlink.com/index/W853163357J37578.pdf.

226 Christie, 'Conflict as Property' p. 61.

227 Comp. Heather Strang and John Braithwaite, *Restorative justice and civil society*. Cambridge UK; New York: Cambridge University Press (2001).
And also: Pelikan, Christa and Katrin Kremmel, ALTERNATIVES-project, '*Restorative Justice*', forthcoming 2013.

228 Claudio Domenig, 'Restorative Justice – vom marginalen Verfahrensmodell zum integralem Lebensentwurf' (TOA-Infodienst Köln, 2011).

intervene in minor disturbances. Police officers, in any case, are unlikely to perform such order maintenance activities without strong inducement, leaving a vacuum in which disorder continues to grow.'[229] Informal methods of conflict-solving are hoped to bear beneficial potential for increasing citizens' subjective trust in security in the local neighbourhood and in the community and subsequently for strengthening civil society through the process of citizens' activation and participation.

Although these processes are meant to be guided and assisted by experts (e.g. justice agencies), it is however obvious that these concepts rely on great trust in the capability of self-organization and the acceptance of high levels of responsibility by members of a community. Such community action raises important questions regarding the application of informal control. First and most important there is evidence that e.g. autonomous community groups have been charged with racism, vigilantism and alike.[230] Second, the question remains to what extent a 'community effort' represents the entire community. '*Even when mobilization is successful, it is important to consider who is being mobilized*,'[231] since evaluation of community policing programmes implied that many individuals and interests are typically underrepresented or even democratic participation efforts are not met at all. Under such negative circumstances, disadvantaged and marginalized groups would not be included, which would violate democratic values.[232]

5.1.3 Communitarianism and community crime prevention

The following statement from Amitai Etzioni emphasizes the Communitarian logic on matters of accountability and responsibility for safety and security neatly: '*Order and autonomy are community needs; centripetal and centrifugal forces either exacerbate or ease the fulfilling of these needs. The relationship between these forces and needs are like those between a new crime wave and the means employed to maintain public safety: They affect each other, but they are hardly identical.* […] *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.*'[233]

[234]Hence, a basic approach within communitarian means of surveillance is the activation of citizens for surveillance–cooperation with the police or with other relevant law enforcement agencies. Such neighbourhood-watch programmes and the like could be seen in the tradition of 'vigilance committees'. This term, which dates back to the 19th century, is based on the idea of citizens' duty to defend their city – even with the force of arms – towards threats from the outside. The idea of using ordinary citizens as regular sources of information – and/or more or less official helpers of the police's everyday work – crops up every now and again under the general term 'community policing'. The term is used for a number of different techniques but is on a general level 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

---

229 D. R. Karp and T. R. Clear, 'Community justice: A conceptual framework', *Boundaries changes in criminal justice organizations* 2 (2000): pp. 323–368, http://www.neighbourhoodjustice.vic.gov.au/webdata/resources/files/Community_Courts_-_an_Evolving_Model.pdf.

230 Ibid.

231 Ibid. p. 358.

232 Karp and Clear, 'Community justice'.

233 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

234 The following four paragraphs are based on our contribution to SurPRISE D2.1 (Draft Key pairs of security challenges and responses).

disorder. For example, citizens asked to report their observations so that governmental authorities can take further steps. Occupational groups such as teachers, social workers, medical staff and other societal actors are requested to report all kinds of 'suspicious incidents' to the relevant governmental bodies.

A recent example of such a procedural method is a campaign launched by the Metropolitan Police, the City of London Police and the British police forces, addressing citizens with a leaflet displaying the following text in bold letters: 'It's probably nothing, but … '; it then goes on in fine print 'if you see or hear something that could be terrorist related, trust your instincts and call the confidential Anti-Terrorist Hotline. Our specially trained officers will take it from there. 0800 789 321 Your call could save lives.' The back of the leaflet elaborates further details under the heading 'Communities can defeat terrorism'. The text starts with the sentence 'Terrorists live amongst us when they are planning their attacks.' It then lists a number of behaviours deemed suspicious: 'Who has bought or stored large amounts of chemicals, fertilizers or gas cylinders for no obvious reason. / Who has bought or hired vehicles in suspicious circumstances. / Who holds passports or other documents in different names for no obvious reason. / Who travels for long periods of time, but is vague about where they're going.'

Communication between police and citizens is a well-researched topic and the studies show a number of converging results. About one third of contacts with police using emergency numbers is triggered by traffic-related incidents (road accidents, cars blocking driveways etc.), around 10% of the calls report person-related problems (drunks, psychopaths, sick persons in public space), and around 30% of the calls fall under the category of false alarm or misuse. A small percentage of the calls originate with other institutions (e.g. public transport authorities). When looking at this communication from the police side, studies suggest between 70% and 90% of police activities (patrol cars driving to the scene of the presumed incident) are based on events reported through external calls to the emergency phone number. The spread of mobile phones has increased the number of police–citizen contacts significantly. Since police resources are limited not every call can be answered adequately in due time. Increasing the number of calls to the police by activating citizens to participate in the search for potential terrorists constitutes a further burden for the police. Investigations reconstructing the information flow (or cognitive division of labour) in particular high-profile cases have shown that some pieces of potentially relevant information have become known to the police but only after the fact (i.e. after a terrorist attack or major crime happened) are identified as having been a lead to the perpetrators.

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. Adding more information that is not very well structured (see the above cited example from the London Police) is not very helpful. (4) Targeted activities in high-profile security cases such as terrorism are problematic because they create a substantial number of false positives, who are then subjected to unpleasant actions of control and investigation by police officials, or who could see their travelling or business practices seriously restricted or impaired. '*Indeed it would appear impossible clearly to separate means from ends in community crime prevention. This may be because, in most formulations of the community approach, the proposed solution – a community structure that controls crime – is also the antithesis of the perceived problem – a community that does not control its own crime. With such circularity,*

means and ends become blurred ...' [235] He also observed another crucial issue: practitioner accounts seem 'muddled, inconsistent and untheorized'.[236]

Overall, the idea of involving ordinary citizens in surveillance purposes can create a number of unintended side effects and hence has to be treated with caution. Bradley and Walters remind us of a pitfall likely to arise through such collaboration: '*Multi-agency crime partnership under neo-liberal conditions inculcates voluntary participation under the guise of empowerment and partnership, yet displaces responsibility via contractual arrangements in what is now referred to as "contracting for community responsibility"*.'[237] It should be noted that such strategies can erode fundamental trust or ontological security in the long run, fostering a climate of insecurity rather than increasing security.

5.1.4 Social resilience and community resilience

What safety engineers have learnt is to simplify and adapt the system to be secured instead of stepping up control over its performance, while at the same time maintaining a high level of output and system safety. Can the debate on societal alternatives learn from insights gained in the field of safety engineering?

Minimizing risk-proneness in structures through simplification creates systems with higher resilience to malfunctions as well as higher resilience to external threats. One of the key concepts emerging in security discourse over the last few years is the idea of 'resilience'. '*Since the turn of the millennium, resilience has risen to the rank of a central paradigm not only for protection against potentially catastrophic ecological risks but for dealing with systemic risks of all sorts and as crucial for national security policies in general*.'[238] Focusing on resilience, security problems appear to be of a two-fold 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 system instead of a consequence of externally monitoring the inner workings (transactions, movements, interactions) of this very system to detect signs of future issues. '*The term "resilience", a borrowing from the science of materials, came into use to describe our vision of a society that would be able to absorb sudden shocks and yet bounce back quickly into its normal shape.*'[239]

Bristow envisages three key factors of resilient regions[240], 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 happen 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 networking and information sharing*'.[241] (3) An important characteristic of resilient

---

[235] Tim Hope, 'Community Crime Prevention', in *Building a safer society*, 1995, 23; Michael Tonry, *Building a Safer Society Strategic Approaches to Crime Prevention* (*Crime and Justice: A Review of Research*) *Volume 19: An Annual Review of Research: v. 19*, University of Chicago Press Journals, (1995).

[236] Hope, '*Community Crime Prevention*', p. 22.

[237] Trevor Bradley and Reece Walters, 'The managerialization of crime prevention and community safety', (2002), p. 255.

[238] Kaufmann, Stefan and Sabine Blum, Governing (In)security: The rise of resilience, pp. 235–258. In: Gander, Hans-Helmuth et al., *Resilienz in der offenen Gesellschaft*, Nomos, Baden-Baden (2012).

[239] David Omand, 'The dilemmas of using secret intelligence for public security', in *The new protective state*, o. J., p. 143; in: Peter Hennessy (Ed.), *The new protective state: government, intelligence and terrorism*. London; New York: Continuum (2007).

[240] 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.

[241] Ibid.

places is their emphasis on small-scale activities embedded in the local structures while not over-depending on mono-cultural key sectors. Also, e.g. invasive bureaucracies are to be minimized. In a comparative study about the resilience of neighbourhoods, Wallman found out that open systems have a strong tendency to be more resilient: '*Each locale is examined as a system which is more or less open or closed; open systems tend to be more resilient when faced with external challenges.*'[242]

Jasanoff points to the problem of imprecise measures for creating resilient structures. She particularly advocates taking the practical experiences of individuals seriously: '[…] *methods of assessment still take populations rather than individuals as the unit of analysis.* […] *Such characterizations leave out of the calculus of vulnerability such factors as history, place, and social connectedness, all of which may play crucial roles in determining human resilience. Through participation in the analysis of their vulnerability, ordinary citizens may regain their status as active subjects, rather than remain undifferentiated objects in yet another expert discourse.*'[243]

Thus, she highlights a core point of resilience approaches: activating community resources and involving civil society actors to create resilience (and therefore enhance security) requires taking 'laypersons' expertise' into account. Edwards is getting this into perspective, describing community resilience as an elastic concept, stating furthermore: '*Community resilience is an everyday activity. It manifests itself in meetings and conversations, dialogue and training, skills and information and – when disaster occurs – action. Although it may be formalized in local parish plans or community risk registers, community resilience is first and foremost about people* […].'[244] He is placing strong emphasis on *engagement*, *education*, *empowerment and encouragement*.[245]

However, for instance, Kaufmann and Blum note that strategies focusing on the resilience of the population 'invariably draw on a particular moral–political rhetoric.[246] The problem of reducing resilience to a purely moralistic concept has to be considered, when discussing alternative approaches to security. Nonetheless resilience has a central advantage over the standard surveillance and prevention strategies. Since complex systems, like e.g. a metropolitan public transport system, cannot be comprehensively protected against attacks, surveillance and prevention strategies can be expanded indefinitely, without ever reaching a satisfying level of security. In an interview, the former head of DG JLS Franco Frattini proposed raising the level of security checks at railway stations to the level of airports, since high-speed trains are vulnerable critical infrastructures and can be the target of terrorist attacks. This reasoning nicely demonstrates the limits of a surveillance and prevention approach. Resilience on the other hand acknowledges the risk of attacks, failures and malfunctions and focuses on the robustness of the system and the mitigating reactions in the face of threats and damages. This refocuses the strategic approach and can help to curtail the unlimited logic of surveillance.

5.2 Other alternative approaches

5.2.1 Urban planning

Conceptual ideas to eliminate disorder in cities through urban planning date back to Le Corbusier and his modernism architecture theory. An earlier approach to urban planning was developed by Ebenezer Howard, who advocated the establishment of garden cities.[247] He happened to initiate the garden city

[242] Sandra Wallman, *The Capability of Places: Methods for Modelling Community Response to Intrusion and Change*. Pluto Press (2011).
[243] Jasanoff, 'Technologies of humility', p. 241.
[244] Edwards, *Resilient Nation*, p. 79.
[245] Edwards, *Resilient Nation*.
[246] Stefan Kaufmann and Sabine Blum, *Governing (In)security: The rise of resilience.*
[247] Ebenezer Howard, *Garden Cities of Tomorrow*. London: S. Sonnenschein (1902).

movement in the UK in 1898, which highlighted the problems cities were facing at that time as a result of rapid industrialization. Howard and the movement wanted to create self-contained communities, surrounded by what Howard called greenbelts, creating areas for residence, industry and agriculture.

Possibly slightly exaggerated but condensing the development of urban planning neatly, one could say that these two different approaches (Le Corbusier versus Ebenezer Howard) are representing the concept of *modernism* one the one hand and the concept of vitality on the other and that these two basic conceptual frameworks of urban planning are then found to be clashing throughout the entire 20th-century history of urban-planning.

Crime prevention through urban or environmental design was intensely discussed in the 1960s.[248] Large tower blocks built in the decades after WWII were increasingly seen to be to some extent to blame for social problems and high crime rates and also alienation in general. Residents' feelings of control over and personal responsibility for their neighbourhood and environment were lower when they lived in (large) tower blocks compared with residents of other areas. This perspective seemed to be approved in statistical crimes rates that were comparatively higher in tower block areas as in other areas.[249]

Environmental determinists like Jane Jacobs[250] and Oscar Newman[251] basically represent the two contrary basic positions to be taken on that matter: Jacobs advocated lively and vivid neighbourhoods, elaborating that communities in the true sense were characterized by complexity, and therefore logically the separation of space would destroy communities and their sense for their environment.[252] On the other hand, Newman's controversial but highly influential Defensible Space Theory came to entirely different conclusions. Besides e.g. promoting ideas of creating open space or juxtaposition of dwellings which allowed for an (panoptic) overview on the public areas and the like, he claimed that areas should clearly be defined for various functions and moreover he also wanted to subdivide residential areas into smaller entities for specific 'similar' inhabitants, so that citizens would adopt proprietary attitudes.[253] This translates into the idea of spatial social sorting via social background, income, age etc. and possibly even pushed approaches of zero tolerance as well as the concept of gated communities. Urban design approaches which followed the basic premise of Newman for decades reject the concept of a vivid public space being reclaimable by all citizens – hence it is believed that a safe living environment consists of regime and arrangement rather than 'chaos'.

This exemplifies very well that *signing out crime approaches* can be followed from two opposite directions: by believing in a vital public space and the 'eyes of the street' (e.g. Jacobs) or by believing in segmentation, fragmentation and control (e.g. Newman).

Since 'urban planning' as a research subject goes far beyond the framework of this task, it cannot be elaborated on in greater length. Representative for the debate are e.g. the works of Benevolo[254] for a general overview of European city development, Taylor[255] for urban planning theory after WWII, or the Global Report on Human Settlement on recent developments.[256]

---

248 Comp. e.g. Jane Jacobs, *The Death and Life of Great American Cities*. New York: Random House (1993) [Original 1961]
And also O. Newman, *Defensible Space: Crime Prevention through Urban Design*. New York: Macmillan (1972).

249 Ibid.

250 Jane Jacobs, *The Death and Life of Great American Cities*.

251 O. Newman, *Defensible Space: Crime Prevention through Urban Design*.

252 For elaboration on the development in European cities, see e.g. Andreas Feldtkeller, *Die zweckentfremdete Stadt: Wider die Zerstörung des öffentlichen Raums*. Campus (1994).

253 Ibid.

254 Leonardo Benevolo, *The European City*. Hoboken, New Jersey: Wiley-Blackwell (1995).

255 Nigel Taylor, *Urban Planning Theory Since 1945*. SAGE (1998).

256 United Nations Human Settlements Programme, *Enhancing Urban Safety and Security: Global Report on Human Settlements 2007*. Earthscan (2007).

Nevertheless it may seem that urban local neighbourhood movements like 'reclaim the streets'[257] or urban community gardening[258] – which have been for at least more than a decade on the rise worldwide – do acknowledge Howard's and Jacobs's positions.

5.2.2 Safety engineering

Looking at the lessons learned in the field of safety technology, the unintended and negative side effects of an unrestrained increase in control measures become obvious. Implementing control structures to oversee the operation of a technical system prone to malfunction (e.g. a nuclear power plant) will create new opportunities for malfunctioning within the operation of the control structures. Charles Perrow talks about tightly knit complex systems escaping comprehensive control owing to unforeseen interaction effects of events that are trivial in themselves but can create severe system failure when combined.[259] A complex technological system equipped with a multi-layer control structure with built-in redundancy is not necessarily less prone to malfunction.

Three types of problems can be identified here: (1) Control devices such as sensors are technical systems, and hence malfunctions are possible. This problem can be addressed by second-order controls or increased redundancy, though both are not a final solution to the problem. (2) Human system operators interacting with the system through a techno-social interface apply their own logic to decide about the state of affairs in a given situation. Frequent false alarms will foster a routine reaction of ignoring these alarms. This in turn increases the probability of ignoring a message conveying a real malfunction. (3) Humans have developed in the process of evolution what could be termed a 'natural alertness' – sometimes referred to as a 'sixth sense' – helping them to automatically identify threats in their environment.[260] But when operating in a context of technological controls, this capacity tends to wither. Information from the environment constituting a warning signal for the human information processing systems is ignored when at the same time the technological control systems communicate that all systems are go.

Safety engineering has undergone a change of paradigms from technical to passive safety solutions, i.e. from a 'more-of-the-same approach' to smart (or resilient) systems design. Taking a technology with a high potential for serious accidents, such as civil nuclear power, the new types of nuclear power plants have a reduced number of parts, including a substantially reduced number of technical safety systems, while at the same time safety has been increased by applying new design principles.[261]

When looking at the 'system' in security terms, at the most general level in security discourse one would have to replace this with the term 'society'. Following the logic of new safety design in security discourse, this translates into looking at the 'design' of society or social systems and not at new control and surveillance measures when talking about increasing security.

---

[257] Comp. Jordan (no date), '*Case Study: Reclaim the streets*' http://beautifultrouble.org/case/reclaim-the-streets/ Also: Marion Hamm, '*Reclaim the Streets: Global Protest, Local Space*', Republicart. (2002).

[258] Ferris, J., Norman, C. and Sempik, J. (2001). People, Land and Sustainability: Community Gardens and the Social Dimension of Sustainable Development. *Social Policy and Administration*. 35(5). pp. 559–568.

[259] Charles Perrow and Klaus Traube, *Normale Katastrophen: die unvermeidlichen Risiken der Grosstechnik*. Frankfurt/Main; New York: Campus (1992).

[260] On Automaticity see: John A. Bargh and Erin L. Williams, 'The Automaticity of Social Life', *Current directions in psychological science* 15, Nr. 1 (February 2006): 1–4 http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2435044/.

[261] Malcolm C. Grimston and Peter Beck, *Double or quits?: the global future of civil nuclear energy*, Sustainable Development Programme (Royal Institute of International Affairs). London: Earthscan (2002). p. 147ff.

5.2.3 Technology-based privacy protection

5.2.3.1 Usability and privacy

Designing interactive systems with personal privacy implications does have a variety of requirements: Systems should be designed in a way which makes their potential for disclosure clear, so that users can adapt the system into their everyday practice.[262] One of the demands of human computer interaction is to make the (privacy) solutions as transparent as possible: '*Many of the specific security and privacy problems facing users of the World Wide Web today are a direct result of the mismatch between what is visible to the user and what is actually happening inside the computer.*'[263] Privacy measures have to be accessible by the end users if so required, but shouldn't get in the way of daily (work) routines.

Historically, security solutions have been designed for highly skilled technical users; that is partly why IT security systems are often difficult in everyday usage and/or interrupting one's workflow. Since the end-user community nowadays includes basically the whole population, a revision of these original premises has become more and more necessary. '*Many people believe that there is an inherent trade-off between security and usability.* […] *But as the world around us makes clear every day, if people are unable to use secure computers, they will use computers that are not secure. At the end of the day, computers that are theoretically secure but not usable do little to improve the security of their users, because these machines push their users away to less secure platforms.*'[264] The challenge for software engineering for non-technical end users is to prevent this from happening.

Evaluations involving in particular the (non-technical expert) layperson end users are to be carried out at various stages in the development of new technological solutions. In human-computer-interaction a new emphasis on privacy is to be seen in the development and deployment of intelligent tutoring systems.[265] Evaluation, auditing and task identity on all levels are core modules in the development process of novel technology solutions. Regular and independent auditing of the design, usability, stability and security of computerized technical hard- and software systems is thereby one necessary provision.

There is also a shift to be observed within the last few years: a growing number of promising easy-to-use web applications and free- and shareware solutions etc. for security purposes is available nowadays, not requiring high technical expertise. Clearly, such applications do not replace the need for usability design in the first place, but support enhancing awareness of security gaps and simplify access to low-threshold solutions feasible for everyday life. Projects like Privacy Choice[266] are not only offering practical services (checking personal privacy settings across Facebook, Google and the like, fixing problematic privacy settings on demand) but are currently creating a Wikipedia for privacy policies.

Bennett points out what could be marked as a core value in the code of practice in recent usability studies: '[…] *new technologies should be shaped to human ends rather than vice versa*'.[267]

5.2.3.2 Privacy by Design (PbD) and Privacy-enhancing Technologies (PETs)

The key functions of privacy-enhancing technologies are to perpetuate anonymity, pseudonymity, unlinkability, unobservability. So roughly speaking, PETs are those kinds of technologies which are to

---

262 Lederer u. a., 'Five pitfalls in the design for privacy'; in: Cranor and Garfinkel, *Security and Usability*.
263 Cranor and Garfinkel, *Security and Usability*, p. 294.
264 Ibid. p. ix ff (Introduction).
265 Clare-Marie Karat, Carolyn Brodie and John Karat, 'Usability design and evaluation for privacy and security solutions', 2005; Cranor and Garfinkel, *Security and Usability*.
266 Privacy Choice: website to be found at: http://privacychoice.org/
267 Bennett, *The privacy advocates*. p. 94.

protect the (end) user from (easy) identification by third parties and therefore create (layperson) end-user empowerment.[268]

According to Ann Cavoukian[269], seven guiding principles for Privacy by Design (PbD) are to be envisaged: PbD is ideally (1) proactive, not reactive, (2) privacy is the default case for the implementation of technologies and not vice versa, (3) privacy has to be embedded into the design, (4) while full functionality is ensured, (5) privacy is about life-cycle (end-to-end) protection, (6) visible and transparent, (7) which all comes down to respecting the user's privacy.[270]

But despite the fact that PbD bears valuable ideas for privacy protection, it has nevertheless to be stated that PbD is to some greater extent limited to those technologies used within local or at the utmost national boundaries. '*But so far its impact on a field where its relevancy is obviously high – ubiquitous computing – has been rather minimal. An increasing number of research projects are under way in the field of internet privacy, some work has already been done in the field of Computer Supported Collaborative Work, but only a small amount of work has so far been accomplished in the area of ubiquitous or pervasive computing.*'[271]

As Cranor states, there are still issues remaining. For instance, most PETs research is only focusing on the prevention aspect and, impractically, PET tools quite often just allow the user to turn the protection on or off, although more levels are needed.[272] (*See also the chapter 'Usability and privacy'.*) Researching the field of PET technologies, Phillips reminds us of another important aspect (already noted before in connection with algorithmic gatekeeping) which is fundamentally true to technological gatekeeping in general: '*Especially when legal and technical infrastructures are seamlessly integrated, the ideologies informing them are embedded into everyday practices and ontologies. Therefore, care must be taken to extrapolate from "common sense" definitions of privacy to the social configurations that those definitions entail, and to suggest other possibilities for the informed design of information technology and policy.*'[273]

Whereas a large number of PbD measures can be applied to (local) CCTV technologies and PbD approaches can also be adopted to mitigate the risks of smart metering in terms of (possible misuse of) surveillance purposes (e.g. preventing the achievability of personal profiling). A vast majority of theoretical approaches are not feasible owing to the impacts of globalization. The mere inherent quality of the World Wide Web as *cyberspace* and the novel possibilities provided by the rapid progress in the field of for instance drone technologies are neglecting PbD attempts in the first place. Another key issue is the fact that '*legislative measures of regulation are not able to keep up with the technical development*'[274], in addition to the even more crucial issue that sound legal protection does not truly exist across national states and their specific national legal frameworks. (*See also the chapter 'Function creep' and D 3.1 for greater elaboration.*)

Concerning cyberspace surveillance, exemplifying DPI and Trojan technologies does show the limitations of PbD. Also, as stated in D3.1 (*chapter 'Effectiveness of Trojans and civil rights impact'*), it is additionally to be '*assumed possible that even the deploying security agencies have neither full control over the technical procedures triggered once the system is brought onto the target device, nor are they able to provide verifiability to supervisory authorities without the aid of the vendor companies. This may lead to a*

---

268 Guagnin, Hempel and Ilten, 'Privacy Practices and the Claim for Accountability'.

269 A. Cavoukian, 'Privacy by design', *Report of the Information & Privacy Commissioner Ontario, Canada* (2012) http://privacybydesign.ca/content/uploads/2012/04/Privacy-by-Design-Origins-Meaning-and-Prospects.pdf

270 See also: S. F. Gürses, C. Troncoso and C. Diaz, 'Engineering privacy by design', *Computers, Privacy & Data Protection* (2011) https://www.cosic.esat.kuleuven.be/publications/article-1542.pdf

271 M. Langheinrich, 'Privacy by design – principles of privacy-aware ubiquitous systems', in *Ubicomp 2001: Ubiquitous Computing*. Zürich (2001), 273–291, p. 1. http://www.springerlink.com/index/y9reah898fcuc2n8.pdf.

272 Lorrie Faith Cranor, 'Privacy Policies and privacy preferences', in: Cranor and Garfinkel, *Security and Usability*.

273 David J. Phillips, 'Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies', *New Media Society* Vol 6 (6) (2004): p. 692.

274 Eva Schlehahn (2013), SurPRISE, D3.1.

major shortage of transparency and accountability in the context of Trojan deployment.'[275] Once for instance DPI is carried out in one country, while the proxy servers are based in another country, the applicable legal ground is already difficult to determine. Third parties can gain access to data, despite this was either never been intended in the first place, or data protection measures could have been waived by the concerned parties accepting the default setting of the system. This was crucial e.g. regarding the diplomatic issues in 2011/2012 between the U.S. and Europe over the DHS collection and storage of detailed personal aircraft passenger data[276]. Interestingly the European Union is contemporarily planning to implement a similar database for intra-European air travel[277]. In general, ubiquitous surveillance of social networks can inherently not be tied down within national boundaries or to national legal frameworks (which was already stressed in the chapter on 'Cybercrime'.)

Privacy policy management could theoretically become a tool to protect the personal information stored about customers, employees etc. (within national boundaries). As Karat et al. state, currently there is no unified way for the implementation of privacy policies in existence[278]. That seems to be one of the reasons why the implementation of reasonable PbD as well as PET solutions seems comparatively slow.

(*For a more in-depth elaboration on and applicability assessment of PET and PbD solutions for SOSTs, see D 3.1.*)

5.2.3.3 Privacy Impact Assessment (PIA)

Murakami Wood et al. strongly emphasize that considerable merit is to be found in adopting Privacy Impact Assessment (PIA), especially for the regulatory practices of jurisdictions[279]. They conceptualize: '*PIA may best be seen as an instrument that those who propose new or revised information systems that process personal data can use themselves to mitigate the potentially harmful effects of these systems upon the privacy of the persons whose data are processed.*'[280]

The value or beneficial potential of PIA is already enhanced in the process itself. Murakami Wood et al. even refer to PIA as a philosophy rather than an approach.[281] Assessing actual or potential effects on privacy is guided by risk-assessment and has a built-in early-warning technique for decision-makers. This is accompanied by the examination of various options to foster alternatives. Ideally, results of such PIA should be made available to the public and especially encourage regulatory bodies.[282] Hence, PIA is not to be seen as just a tool for auditing or '*a tick-box exercise giving an answer or "score" at the end*'[283], but rather a process of raising questions and highlighting issues that need to be resolved.

The UK's Information Commissioner's Office offers a Guideline Handbook Online on PIA[284], containing PIA screening questions, checklist templates and various privacy strategies as initial starting points. Four

---

275 Eva Schlehahn (2013), SurPRISE, D3.1.

276 Krick (2012), 'Fluggastdatenabkommen mit den USA: Europäischer Offenbarungseid' http://www.spiegel.de/reise/aktuell/fluggastdaten-pnr-der-eu-abkommen-mit-der-usa-in-der-kritik-a-828814.html

277 No author (2012), 'Flüge von and nach Europa: EU will massenhaft Passagierdaten sammeln' http://www.spiegel.de/politik/ausland/vorratsdatenspeicherung-eu-will-flugpassagiere-ueberpruefen-lassen-a-871789.html

278 Karat, Brodie and Karat, 'Usability design and evaluation for privacy and security solutions'; in: Cranor and Garfinkel, *Security and Usability*.

279 D. Murakami Wood (Ed.), K. Ball, D. Lyon, C. Norris, and C. Raab, *A Report on the Surveillance Society*. Wilmslow: Office of the Information Commissioner (2006), p. 89ff.

280 Ibid. p. 91.

281 Ibid. p. 91f

282 Ibid. p. 91f

283 Ibid. p. 92.

284 UK Information Commissioner's Office: (no date), Website: Handbook: http://www.ico.gov.uk/pia_handbook_html_v2/html/0-advice.html

different types of privacy strategies are envisaged: minimalist, comprehensive, broad and social impacts/public policy.[285] The document also states that the PIA process is partly covering the same ground as stakeholder management and highly recommends deciding on a privacy strategy *before* a PIA process is implemented.

Clearly, a broad perspective taking social impact and the underlying philosophy into account can be stated as the most beneficiary one: '*The essential goal is to describe personal data flows as fully as possible so as to understand what impact the innovation or modification may have on the personal privacy of employees or customers and how fair information practices may be complied with. Ultimately, a privacy impact assessment is a risk assessment tool for decision-makers that can address not only the legal, but the moral and ethical, issues posed by whatever is being proposed.*'[286] Thus, privacy impact assessment is possibly one of the most interesting relatively novel approaches to advocate awareness and protection of privacy based on a conceptual framework. However, such assessment is only applicable for those technologies already employed and has hence no impact on the developmental processes of novel technologies.

As the previous paragraphs show, 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 understanding of science and technology can be considered to have a positive impact on security by providing the basis for a rational public discourse.

5.2.4 Public Understanding of Science (PUS)

The concepts grouping around Public Awareness of Science (PAwS) and Public Understanding of Science (PUS) can be regarded as key conceptual frameworks for an inclusion of the (lay) public into policy-making. PUS came to recognition as a self-contained term in Great Britain in 1985 through a report by the British Royal Society[287] titled 'The Public Understanding of Science', also known as the Bodmer Report. It contained a large number of recommendations aiming at the educational system as well as mass media and the general course of science communication. It demanded that research shall be conducted on the ways of measuring public understanding of technology and science to monitor citizens' attitudes to science, and that popular versions of scientific reports be made available to a broad public. Science education, consumer education and especially public controversies over science and technology are core points for citizens' ability to take part in the debates and to exercise their democratic rights. As Bennett reminds us, '*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.*'[288]

Burns et al. define science communication '*as the use of appropriate skills, media, activities, and dialogue to produce one or more of the following personal responses to science* […]*: Awareness, Enjoyment, Interest, Opinion-forming, and Understanding Science.*'[289] PUS approaches not only play therefore a significant role

---

285 Ibid. http://www.ico.gov.uk/pia_handbook_html_v2/html/1-Chap1-1.html#stakeholder

286 Flaherty (2000), Webpage: Presentation held on the Annual Meeting of Privacy and Data Protection Officials in Venice, 2000; *Privacy Impact Assessment: an essential tool for data protection.* http://aspe.hhs.gov/datacncl/flaherty.htm

287 British Royal Society, Website (1985) http://royalsociety.org/policy/publications/1985/public-understanding-science/

288 C. Bennett, *The privacy advocates*, p. 98.

289 T. W. Burns, D. J. O'Connor, and S. M. Stocklmayer, 'Science Communication: A contemporary definition', *Public Understanding of Science*, Nr. 12 (2003): pp. 183–202.

in a better public understanding of technologies but also help create or even push an informed public debate about the impact technologies have in general and also for matters of security and surveillance in our society. This appears even more important because '*appeals to public opinion have become central in political discourse, since public opinion provides the ultimate ground of legitimacy for a specific political and legislative agenda.*'[290]

In short, PUS is engaging in the interdependencies between policymakers, the scientific community and the lay public, aiming for a comprehensive public understanding of science to create an informed public debate and therefore a sensitive, responsible handling of novel technologies by all parties concerned. *For an elaboration on the background and contemporary strains as well as practical applications (addressing public participatory exercises such as citizen summits and the like) of the concept 'Public understanding of science' in Europe, see D2.2 and also SurPRISE task 4, forthcoming.*

'*It has become an article of faith in the policy literature that the quality of solutions to perceived social problems depends on the way they are framed. If a problem is framed too narrowly, too broadly, or wrongly, the solution will suffer from the same defects.* […] *Frame analysis thus remains a critically important, though neglected, tool of policy-making that would benefit from greater public input.*'[291] Public events in the course of PUS approaches – such as citizen summits and further participatory exercises – are yet another component to strengthen citizens' trust in (their) democratic system(s) and to trigger civic engagement in the benefit for responsible and sustainable policy-making.

5.2.5 Some paradoxes and ironies

Sofsky reminds us of the fact that freedom is not equal to democracy, and not even necessarily connected.[292] He states that freedom (to privacy), 'the desire to remain undisturbed', seems to be of less importance than desire for approval, care, protection, or companionship. Freedom is neither the sovereignty of the majority, nor the equality of life chances. Freedom as a political order must be measured against the strengths of the barriers protecting the individual against actions of the government as well as against assaults by neighbours and attacks of enemies. On the contrary, democracy can be translated as supremacy of the majority. According to Sofsky, democracies do not only have the power to impact the lives of citizens intolerably, democratic majorities are able to oppress minorities.[293] Taking this into consideration, the variety of community-based concepts – especially in the areas of restorative justice or community crime prevention – has obviously to be treated with great caution.

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.*'[294]

Under the Fordist welfare regime of social policy, which is fading away 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

---

http://www.somedicyt.org.mx/assets/hemerobiblioteca/articulos/Burns_SciCom_a_contemporary_definition.pdf

290 G. Vanderveen, *Interpreting Fear, Crime, Risk, and Unsafety*, p. 8 (also citing Zaret, 2000).
291 Sheila Jasanoff, '*Technologies of humility*', p. 240.
292 Wolfgang Sofsky, *Das Prinzip Sicherheit*. Frankfurt am Main: S. Fischer Verlag (2005), p. 148ff.
293 Sofsky, *Das Prinzip Sicherheit*.
294 Vincenzo Pavone (2013), SurPRISE project D2.2.

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 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 these 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.

6. Conclusion: Towards balanced risk awareness

Where does an analysis of security challenges from a social science perspective leave us? 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 proactive 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 predominantly look at these inner processes as root causes of security problems.

When looking at the second dimension of security problems, i.e. mitigation, in the debate on crime the main ideas discussed here are not focusing on the selective exclusion or incapacitation of perpetrators but on reintegrating or restoring a status quo ante after a conflict. Perceiving a criminal act as a disturbance of a peaceful and non-violent social life or social world, the main option for mitigation from a resilience perspective would be some sort of re-integrative repair of the disturbed order (instead of an approach focusing on exclusion of the 'faulty' part/member). Such ideas are developed in the debate on restorative justice. Crime is not seen primarily as transgression or breaking of a norm, but as an element of a conflict, involving members of the community.[295]

In comparing technical systems and the perspective of safety engineering experts on the one hand with social systems and the problem of improving societal security on the other, a crucial difference has to be taken into account: while technical systems can be designed and engineered from an external position, social systems are always performative, i.e. they cannot (and should not) be designed or redesigned from the outside. Here, the 'observers' and 'engineers' are at the same time members and citizens or in other words: societies when seen from a sociological perspective can be analysed only from within.[296] This observation has a number of consequences when it comes to the analysis of social problems and the more so, the bigger and more pressing these problems appear to be. Security problems are among these "big" problems. The state of affairs cannot be observed from some outside vantage point.

With regard to the problem of security, such an internal perspective requires a 'horizontal' process of deliberation as opposed to a technical external approach, drawing on objective knowledge providing the magic bullet for the problem at hand. What has to precede any discussion of 'solutions' is a robust understanding of what the problem is in the first place. As mentioned above, the evolution of modern globalized societies has created a number of risk-prone structures and processes, and an awareness of these risks is gradually emerging in public discourse and taken up in political debate. Ideas from social theory like 'risk society'[297] have developed into household words of the educated classes, used to describe the living conditions in contemporary societies.

A central argument in the debate about this type of society is the devaluation of traditional expert knowledge. As Beck has pointed out, modern societies, or what he calls the societies of the first modernity, were based on the idea of (economic, social and cultural) progress as a consequence of new and improved technologies (in production, communication etc.). What became obvious though are the destructive and disruptive potentials of modern technologies and the impact of the modes of

---

[295] Strang and Braithwaite, *Restorative justice and civil society*.
Also: Marian Liebmann, *Restorative justice: how it works*. London; Philadelphia: Jessica Kingsley Publishers (2007).

[296] Niklas Luhmann, *Die Gesellschaft der Gesellschaft*. 1. Aufl., Frankfurt am Main: Suhrkamp (1997).

[297] U. Beck, 'Living in the world risk society', *Economy and Society* 35, Nr. 3 (2006): pp. 329–345 http://www.tandfonline.com/; Beck, *Risk society*.

production based on these technologies. The close links between modern technology, surveillance and ecological disasters have been addressed by a number of scholars for quite some time.[298] Their analysis has a strong dystopian ring to it. Beck's idea of the risk society goes beyond dystopian scenarios in pointing out solutions for social problems created by modern technology beyond a techno-critical attitude.

Deconstructing techno-optimism can help to produce a reflexive attitude towards the problems emerging in advanced late-modern or post-industrial societies. With regard to the problems of security, this means acknowledging the emerging security problems without relying on the proposed (technological) solution and putting threats and solutions into perspective.

In the most general terms, it is the internal dynamic of modern global society producing the hazards, risks and dangers justifying the application of surveillance-orientated security technologies. Referring to the global risk society, the term 'internal' entails protracted conflicts, migration, pollution and poverty alongside the second- and third-order problems emerging in industrialized regions of the Atlantic rim.

With growing complexity and interconnectedness, vulnerabilities are increasing in this society. And high vulnerabilities plus high potential damage combine into the toxic brew for increasing surveillance and control. Vulnerabilities increase since members of Atlantic rim societies are depending on a number of critical infrastructures – from electricity to logistic chains in food supply and the Internet. But they also depend on global trade and global economies, producing rich and poor nations and thus not only global migration from the global south but also a substantial potential for political and social conflicts. These conflicts take on the form of security risks in Western societies.

As pointed out in the previous chapters, a number of surveillance practices make use of data produced in the context of mundane activities such as shopping, communicating and travelling. The conveniences of contemporary consumer culture are traded in for a number of dependencies on (cognitive and technological) abstract systems. These systems are vulnerable and have to be protected against different sorts of failures and attacks. Critical security studies point to these kinds of internal vulnerabilities. But beyond this aspect of the vulnerabilities of the mega-machine, as Lewis Mumford has called it,[299] there is a global dimension to security in a more material sense.

It would be easy to draw up a balance sheet relating the amenities enjoyed by the smaller part of the world population to the suffering of the rest. It is a truism in criminology that social inequalities breed violence and crime, and this is true on a global scale as well. Securing the supply with different kinds of resources (from crude oil to rare earths to food) translates into exploiting a substantial part of the world and maintaining a more or less peaceful imperialist global regime. Taking this aspect into account, the discussions about security take a different twist. 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 Western 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 trade-off between convenience and security feeding into the trade-off between 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

[298] Robert Jungk, Der Atomstaat: vom Fortschritt in die Unmenschlichkeit. München: Heyne (1991); Perrow and Traube, Normale Katastrophen; Günther Anders, Über die Zerstörung des Lebens im Zeitalter der dritten industriellen Revolution. München: Verlag C.H. Beck (2002).

[299] Lewis Mumford, *Myth Of The Machine*, Bd. 2 Volumes. Harcourt Brace Jovanovich (1967) http://archive.org/details/MythOfTheMachine.

highly mobile society requires an elaborate infrastructure of data processing. As was pointed out above, such transactions produce data-trails and data-doubles that are used for social sorting and surveillance.

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.

Against the background of this trilemma, non-technical alternatives to SOSTs can be critically assessed. 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 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.

What are the consequences of this assessment for a rational approach to the security challenges evolving in modern 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.

Bibliography

Note: All references based on online articles from *newspapers and the like* quoted in this report were to be found on the Internet under the URLs provided in the footnotes at the appointed date January 5th, 2013. Since these numerous articles are referenced in the footnotes, including the URLs, they are not part of the following bibliography. This bibliography comprises all other references, e.g. monographs, anthologies, magazine articles etc.

Ackerman, Mark S., and Scott D. Mainwaring, 'Privacy issues and human–computer interaction', 2005. 381–400, in: Cranor, Lorrie and Simson Garfinkel (Ed.) *Security and Usability: Designing Secure Systems That People Can Use*. O'Reilly Media, Inc., 2007.

Adler, Emanuel, and Michael Barnett, 'A framework for the study of security communities', 1998. 29–65, in: Adler, Emanuel, and Michael Barnett *Security Communities*. Cambridge University Press, 1998.

Allmer, T., 'A critical contribution to theoretical foundations of privacy studies', *Journal of Information, Communication and Ethics in Society* 9, Nr. 2 (2011): 83–101.

Amoore, Louise, and Marieke Goede, 'Governance, risk and dataveillance in the war on terror', *Crime, Law and Social Change* 43, Nr. 2–3 (April 2005): 149–173.

Anders, Günther, *Über die Zerstörung des Lebens im Zeitalter der dritten industriellen Revolution*. München: Verlag C.H. Beck, 2002.

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

Baghai, Katayoun, 'Privacy as a Human Right: A Sociological Theory', *Sociology* 46, Nr. 5 (October 1, 2012): 951–965.

Bargh, John A., and Erin L. Williams, 'The Automaticity of Social Life', *Current directions in psychological science* 15, Nr. 1 (February 2006): 1–4.

Beck, Ulrich, 'Living in the world risk society', *Economy and Society* 35, Nr. 3 (2006): 329–345.

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

Beckett, Katherine, *Making Crime Pay: Law & Order in Contemporary American Politics*. New York: Oxford University Press, 1999.

Bellanova, Rocco, and Michael Friedewald (eds.), *D 1.1: Smart Surveillance – State of the Art*, FP7 SAPIENT Project, Brussels, 2011.

Benevolo, Leonardo, *The European City*. Hoboken, New Jersey: Wiley-Blackwell, 1995.

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

Bennett, Colin J., and Priscilla M. Regan, 'Surveillance and Mobilities,' *Surveillance & Society* 1, Nr. 4 (2002).

Bigo, Didier, Gertjan Boulet, Caspar Bowden, Sergio Carrera, Julien Jeandesboz and Amandine Scherrer, '*Fighting cyber crime and protecting privacy in the cloud*', European Parliament, 2012. http://www.europarl.europa.eu/studies.

Bilgin, Pinar, 'Identity/Security', in: *The Routledge Handbook of New Security Studies*, 81–89, 2010.

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

Borking, John, 'The use and value of privacy-enhancing technologies', 69–95, 2005, in: Lace, Susanne, (Ed.), *The Glass Consumer: Life in a Surveillance Society*. The Policy Press, 2005.

Bradley, Trevor, and Reece Walters, 'The managerialization of crime prevention and community safety', 240–259, 2002, in: McLaughlin, Eugene, Gordon Hughes, and John Muncie (Ed.) *Crime Prevention and Community Safety: New Directions*. SAGE, 2002.

Brin, David, 'Three cheers for the Surveillance Society!' 2004. http://www.salon.com/2004/08/04/mortal_gods/

Bristow, G., 'Resilient regions: re-placing regional competitiveness', *Cambridge Journal of Regions, Economy and Society* 3, Nr. 1 (2010): 153–167.

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

Burns, T. W., D. J. O'Connor, and S. M. Stocklmayer, 'Science Communication: A contemporary definition', *Public Understanding of Science* Nr. 12 (2003): 183–202.

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

Cavoukian, A., 'Privacy by design'. *Report of the Information & Privacy Commissioner Ontario, Canada* 2012.

Christie, Nils, 'Conflict as Property.' Original: *British Journal of Criminology*, 1977. 57–69, 2003.

Clarke, Roger, no date, his own website, 'While you were sleeping' http://www.rogerclarke.com/DV/

Cranor, Lorrie Faith, 'Privacy policies and privacy preferences', in: Cranor, Lorrie, and Simson Garfinkel (Ed.), *Security and Usability: Designing Secure Systems That People Can Use*. O'Reilly Media, Inc. 2007.

Demchak, Chris C., and Kurt D. Fenstermacher, 'Institutionalizing Behaviour-Based Privacy', *Administration & Society* 41: (7) (2009): 783–814.

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*. Ashgate/Dartmouth, 2000.

Domenig, Claudio, 'Restorative Justice – vom marginalen Verfahrensmodell zum integralem Lebensentwurf'. *TOA-Infodienst* Köln, 2011.

Donahue, J., N. Whittemore, and A. Heerman, *Ethical Issues of Data Surveillance*. Ethica Publishing, http://www. ethicapublishing. com/ethical/3CH20. pdf

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

Elias, Norbert, *On Civilization, Power, and Knowledge: Selected Writings*. Chicago: University of Chicago Press, 1998.

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

Ericson, Richard Victor, and Kevin D. Haggerty (Ed.), *The New Politics of Surveillance And Visibility*. University of Toronto Press, 2006.

ETICA-project, Ethical Issues of Emerging ICT Applications, Glossary, DEL 5.3. http://ethics.ccsr.cse.dmu.ac.uk/etica/deliverables

Farinosi, M., 'Deconstructing Bentham's Panopticon: The New Metaphors of Surveillance in the Web 2.0 Environment', *tripleC-Cognition, Communication, Co-operation* 9, Nr. 1 (2011): 62–76.

Feldtkeller, Andreas, *Die zweckentfremdete Stadt: Wider die Zerstörung des öffentlichen Raums*. Campus, 1994.

Ferris, J., Norman, C. and Sempik, J., 'People, Land and Sustainability: Community Gardens and the Social Dimension of Sustainable Development', *Social Policy and Administration*, 35(5) (2001): 559–568.

Flaherty; David H., Webpage: 'Presentation held at the Annual Meeting of Privacy and Data Protection Officials in Venice, 2000; Privacy Impact Assessment: an essential tool for data protection'; http://aspe.hhs.gov/datacncl/flaherty.htm

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

Frehsee, Detlev, 'Zur Abweichung der Angepassten', *Kriminologisches Journal 23,* 23 (1991): 25–45.

Frumkin, D., Wasserstrom, A., Davidson, A., and Grafit, A., 'Authentication of forensic DNA samples', *Forensic science international. Genetics*, 4 (2), (2010): 95–103.

Fuchs, Christian, Kees Boersma, Anders Albrechtslund, and Marisol Sandoval (Ed.), *Internet and Surveillance – The Challenges of Web 2.0 and Social Media*. London: Routledge, 2011.

Gandy, Oscar H., 'Consumer Protection in Cyberspace', *tripleC*: *Cognition, Communication, Co-operation*, Vol. 9, Nr. 2 (2011): 175–189.

Gandy, Oscar H., *The Panoptic Sort: a Political Economy of Personal Information*. Boulder, CO: Westview, 1993.

Gilbert, Martin, and Randolph S. Churchill, *Winston S. Churchill. Vol. 4. Companion volume. Part 1, January 1917–June 1919*. Boston: Houghton Mifflin, 1978.

Greenleaf, Graham, 'Global data privacy in a networked world', for publication in: *Research Handbook on Governance of the Internet*. Cheltenham: Edward Elgar, 2011. http://ssrn.com/abstract=1954296.

Grimston, Malcolm C., and Peter Beck, *Double or quits?: the global future of civil nuclear energy*. Sustainable Development Programme (Royal Institute of International Affairs). London: Earthscan, 2002.

Guagnin, Daniel, Leon Hempel, and Carla Ilten, 'Privacy Practices and the Claim for Accountability', in Schomberg, Rene, *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*. 2011: Luxembourg: Publication Office of the European Union., o. J.

Gürses, S. F., C. Troncoso, and C. Diaz, 'Engineering privacy by design', *Computers, Privacy & Data Protection,* 2011.

Haggerty, Kevin D., and S. Ericson, 'The surveillant assemblage', *The British Journal of Sociology* 51, Nr. 4 (2000): 701–717.

Hamm, Marion, 'Reclaim the Streets: Global Protest, Local Space'. Republicart 2002.

Hansen, L., and H. Nissenbaum, 'Digital disaster, cyber security, and the Copenhagen School', *International Studies Quarterly* 53, Nr. 4 (2009): 1155–1175.

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

Heller, Christian, *Post Privacy: prima leben ohne Privatsphäre*. München: Beck, 2011.

Hennessy, Peter (Ed.), *The new protective state: government, intelligence and terrorism*. London; New York: Continuum, 2007.

Hillmann, Karl-Heinz, *Wörterbuch der Soziologie: mit 19 Grafiken und einer Zeittafel*. Stuttgart: Kröner, 2007.

Hope, Tim, 'Community Crime Prevention', in: Tonry, Michael, *Building a Safer Society: Strategic Approaches to Crime Prevention. Crime and Justice: A Review of Research*, Volume 19: *An Annual Review of Research*. University of Chicago Press Journals, 1995).

Howard, Alex, 'Insecurity: philosophy and psychology', 58–72, in: Vail, John, Jane Wheelock, and Michael J. Hill, *Insecure times: living with insecurity in contemporary society*. London; New York: Routledge, 1999.

Howard, Ebenezer, *Garden Cities of Tomorrow*. London: S. Sonnenschein, 1902.

IRISS-project, 'Increasing Resilience in Surveillance Societies' DEL 1, 2012 '*Surveillance, fighting crime and violence Report*' http://irissproject.eu/?page_id=9

Jacobs, Jane, *The Death and Life of Great American Cities*. New York: Random House, 1993 [Original 1961].

Jasanoff, S., 'Technologies of humility: citizen participation in governing science', *Minerva* 41, Nr. 3 (2003): 223–244.

Jungk, Robert, *Der Atomstaat: vom Fortschritt in die Unmenschlichkeit*. München: Heyne, 1991.

Karat, Clare-Marie, Carolyn Brodie, and John Karat, 'Usability design and evaluation for privacy and security solutions', 2005, in: Cranor, Lorrie Faith, 'Privacy Policies and privacy preferences', in: Cranor, Lorrie, and Simson Garfinkel (Ed.) *Security and Usability: Designing Secure Systems That People Can Use*. O'Reilly Media, Inc., 2007.

Karp, D. R., and T. R. Clear, 'Community justice: A conceptual framework', *Boundary changes in criminal justice organizations* Vol. 2. (2000): 323–368.

Kaufmann, Stefan and Sabine Blum, 'Governing (In)security: The rise of resilience', 235–258, in: Gander, Hans-Helmuth et al., *Resilienz in der offenen Gesellschaft.* Baden-Baden: Nomos, 2012.

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

Kreissl, Reinhard, *Mob oder Souverän: Diskurse über die rechtliche Regulierung kollektiver Protestformen*. Leske + Budrich, 2000.

Lace, Susanne (Ed.), *The Glass Consumer: Life in a Surveillance Society*. The Policy Press, 2005.

Langheinrich, M., 'Privacy by design – principles of privacy-aware ubiquitous systems', in *Ubicomp 2001: Ubiquitous Computing*, 273–291. Zürich, 2001. http://www.springerlink.com/index/y9reah898fcuc2n8.pdf

Lederer, Scott, Jason I. Hong, Anind K. Dey, and James A. Landay, 'Five pitfalls in the design for privacy', 2005, In: Cranor, Lorrie, and Simson Garfinkel (Ed.), *Security and Usability: Designing Secure Systems That People Can Use*. O'Reilly Media, Inc., 2007.

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

Lianos, Michaelis, and Mary Douglas, 'Dangerization and the End of Deviance: The Institutional Environment', *British Journal of Criminology* 40, Nr. 2 (March 1, 2000): 261–278. doi:10.1093/bjc/40.2.261.

Liebmann, Marian, *Restorative justice: how it works*. London; Philadelphia: Jessica Kingsley Publishers, 2007.

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

Lüderssen, Klaus, and Fritz Sack, *Seminar abweichendes Verhalten II Die gesellschaftliche Reaktion auf*

Kriminalität. Frankfurt/Main: Suhrkamp, 1975.

Luhmann, Niklas, *Die Gesellschaft der Gesellschaft*. 1. Aufl. Frankfurt am Main: Suhrkamp, 1997.

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

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

MacNaughton-Smith, P., 'Der zweite Code.', o. J. in: Lüderssen, Klaus, and Fritz Sack, *Seminar abweichendes Verhalten II Die gesellschaftliche Reaktion auf Kriminalität*. Frankfurt/Main: Suhrkamp, 1975.

Marx, Gary T., *Undercover: Police Surveillance in America*. University of California Press, 1990.

Massoud Amin, S., and B. F. Wollenberg, 'Toward a smart grid: power delivery for the 21st century', *IEEE Power and Energy Magazine,* 3, Nr. 5 (2005): 34–41. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1507024.

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

Merton, Robert K., 'The Thomas Theorem and The Matthew Effect', *Special Forces* 74 (2) (1995): 379–424.

Minow, Newton N., *Safeguarding Privacy in the Fight Against Terrorism: Report of the Technology and Privacy Advisory Committee*. DIANE Publishing, o. J.

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

Moore, Barrington, *Privacy: Studies in Social and Cultural History*. M.E. Sharpe, 1984.

Morozov, Evgeny, *The net delusion: how not to liberate the world*. London: Allen Lane, 2011.

Mumford, Lewis, *Myth Of The Machine*. Bd. 2 Volumes. Harcourt Brace Jovanovich, 1967. http://archive.org/details/MythOfTheMachine

Murakami Wood, D. (ed.), Ball, K., Lyon, D., Norris, C. and Raab, C., *A Report on the Surveillance Society*. Wilmslow: Office of the Information Commissioner, 2006,

Newman, Oscar, *Defensible Space: Crime Prevention through Urban Design*. New York: Macmillan, 1972.

O'Malley, Pat, *Crime and Risk*. London et al: SAGE, 2010.

Olesen, Thomas, 'Transnational Publics: New Spaces of Social Movement Activism and the Problem of Global Long-Sightedness', *Current Sociology* 53, Nr. 3 (January 5, 2005): 419–440.

Omand, David, 'The dilemmas of using secret intelligence for public security', in: *The new protective state*, 142–169, In: Hennessy, Peter (Ed.), *The new protective state: government, intelligence and terrorism*.

London; New York: Continuum, 2007.

Owen, Taylor, 'Human Security. A Contested Contempt', in *New Security Studies*, 39–49, 2010.

Pelikan, Christa and Katrin Kremmel, ALTERNATIVES-project, '*Restorative Justice',* forthcoming 2013.

Perrow, Charles, and Klaus Traube, *Normale Katastrophen: die unvermeidlichen Risiken der Grosstechnik*. Frankfurt/Main; New York: Campus, 1992.

Phillips, David J., 'Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies', *New Media Society* Vol. 6 (6) (2004): 691–706.

Programme, United Nations Human Settlements, *Enhancing Urban Safety and Security: Global Report on Human Settlements 2007*. Earthscan, 2007.

Regan, Priscilla M., *Legislating Privacy: Technology, Social Values, and Public Policy*. Univ. of North Carolina Press, 1995.

Richards, K., 'Restorative Justice and "Empowerment": Producing and Governing Active Subjects through "Empowering" Practices', *Critical Criminology* 19, Nr. 2 (2011): 91–105.

Rose, N., and C. Novas, *Biological citizenship* (Global Assemblages, 2005), Blackwell Publishing, 2004. http://webfirstlive.lse.ac.uk/sociology/pdf/RoseandNovasBiologicalCitizenship2002.pdf

Scheingold, Stuart A., *The Politics of Law and Order: Street Crime and Public Policy*. New York: Longman, 1984.

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

Sofsky, Wolfgang, *Das Prinzip Sicherheit*. Frankfurt am Main: S. Fischer Verlag, 2005.

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

Strang, Heather, and John Braithwaite, *Restorative justice and civil society*. Cambridge UK; New York: Cambridge University Press, 2001.

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

Taylor, Nigel, *Urban Planning Theory Since 1945*. SAGE, 1998.

Tonry, Michael, *Building a Safer Society: Strategic Approaches to Crime Prevention. Crime and Justice: A Review of Research. Volume 19: An Annual Review of Research: v. 19*. University of Chicago Press Journals, 1995.

Tusicisny, Andrej, 'Security Communities and Their Values: Taking Masses Seriously', *International Political Science Review* 28, Nr. 4 (January 9, 2007): 425–449.

Tversky, Amos and Daniel Kahneman, 'The Framing of Decisions and the Psychology of Choice', *Science*, New Series, Vol. 211, No. 4481. (Jan. 30, 1981), pp. 453–458.

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

Urry, John, *Mobilities*. Cambridge, UK; Malden, MA: Polity, 2007.

Vail, John, Jane Wheelock, and Michael J. Hill, *Insecure times: living with insecurity in contemporary society*. London; New York: Routledge, 1999.

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.

Vanderveen, Gabry, *Interpreting Fear, Crime, Risk, and Unsafety: Conceptualisation and Measurement*. Boom Juridische Uitgevers, 2006.

Waever, Ole, 'Insecurity, security and asecurity', 69–118, 1998, in: Adler, Emanuel, and Michael Barnett, *Security Communities*. Cambridge University Press, 1998.

Wallman, Sandra, *The Capability of Places: Methods for Modelling Community Response to Intrusion and Change*. Pluto Press, 2011.

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.

Zedner, Lucia, *Security*. London; New York: Routledge, 2009.