European University Institute
DEPARTMENT OF LAW

EUI WORKING PAPERS

LAW 2015/39
Department of Law

SURVEILLE
Surveillance: Ethical Issues, Legal Limitations, and Efficiency

Effects and Effectiveness of Surveillance Technologies: Mapping Perceptions, Reducing Harm

Elisa Orrù

SURVEILLE

Funded by the European Union

European University Institute

Department of Law

SURVEILLE
Surveillance: Ethical Issues, Legal Limitations, and Efficiency

EFFECTS AND EFFECTIVENESS OF SURVEILLANCE TECHNOLOGIES: MAPPING PERCEPTIONS, REDUCING HARM

Elisa Orrù

EUI Working Paper **LAW** 2015/39
SURVEILLE Project
Surveillance: Ethical Issues, Legal Limitations, and Efficiency

ISSN 1725-6739

Printed in Italy
European University Institute
Badia Fiesolana
I-50014 San Domenico di Fiesole (FI)
Italy
www.eui.eu
cadmus.eui.eu

Foreword

This EUI Working Paper is based on research conducted in 2012-2015 in the FP7 project SURVEILLE. The research has earlier been reported to the European Commission in the form of what in that context is called project deliverables. Most of the deliverables have also been published on the website of the project. In order better to reach academic audiences in Europe and beyond, the EUI Law Department decided to publish selected SURVEILLE research reports also in the form of Working Papers. The current paper is one in that series.

SURVEILLE (Surveillance: Ethical Issues, Legal Limitations, and Efficiency) was a multidisciplinary project that developed a new methodology for the assessment of surveillance technologies. This methodology seeks to enable a more rational and structured process of decision-making concerning the use of surveillance technologies, as compared to abstract references to the need to find a "balance", for instance between privacy and security. The methodology developed in SURVEILLE is based on three parallel expert assessments of the use of any specific surveillance technology in a given context. The technology assessment incorporates issues of actual delivery towards a legitimate aim such as improved security, and issues of various types of financial cost. It results in a so-called usability score, based on ten different criteria. This score can be compared against a fundamental rights intrusion score that is based on expert assessments of the importance of a fundamental right (often the right to privacy or the right to the protection of personal data) in the situation at hand, and of the depth of the intrusion into that right as results from the surveillance. An independent ethics assessment will inform the holistic overall assessment and the comparison between the two scores, by indicating three different levels of moral hazard in the use of surveillance. The SURVEILLE methodology can assist legislators, policymakers, technology developers and end-users of surveillance technologies (such as the police or local authorities) in a process of rational, transparent and controlled decision-making over surveillance. The traditional legal requirements of legitimate aim, necessity and proportionality are all incorporated into the SURVEILLE methodology but in a manner that allows their operationalisation through the multidisciplinary approach of the three parallel assessments and an informed comparison of their outcomes.

In addition to developing the assessment methodology as just described, SURVEILLE generated multiple lines of academic research on technological, sociological, ethical and legal issues concerning surveillance. The current Working Paper emanates from that research.

In Florence, 30 September 2015

Martin Scheinin, Professor of International Law and Human Rights, EUI

SURVEILLE Consortium Leader

SURVEILLE - Surveillance: Ethical Issues, Legal Limitations, and Efficiency

The SURVEILLE project received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 284725, for the period 1 February 2012 to 30 June 2015.

Author's Contact Details

Elisa Orrù

University of Freiburg
Centre for Security and Society / Husserl Archive
elisa.orru@philosophie.uni-freiburg.de

Correspondence address:
Albert-Ludwigs-University Freiburg
POB 117 Platz der Universität
79098 Freiburg, Germany

+49 (0)761 203 97727

Abstract

This paper addresses issues regarding perceptions of surveillance technologies in Europe. It analyses existing studies in order to explore how perceptions of surveillance affect and are affected by the negative effects of surveillance and how perceptions and effectiveness of surveillance technologies relate to each other. The paper identifies 12 negative effects of surveillance including, among others, privacy intrusion, the chilling effect and social exclusion, and classifies them into three groups. It further illustrates the different ways in which perceptions and effectiveness of surveillance interact with each other, distinguishing between perceived security and perceived effectiveness. Finally, the paper advances a methodology to take into account perception issues when designing new surveillance technologies. By doing so, it rejects manipulative measures aiming at improving perceptions only and suggests measures that address the background conditions affecting perceptions.

Keywords

perceptions of surveillance, effects of surveillance, effectiveness of surveillance, privacy by design, minimum harm by design

Table of contents

Introduction[1]

As in the SURVEILLE project as a whole, in this paper "surveillance" refers to activities which aim at identifying hazards, typically expected to derive from human criminal conduct. This report focuses on "European" perceptions of surveillance, i.e. the way in which surveillance is regarded, understood or interpreted by European citizens in the European Union. Moreover, the report explores ways to take into account these perceptions when designing new surveillance technologies. Since there is no such thing as "the" perception of "the" European citizen, this report is not meant to provide definitive statements on "the" way Europeans perceive surveillance. However, taking European citizens as the focus of the research means assuming a particular perspective on surveillance. Beyond national, cultural and personal differences, indeed, European citizens share a number of common factors that influence their perception of surveillance: on the one hand, Europe enjoys a privileged position in the world's politics and economy; on the other, the European Union traces its political, normative framework back to the principles of democracy and the rule of law. It is from this privileged, normatively (civil and political) rights-based stance that European citizens expressed the points of view reported here.

The paper consists of two parts. The first part maps perceptions of surveillance organising them around ethical issues. The second part develops a methodology to take into account perception issues when designing new surveillance technologies.

I.

Perception issues relating to surveillance technologies can be divided into two broad categories. The first category includes negative perceptions, which in the SURVEILLE project are considered to be a cost of surveillance. The second category concerns perceived effectiveness, a desired effect of surveillance technologies.

As to negative perceptions in general, the surveys analysed allow us to conclude that a negative perception of surveillance in Europe is a significant phenomenon which, under certain circumstances, may concern up to the majority of citizens. This study identifies 12 effects and side effects of surveillance. They are connected to negative perceptions of surveillance in three ways: 1) they may be direct sources of negative perception; 2) they may derive from negative perceptions and consist of influences on people's behaviour or 3) since they may pose threats to democracy, rule of law and solidarity, they have an impact on society and may influence perceptions of surveillance negatively. The table below reports the effects and side effects for each group.

Negative-perception related effects and side effects of surveillance

Potential sources of negative perceptions:	**Potential consequences of negative perceptions:**	**Impact on society:**
Technologies perceived as threats	Self-surveillance	Control society
Security dilemma and surveillance spiral	Chilling effect	Social exclusion and discrimination

[1] The author is grateful to Sophie Arndt, Iain Cameron, Heather Draper, John Guelke, Coen van Gulijk, Katerina Hadjimatheou, Jonathan Herington, Erik Krempel, Brian McNeill, Sabine Roeser, Martin Scheinin, Sebastian Sperber and Sebastian Volkmann for their input on a previous draft of this paper and for their literature advice. As per their useful comments, she also thanks the participants to the SURVEILLE's Second Annual Forum for Decision Makers, which took place in Brussels on the 23th of September 2013.

Fear of misuse (incl. function creep)	Conformism and loss of autonomy	Social homogenisation
Fear of insufficient protection of personal data		Decline of solidarity
Fear of unlimited expansion and irreversibility		

As to the positive aspects, i.e. perceived effectiveness of surveillance, this paper identifies three ways in which perception and effectiveness relate to each other. First, there is the direct relationship between surveillance and perceived security, i.e. the question whether surveillance, independently of its actual security improvements, increases perceived security. Studies show little evidence of a causal relationship between the deployment of surveillance technologies and a reduction in fear of crime or an increase in feelings of security. It seems therefore that feelings of safety depend less on technical factors like the installation of a CCTV system and more on other elements like the actual reduction of victimisation, familiarity with people, situations and places and the presence of other people. Second, there is the relationship between actual and perceived security, i.e. the question whether an improvement in actual security brings about an increase in perceived security. The review of existing studies points out the so-called "fear of crime paradox", that is the discrepancy between the objective situation and the subjective feeling of security, more precisely: the fear of crime seems to increase or decrease independently of crime rates. Third, there is the question whether people think surveillance is effective, typically in reducing crime and reducing the fear of crime.[2] Most of the surveys consulted report that the majority of those interviewed does not think of CCTV as effective.

II.

The second part of the paper designs a methodology in order to incorporate perception issues in the development of new technologies. The proposed methodology builds on the basic assumption that interventions to address perception issues are meaningful and compatible with a non-paternalistic approach only when preceded by measures that address the background conditions affecting perceptions. As to negative perceptions, our methodology envisages three levels of intervention: Minimum Harm by Design, Transparency by Design and Accountability by Design. The first level aims to minimise the negative impact of technologies on individuals and societies, the second to make the way surveillance functions and its improvements transparent to the public and to the people affected by surveillance and finally, the third level aims to enable the misuse of technologies to be held into account and its authors to be sanctioned.

Pertaining to perceived effectiveness, the presented methodology foresees two levels of interventions: measures at the first level aim at improving effectiveness compatibly with legal, ethical and societal restraints and measures at the second aim at making success rates and improvements in effectiveness transparent to the public and to people affected by surveillance.

The part addressing negative perceptions adopts the analysis of perception-related effects and side effects of surveillance as its starting point. Its basic assumption expresses the need for individuating, addressing and, as far as possible, correcting the rationales for negative perceptions rather than simply making the particular technology or its particular use appear "better" than it is. Once the background conditions relating to negative perceptions are identified, the proposed methodology envisages three levels of intervention:

[2] As we will see, there are many ways people may think of surveillance being effective in reducing crime. They may refer to the prevention of crimes being committed through deterrence of potential offenders as well as to the identification of offenders in the prosecution phase. See section 3 of this part.

1. "Minimum harm by design" (MHbD). Implementing MHbD for surveillance technologies implies designing them in a way which makes their negative impact on individuals, on their behaviour and on society as small as possible. Although such measures overlap in part with the ones prescribed by Privacy by Design, this paper argues that it is more appropriate in this context to refer to MHbD.
2. Transparency by design (TbD). Complying with TbD requires designing technologies in a way that makes as much information as possible accessible to the public or to the people affected by surveillance.
3. Accountability by design (AbD). The claim for AbD expresses the idea that the way technologies are designed should make cases of misuse and their authors traceable, accountable and sanctionable.

The part of the methodology addressing perceived effectiveness rests upon the idea that interventions should first address the background conditions affecting perceived effectiveness and avoid measures inspired by the "security theatre". After identifying the background conditions of poorly perceived effectiveness, the proposed methodology requires designing technologies in order to achieve:

1. Higher effectiveness. This requires improving the system's effectiveness as much as possible considering legal, ethical and social restraints;
2. TbD. In order to achieve TbD for addressing perceptions of effectiveness, technologies should be designed in a way that keeps track of their operations. Combined with further information, this data on system operations should make it possible to document the success rate of the system.

For both negative perceptions and perceived effectiveness, measures at the institutional, societal and legal levels are also required in order to make design interventions fruitful.

PART I: Perceptions of surveillance in Europe

Exploring perceptions

Definitions and scope

In the SURVEILLE project, "surveillance" is defined as "targeted or systematic monitoring of persons, places, items, means of transport or flows of information, in order to detect specific, usually criminal, forms of conduct, or other hazards, and enable, typically, a preventive, protective or reactive response, or the collection of data for preparing such a response in the future".[3]

As it follows from the definition above, surveillance is defined as an activity which aims at identifying hazards, typically expected to derive from human criminal conduct. The same technologies used for surveillance purposes, however, can be, and indeed often are, used for monitoring people's actions or flows of information for purposes other than detecting criminal behaviour or even for criminal purposes. This is the case, for instance, when companies use data-analysis software for marketing, when CCTV cameras are used by employers to monitor their employees, or when a telephone tap is used to collect information in order to plan a kidnapping. These uses are not covered by the aforementioned definition of "surveillance" and, although they are not irrelevant in SURVEILLE, they are not its focus; consequently, they are not considered here.

This paper addresses issues related to the perception of surveillance, its effects and side effects.

At least two basic meanings of "perception" can be identified. They pertain respectively to 1) the phenomenon of perceiving objects with our senses: sight, hearing, touch, olfaction and taste and 2) "the way in which something is regarded, understood, or interpreted".[4] Within the context of surveillance, it is almost exclusively this second meaning that is dealt with. As we will see, perceptions of surveillance include different attitudes such as acceptance or refusal, the feeling of being safe, of being under suspicion and so on. These meanings and the way they relate to each other are explored extensively below.

Issues of perception are relevant in SURVEILLE from two points of view. On the one hand, in the technology assessment, *negative* perception is considered to be a cost of surveillance.[5] "Negative" means here a perception subjectively associated with feelings such as unease, fear, annoyance, etc., or influencing a person's attitude toward surveillance in a way that brings this attitude closer to criticism or rejection than it was previously. On the other hand, *positive* perception is to be addressed as perceived effectiveness of surveillance, which in turn, aside from actual effectiveness, is a desired effect of surveillance technologies.

The paper analyses the effects and side effects of surveillance by focusing on the relationships between them and perceptions. It identifies three groups: the first one consists of effects and side effects that may result *in* negative perception of surveillance, while the second group includes the effects and side effects that may result *from* negative perceptions (i.e. affect people's behaviour). The effects and side effects of surveillance comprised in the third group are more indirectly related to perception but are nevertheless relevant here. They have in common 1) an influence on society rather than individuals and 2) a negative impact on societal solidarity, the conditions of democracy and the

[3] Surveille Project Consortium, Description of Work of the Surveillance Project: Ethical Issues, Legal Limitations and Efficiency', internal document, p. 5.

[4] Oxford Dictionary, http://oxforddictionaries.com/definition/english/perception?q=perception, last visit August, 3rd 2015.

[5] Surveille Project Consortium, Description of Work, cit., p. 4-5.

rule of law. Although in a more reflective way than the effects previously mentioned, the latter effects may operate as rationales for negatively perceiving surveillance technologies.

The paper also investigates the complex relationship between perception and effectiveness of surveillance. First, it addresses the question whether the very deployment of surveillance technologies, independently of the level of security achieved, increases citizens' perceived security. Second, it examines the relationship between improvements in actual and perceived security. Finally, it deals with the question of perceived effectiveness in the narrow sense, i.e. whether the interviewees believe that surveillance meets its objectives.

The subjects of perception

Perception of surveillance is always situated. This means that it always presupposes not only an object but also a subject; it is always a perception *of* something *by* somebody. Moreover, the subjects do not passively receive the objects of perception, rather they actively constitute what is perceived, for they always bring their own (moral) horizons which influence the way they perceive the world.[6] SURVEILLE assumes that the subjects of perception are European citizens. Of course, it is not possible to speak in abstract and general terms of "the" perceptions of "the" European citizen. However, there are some general background conditions that are common to European citizens and which may contribute to shaping their perceptions of surveillance. To make them explicit, it is therefore necessary to contextualise the following work.

First of all, seen from a global point of view, Europeans along with the rest of the Western world share a privileged position in terms of economic wealth and political power, which has far-reaching historical roots, including European expansion into the rest of the world and its aftermath: violent conquest, colonialism, exploitation. Secondly, from an internal point of view, European societies share a normative political framework marked by the principles of democracy and the rule of law. The civil and political rights, now codified in the Charter of Fundamental Rights of the European Union, are centrepieces of this political tradition. This does not mean that authoritarian tendencies and violations of human rights are alien to Europe; on the contrary, they are as much inscribed in its history as democracy and the rule of law. But on a normative level, political action should be legitimised on the basis of the values expressed by the principles of democracy and the rule of law and those values constitute an important part of the normative background which influences European citizens' judgements about political choices.

Beyond such a common European background there are many variables that influence Europeans' perceptions of surveillance. On a national level, for instance, elements such as the history of the country (for example a past dictatorship), the level of security attained in a country, the diffusion of already existing technologies and the ways the media report surveillance-related issues influence citizens' attitudes toward surveillance. On a personal level the perception of surveillance may be influenced by factors such as gender, age, the level of information or misinformation and past experience with crime. Personal stances and opinions and the personal level of trust in a given government also shape an individual's perception of surveillance. Moreover, perception is not static and contingent factors and occurrences like a terrorist attack and its media resonance can also enormously influence people's understanding and feelings towards surveillance at a particular time.[7]

---

[6] M. Merleau-Ponty, Phénoménologie de la perception, Paris 1945, 491-492; C. Taylor, Sources of the Self. The Making of the Modern Identity, Cambridge 1989, p. 3-24.

[7] For the multiple variables influencing perception see PRESCIENT D3, Privacy, data protection and ethical issues in new and emerging technologies: Assessing citizens' concerns and knowledge of stored personal data, 2012, p. iv and 4-6, http://www.prescient-project.eu/prescient/inhalte/download/PRESCIENT_Deliverable_3_Final.pdf?WSESSIONID=4a58cf9a966a6979f5022efc190c7ee2, last access August, 3rd 2015; NG-Kruelle et al., Biometrics and e-identity (e-passport) in the European

Finally, perceived proximity to the sources of surveillance is also an important factor influencing attitudes towards surveillance: the higher one's identification with the group surveillance originates from, the easier its acceptance.[8] This is important to point out here because in SURVEILLE the focus is on European citizens' perceptions of practices typically carried out by national security agencies or by private security agencies commissioned by domestic institutions, even when, as anticipated above, the main targets of such surveillance measures often do not belong to the groups addressed by the surveys.[9]

Although in this paper I also consider studies that interview not just EU-citizens, it can be reasonably concluded from their recruitment strategy that most of those interviewed are EU-citizens. Therefore the factors mentioned above may be considered to have significantly impacted the points of view on surveillance in the surveys analysed here.

Methodology

The results presented here are based on the analysis of 22 (meta-)studies, including two reviews of several further empirical studies. The studies are listed in Annex 2. I selected them from a broader number (over 60) of *prima facie* relevant studies because they: a) also concern surveillance as defined above; b) refer at least in part to Europe; c) make their methodology transparent to the reader, or elaborate on existing studies which do the same.

Project information: SAPIENT

Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies, http://www.sapientproject.eu/

SAPIENT is a 36-months lasting project which started in February 2011. It aimed "to provide strategic knowledge on the state of the art of surveillance studies, emerging smart surveillance technologies, and the adequacy of the existing legal framework" (SAPIENT Deliverable 1.1: Smart Surveillance – State of the Art, p. ii, http://www.sapientproject.eu/docs/D1.1-State-of-the-Art-submitted-21-January-2012.pdf).

The studies are very heterogeneous in the type of questions they pose to respondents, the range of population they target and the kind of surveillance they deal with, with a significant bias for visual surveillance and CCTV in particular (for these two aspects see Annex 3). To look for univocal, definitive results that are descriptive of "European" perceptions of surveillance seems therefore to be a doomed task. This is confirmed by two recent, broad-scoped reviews of empirical studies on perceptions of surveillance in Europe, both carried out in EU FP7 programmes: SAPIENT and PRISMS (for more details on these projects see the info-boxes below).

(Contd.)

Union: End-user perspectives on the adoption of a controversial innovation, *Journal of Theoretical and Applied Commerce Research*, 1 (2006), 2, 12-35, p. 27, http://www.jtaer.com/, last access August, 3rd 2015; C. Bozzoli, C. Müller, Perceptions and attitudes following a terrorist shock: Evidence from the UK, *European Journal of Political Economy*, 27 (2011), 89-106.

[8] A. T. O' Donnel et al., Who is watching over you? The role of shared identity in perceptions of surveillance, *European Journal of Social Psychology*, 40 (2010), 135–147.

[9] On the increasing engagement of the private sector in the security domain and its implications see: L. Zedner, Security, London/New York 2009.

As a part of the review of the state of the art, the SAPIENT Deliverable 1.1 analyses existing statistical studies on citizens' perception of surveillance. In doing that, it stresses that there is no single public perception of surveillance technologies and that positions are variable, nuanced and context-dependent.10 As to the use of closed-circuit televisions (CCTVs), probably the kind of surveillance technology which the largest amount of perception studies deal with, the SAPIENT researchers state: "From reviewing existing studies dealing with the public's acceptance or resistance to CCTV surveillance, we do not find an overarching or common European set of concerns".[11]

Project information: PRISMS

PRISMS, The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making, http://prismsproject.eu/?page_id=13

PRISMS began in February 2012 and ended in July 2015. It aimed to "analyse the traditional trade-off model between privacy and security and devise a more evidence-based perspective for reconciling privacy and security, trust and concern". To this purpose it also conducted "a representative, trans-European survey, including 27,000 telephone interviews to ascertain citizens' privacy and security perceptions" (PRISMS, http://prismsproject.eu/?page_id=124).

As a preliminary study for conducting its own survey, the PRISMS Work Package (WP) 7 conducted an in-depth analysis of 20 existing statistical studies "on privacy, security, surveillance and trust with an evaluation of their reliability, shortfalls and applicability for policy-makers".[12] Also the PRISMS report on existing surveys stresses the fact that studies on people's perception of surveillance lead to contradictory findings: "In relation to public attitudes towards surveillance technologies in society, eight of the 12 surveys [considered, author's note] provide evidence that some individuals respond positively to the use of surveillance measures to help enhance their security [...]. However, our analysis illustrates that individuals' support of surveillance in the form of CCTV is somewhat contradicted by findings from other surveys".[13]

Given this background, the analysis of negative perceptions of surveillance, its effects and side effects includes the following two steps:

(a) First, the analysis bears upon the findings of two large-scale studies in order to make general statements about the percentage of people who worry about surveillance being deployed (not necessarily on themselves) and how much they worry about surveillance. Here are the questions to be addressed in this first phase: Is the negative perception of surveillance a relatively limited or a widespread matter? And just how negatively can surveillance be perceived? The aim of this part will be to give an idea of the scope of the problem in order to be able to better contextualise the results of the second phase. This is not to suggest that scope should be equated with relevance. While a widespread phenomenon can be considered relevant as such, the reverse is not true: A phenomenon could be relevant even if it affects only a small group of people. Moreover, if the group in question is a minority (racial, religious, etc.), this may make the phenomenon even more relevant.

[10] SAPIENT Deliverable 1.1: Smart Surveillance – State of the Art, 2012, p. ii, http://www.sapientproject.eu/docs/D1.1-State-of-the-Art-submitted-21-January-2012.pdf), p. 166 and 169, last access August, 3rd 2015.

[11] Ivi, p. 163.

[12] http://prismsproject.eu/?page_id=124, last access 24/7/2013.

[13] PRISMS D7.1: Report on Existing Surveys, 2013, http://prismsproject.eu/wp-content/uploads/2013/03/PRISMS-D7-1-Report-on-existing-surveys.pdf p. 135, last access August, 3rd 2015. Moreover, I find these statements to be an example of how vaguely a general thesis must be formulated in order to be able to condense the results of several surveys.

(b) Second, the study draws attention to factors that are related to perceptions of surveillance in the following ways: They can 1) affect perception negatively; 2) potentially derive from negative perceptions and result in an influence on people's behaviour; or 3) through their impact on society, operate as further rationales for negative perceptions. Here are the questions to be addressed: In which cases do people have a negative perception of surveillance? And, how can negative perception affect one's behaviour? Such analysis leads to identify and describe perception-related effects and side effects of surveillance and refers to both surveys and literature. It identifies 12 different categories of effects and side effects of surveillance.

For the part dealing with perceived effectiveness, few studies are available.

Moreover, they focus almost exclusively on CCTV and have local character, most of them having been carried out in cities. This is consistent with the character of the crimes the installed CCTV systems are supposed to reduce, which are also local in character (theft, burglary, etc.).

Negative effects of surveillance

Negative perception: the dimension of the phenomenon

To address the first cluster of issues, I consider those studies to be adequate which: a) Like the other studies considered here, apply to surveillance as defined in SURVEILLE; b) have a large number of respondents involved as opposed to a small sample; c) carry out interviews in a significant number of European countries and d) carry out the studies on the basis of a clear, transparent and rigorous methodology.[14] Although I present the main results of those studies, I use them only to give a rough idea of the dimension of the phenomenon and not to further calculate averages and percentages based on their results.

Only two studies meet the aforementioned criteria: URBAN EYE and Flash EUROBAROMETER 225 (hereafter just EUROBAROMETER 225, for more details on both projects see the info-boxes below). Out of the six broad surveillance-areas that can be identified (visual surveillance, dataveillance, biometrics, communication surveillance, sensors and location determination technologies),[15] the URBAN EYE and EUROBAROMETER 225 studies cover only three: visual surveillance (URBAN EYE), dataveillance and communication surveillance (EUROBAROMETER 225). This deficit might be overcome by the PRISMS survey, whose results have been only partially published so far.[16]

Project information: URBAN EYE

http://www.urbaneye.net

The URBAN EYE project started in September 2001 and ended in June 2004. It took an interdisciplinary perspective to study the expansion, deployment, social impact and political implications of CCTV in seven European countries: Austria, Denmark, Germany, Great Britain, Hungary, Norway and Spain. It focused on "CCTV surveillance in both public areas and private but publicly accessible spaces such as shopping malls or railway stations" (Hempel, L., Töpfer, E.: URBAN EYE Working Paper n. 15: CCTV in Europe, Final Report, p. 10). In order to investigate the social implications of CCTV, in 2003 the research team conducted street interviews with 1000 citizens in Berlin, Budapest, London, Oslo and Vienna. The interviews were based on standardized questionnaires. In addition, the URBAN EYE team conducted in-depth interviews with 30 respondents.

Although the authors of the URBAN EYE final report warn: "our findings are in formal methodological terms neither strictly representative nor comparable",[17] the main findings of the interviews may be tentatively summarised as follows.

As to the acceptance of CCTV, attitudes differ considerably depending on where the CCTV is placed and the city where the interview is carried out. At a minimum, 4.3% of respondents find CCTV in banks to be a "bad thing", while disapproval is highest regarding CCTVs placed in clothing store fitting rooms (73% of respondents). As to CCTVs in general, the largest number of people who have critical attitudes are in Vienna (41% of respondents), while

[14] The assessment of this last point also relies on the analysis carried out in PRISMS, for both of the selected studies are also considered in PRISMS.

[15] SAPIENT D1.1, cit., p. 23

[16] As of August, 3rd 2015.

[17] L. Hempel, E. Töpfer, URBAN EYE WP 15: CCTV in Europe, Final Report, 2004, p. 1, http://www.urbaneye.net/results/ue_wp15.pdf. Last access: August, 3rd 2015.

the smallest number is reported in London (4% of respondents). As to risks connected to CCTV, 53% of respondents agree that "CCTV footage can be easily misused"[18] and 40% "believe that CCTV invades privacy".[19]

According to the EUROBAROMETER 225, a majority of citizens are concerned about privacy when their personal data are held by organisations (64% of respondents). More than one third (34%) of respondents are very concerned. Such results, however, do not distinguish between the different types of organisations that can hold citizens' data and also relate to organisations that have nothing to do with surveillance. However, the study also provides specific information about police and local authorities, two organisations that also handle citizens' data for surveillance purposes. As to the police, there is a European average of 17% of respondents who do not trust them handling their personal data. This study, like the URBAN EYE survey, shows a considerable diversity of results among the European countries. For instance, in Finland only 5% of respondents do not trust the police to handle their personal data, whereas in Lithuania the rate of mistrust reaches 49% of respondents. A European average of 29% of respondents do not trust local authorities to hold their data, with a minimum in Denmark (10%) and a peak in Lithuania (52%). As to communication surveillance, a European average of 19% of respondents would not accept, under any circumstances, monitoring internet usage to combat terrorism and 25% of respondents would not accept, under any circumstances, monitoring telephone calls for the same purpose.

Project information: EUROBAROMETER 225

http://ec.europa.eu/public_opinion/index_en.htm

The **Eurobarometer** surveys are conducted on behalf of the European Commission to monitor attitudes and perceptions of European citizens on a wide range of topics. EUROBAROMETER 225 was conducted in 2008 and consists of interviews mainly carried out via landline-telephones. The interviews cover all the 27 member states and include about 1000 citizens from each state. The focus of the survey is on data protection, data privacy and data security but do not relate exclusively to surveillance.

As we have seen, the results of both the URBAN EYE and the EUROBAROMETER 225 survey can be used here only with caution and should not be generalized. With regard to the former, the findings are admittedly not representative and with regard to the second, the focus of the surveys is not on surveillance. Moreover, the percentage of citizens who have a negative perception of surveillance (in the form of or depending on non-acceptance, mistrust of the surveillors, or privacy-intrusion) varies considerably depending on the context of deployment and the country of provenience. However, the results presented above seem to provide a sufficient basis to formulate the following, quite modest but sufficient for our purposes, conclusion:

Negative perception of surveillance in Europe is not a marginal phenomenon. Under certain circumstances it may concern up to the majority of citizens.[20] A considerable number of them may perceive surveillance in a *very* negative way.

Negative-perception related effects and side effects of surveillance

This enquiry refers to both small-scale studies and literature. Studies are considered that: a) relate at least in part to "surveillance" as defined in SURVEILLE and b) involve at least one European country.

The relevant effects and side effects of surveillance that emerge from the studies are related to negative perception in three ways: 1) they may be direct sources of negative perceptions; 2) they may

[18] Ivi, p. 45.

[19] Ibidem.

[20] I am not considering cases here in which the rate of citizens perceiving surveillance negatively is higher because they refer to situations that are too specific (i.e. the use of CCTV in fitting rooms) to be generalisable.

derive from negative perceptions and consist of influences on people's behaviour or 3) their impact on society may influence the perception of surveillance negatively.

The 12 types of effects and side effects of surveillance are summarised in Annex 1, organised accordingly to the group they belong to.

Potential sources of negative perceptions

(a) Surveillance technologies being perceived as threats/harassments themselves

This side effect of surveillance concerns the fact that surveillance technologies can make people feel uncomfortable even when perceived as being used properly, i.e. in conformity with the stated goals and legal requirements.

This has to do with the fact that "surveillance technologies may interfere with various aspects of people's lives" and may be perceived as restricting people's privacy and freedom of movement.[21]

Examples of this kind of side effect are reported, among others, in the study BIOMETRICS AND E-IDENTITY with regard to the proposed introduction of e-passports and in the URBAN EYE project regarding CCTV.[22] In both surveys, the deployment of surveillance is felt as an invasion of privacy.

A slightly different variant of this side effect which surveillance may cause has to do with the feeling of being "under suspicion". On the one hand, surveillance can make people feel like a suspect *a priori*, for they may be and often are surveilled without having previously shown any "dangerous" behaviour. On the other hand, as reported by the PRISE Project,[23] surveillance may make surveilled persons afraid of confirming such prejudice and being classified as "dangerous" by authorities. This time it is not on the basis of a general "presumption of guiltiness", but as a consequence of their behaviour, as it is difficult to know in advance which behaviour could be classified as suspect.[24]

(b) Security dilemma and surveillance spiral

The security dilemma consists of security technologies increasing people's feelings of insecurity rather than making them feel safer. This may happen in two ways.

First, "the usage of surveillance technologies […] may have the effect of (over-) sensitizing people to the perception of threats and just making them feel unsafe: «The more these security strategies take effect, the greater the sensitivity to the continuing lack of security, the remaining risks and to the fact that threats have not disappeared by far»".[25] This phenomenon may take many forms, result in diffused sensitivity involving society as a whole or manifest itself in very specific circumstances. In

[21] SURVEILLE D3.1, Report describing the design of the research apparatus for the

European level study of perceptions, 2012, http://surveille.eui.eu/wp-content/uploads/2015/04/D3.1-Report-describing-the-design-of-the-research-apparatus.pdf, last access August, 3rd 2015, p. 14.

[22] NG-Kruelle et al., Biometrics and e-identity, cit., p. 21 and L. Hempel, E. Töpfer, URBAN EYE WP 15, cit., p. 8. See also M. Gill et al., Public perceptions of CCTV in residential areas: "It is not as good as we thought it would be", *International Criminal Justice Review*, 17(2007), 304-324, p. 321.

[23] PRISE ("Privacy enhancing shaping of security research and technology", http://www.prise.oeaw.ac.at/index.htm).

[24] V. Pavone, M. Pereira, The privacy vs. security dilemma in a risk society. Insights from the PRISE project on the public perception of new security technologies in Spain, 2008, http://www.wiscnetwork.org/ljubljana2008/papers/WISC_2008-110.pdf, p. 22, last access August 3rd 2015.

[25] SURVEILLE D3.1, cit., p. 15; quote from H. Münkler, Strategien der Sicherung. Welten der Sicherheit und Kulturen des Risikos. Theoretische Perspektiven, in H. Münkler, M. Bohlender, S. Meurer (eds.): Sicherheit und Risiko. Über den Umgang mit Gefahr im 21. Jahrhundert, Bielefeld 2010, 11-34, p. 12-13: „Je besser diese Strategien der Sicherung greifen, desto stärker wird die Sensibilität für die fortbestehende Unsicherheit, für immer noch vorhandene und noch längst nicht verschwundene Bedrohungen."

this restricted form it may manifest itself, for instance, when the fear of crime diminishes in the places where CCTVs were installed but increases in places where there is no video surveillance.[26] Studies carried out in the UK and in Germany also report that people worry more about crime when a CCTV system is installed, possibly because the presence of cameras makes the places seem more dangerous than otherwise.[27]

Second, those very surveillance technologies may be perceived as sources of new risks. For instance, the very fact that there are people surveilling others gives rise to the risk of misuse by the surveillance operators,[28] or the very deployment of surveillance (in combination with repressive migration laws) at borders may increase the risk of death or injury during attempts to cross these borders.

In both cases this may lead to a further side effect of surveillance: in order to compensate for increasing insecurity, more surveillance is required, which in turn may further increase insecurity. As a result, a sort of surveillance spiral is triggered.[29]

(c) Fear of misuse, including function creep

The fear of the misuse of surveillance is somehow related to the former, since this too may be derived from a perceived lack of control of or mistrust of the operators.

The Synthesis Report of the PRISE Project deals with such a phenomenon in its generality, affirming that "more than 60 percent of the participants in the six countries [where the survey was carried out, author's note] believe that new security technologies are likely to be abused by governmental agencies".[30] The URBAN EYE report also shows similar findings telling that 50% of respondents believe that "footage can be easily misused".[31] The report BIOMETRICS AND E-IDENTITY also refers to the perceived risk of abuse of personal information made available for e-passports[32].

A specific kind of misuse of surveillance known as "function creep" occurs when the use of a technology expands gradually beyond its original scope and purpose. Examples of function creep include: drones developed for military purposes used in civilian contexts to observe public assemblies, demonstrations and other public events;[33] CCTVs installed in the retail sector for the purpose of

---

[26] Chen-Yu Lin, Öffentliche Videoüberwachung in den USA, Großbritannien und Deutschland – Ein Drei-Länder-Vergleich, 2006, http://ediss.uni-goettingen.de/bitstream/handle/11858/00-1735-0000-0006-B3C4-7/lin.pdf?sequence=1, last visit August, 3rd 2015 p. 87-88.

[27] D. Williams, J. Ahmed, The Relationship Between Antisocial Stereotypes and Public CCTV Systems: Exploring Fear of Crime in the Modern Surveillance Society, 2009, https://uhra.herts.ac.uk/dspace/bitstream/2299/4794/1/903645.pdf, last access 24/7/2013; N. Zurawski, „It is all about perceptions': CCTV, feelings of safety and perceptions of space - what the people say", *Security Journal*, 23 (2010), 259-275.

[28] C. Ketzer, Securitas ex Machina. Von der Bedeutung technischer Kontroll- und Überwachungssysteme für Gesellschaft und Pädagogik, 2005, http://kups.ub.uni-koeln.de/1861/, last access August, 3rd 2015, p. 36.

[29] Jonathan Herington also points out: "In surveillance the actions of the government to prevent terrorism (i.e. by surveilling email) are often interpreted by targeted communities as suspicious, so they respond defensively (by using Lavabit), which is then interpreted by the government as suspicious, so they take steps to counter (i.e. by shutting down Lavabit), and so on...", Jonathan Herrington, personal comment on this paper.

[30] PRISE D5.8, Synthesis Report - Interview Meetings on Security Technology and Privacy, 2008, http://www.prise.oeaw.ac.at/docs/PRISE_D_5.8_Synthesis_report.pdf, last access August, 3rd 2015, p. 25.

[31] L. Hempel, E. Töpfer, URBAN EYE WP 15, cit., p. 8.

[32] NG-Kruelle et al., Biometrics and e-identity, cit., p. 21. For a general reference to function creep see also PACT Summary of PACT Deliverables D1.1 - D1.6, 2012, http://www.projectpact.eu/documents-1/privacy-security-research-paper-series/%233_Privacy_and_Security_Research_Paper_Series.pdf, August, 3rd 2015, p. 94.

[33] SURVEILLE D3.1, cit., where it is also brought up that: "this phenomenon is sometimes given another name. Daniel Solove, for example, uses the concept of «secondary use» in his essay «I've got nothing to hide and other misunderstandings of privacy»: «Secondary use is the use of data obtained for one purpose for a different unrelated purpose without the person's consent», s. D. J. Solove, I've got nothing to hide and other misunderstandings of privacy, *San Diego Law Review*, 44 (2007), 745-772, p. 767.

preventing theft subsequently being used to monitor employees[34] or for voyeurism;[35] CCTV originally intended to monitor traffic used for observing "social fringe groups";[36] dataveillance technologies developed in democratic states and then sold to authoritarian regimes to oppress political opponents.[37]

(d) Fear of insufficient protection of personal data

Similar to the previous effect but still different is the fear that personal data collected through surveillance may be not sufficiently protected from other people or organisations accessing them. Although this effect may also derive from mistrust of the operators, it differs from the previously discussed effect because it does not concern the fear of a potential misuse by the operators; rather, it relates to their possible carelessness in allowing third parties access to the information held by them. The study BIOMETRICS AND E-IDENTITY reports this side effect, referring to respondents worrying about possible illegal access to biometric information held by authorities for producing e-passports.[38]

(e) Fear of unlimited expansion and irreversibility of surveillance

A last side effect of surveillance that may influence people's perception negatively has to do with the feeling that some protective barriers are falling away once surveillance technologies are introduced.

This may happen in two ways.

First, while the initial introduction of a particular technology may put up with resistance, it is much easier to expand its use after overcoming initial opposition. This is distinct from function creep because there must not necessarily be a change in the function for which the technologies are used. This aspect is mentioned in the PACT report "Privacy and Security".[39]

Second, as reported by the PRISE project, there is the feeling that once a technology has been introduced it will be almost impossible to make it disappear again, even if it emerges that the technology is misused, ineffective, unnecessary or dangerous.[40]

Potential consequences of negative perception: self-normalization and influences on behaviour

We shall now turn to the effects of surveillance that, potentially deriving from negative perceptions, result in a modification of people's behaviour.

(a) Self-surveillance

A common basis of these effects can be traced back to self-surveillance as the mechanism that links negative perception and behaviour. The concept of self-surveillance has been developed by Michael Foucault[41] and is described by Daniel Solove as follows: "by always being visible, by constantly living under the reality that one could be observed at any time, people assimilate the effects of surveillance into themselves. They obey not because they are monitored but because of their fear that they could be

---

[34] W. Peissl et al., Aktuelle datenschutzrechtliche Fragen der Videoüberwachung, 2011, <http://epub.oeaw.ac.at/ita/ita-projektberichte/d2-2a58.pdf>, last access August, 3rd 2015, p. 5.

[35] Chen-Yu Lin, Öffentliche Videoüberwachung, cit., p. 84.

[36] EPTA, ICT and Privacy in Europe. Experiences from technology assessment of ICT and Privacy in seven different European countries, 2006, http://www.ta-swiss.ch/publikationen/2006/, last access August, 3rd 2015, p. 36.

[37] This was for instance the case of Siemens Nokia selling technologies to the Iranian regime, s. PACT Summary of PACT deliverables D1.1 - D1.6, cit., p. 85.

[38] NG-Kruelle et al., Biometrics and e-identity, cit., p. 21.

[39] PACT Summary of PACT deliverables D1.1 - D1.6, cit., p. 95. The pact report, however, does not rigorously distinguish such phenomenon from function creep.

[40] PRISE D5.8, Synthesis Report - Interview Meetings on Security Technology and Privacy, cit., p. 24.

[41] M. Foucault, Surveiller et punir. Naissance de la prison, Paris 1975.

watched. This fear alone is sufficient to achieve control."[42] Surveillance need not actually take place: the possibility of being surveilled is already enough to bring about obedience.

This phenomenon is also known to psychologists, who stress that the feeling of being continuously watched can bring about changes in the psyche of the observed, who becomes "more circumspect, timorous and suspicious".[43]

(b) Chilling effect

The chilling effect is defined as "the disinclination to take part in certain activities which liberal theory considers entirely legitimate, such as free association, free speech and political organisation. If one worries that such behaviour is punishable in any way, or that it draws unwanted attention to oneself on the part of authorities, one is subject to [it, author's note]".[44] Moreover, for fear of "doing wrong", people can also withhold from helping people in need. In the words of Nils Zurawski: "people abdicate from their responsibility as soon as a camera is recording. Interviews, for example, have shown that some people are afraid of doing wrong when helping someone. Thus, they preferred not to help when under surveillance."[45]

(c) Conformism and loss of autonomy

Besides refraining from engaging in some public activities, people may also develop a tendency to conform as a consequence of surveillance. This derives from the feeling of being "under suspicion" described above: if people know that any movement, any word might be recorded and considered "suspect", they may try to avoid any "deviant" behaviour in order to avoid attracting attention.[46]

Seen from another point of view, this side effect may be described as a loss of autonomy: people under surveillance do not behave in accordance with their "own" reasons but rather in accordance with what they think they are supposed to do in order not to be sorted out as "deviant".[47]

Effects of surveillance on society

There is a third group of effects and side effects of surveillance which affect society as a whole rather than individuals. Its common characteristic is the restrictive impact on the background conditions and basic principles of democracy, rule of law and solidarity.

Thereafter they may influence people's perceptions of surveillance negatively, although in a more reflective way than the effects listed above, for the negative perception derives here from the knowledge of the impact such technologies may have on our societies.

For the description of such effects we rely more on literature than on surveys. This derives from the societal character of the effects listed here. Since they do not directly impact individuals, they are seldom mentioned in interviews asking about citizens' perceptions of surveillance (as opposed to effects affecting individuals more immediately, like the ones listed above). As a consequence, their description is based more on scholars' elaborations than on survey results.

---

[42] D. J. Solove, The Digital Person. Technology and Privacy in the Information Age, New York 2004, p. 31.

[43] Chen-Yu Lin, Öffentliche Videoüberwachung, cit., p. 82.

[44] DETECTER D 12.2.1, Quarterly Update on Technology 1, 2009, http://www.detecter.eu/index.php?option=com_content&view=section&id=7&layout=blog&Itemid=9, last access August, 3rd 2015, p. 4.

[45] N. Zurawaski: Kameras lösen keine Probleme, ZEITonline, Available at: http://www.zeit.de/gesellschaft/schule/2011-11/schule-kamera-zurawski, last visit August, 3rd 2015; as quoted in SURVEILLE D3.1, cit., p. 15.

[46] W. Peissl, et al., Aktuelle datenschutzrechtliche Fragen, cit., p. 10 and F. Helten, B. Fischer, Urban Eye WP 13, What do people think of CCTV. Findings from a Berlin Survey, 2004, http://www.urbaneye.net/results/ue_wp13.pdf, last access August, 3rd 2015.

[47] W. Peissl, Surveillance and Security. A Dodgy Relationship, 2002, http://www.oeaw.ac.at/ita/pdf/ita_02_02.pdf, last access August, 3rd 2015, p. 8-9.

(a) Control Society: Reversing the presumption of innocence

According to Gilles Deleuze, from the beginning of the Nineties Western societies were developing from disciplinary societies into "control societies".[48] In such a society, different but interrelated mechanisms provide the possibility for a short-term, quick-response, continuous and unlimited control over individuals. As examples of such mechanisms, Deleuze mentions locating technologies that make information available on people's positions in open spaces at any time.

Clive Norris and Gary Armstrong have elaborated on Deleuze's interpretation. In their view, in control societies, the maximisation of control over citizens is justified as a means to prevent as many offences as possible. Such an ambition of control societies to prevent offences from being committed requires a further critical change: instead of being considered innocent until proven guilty, "everyone is assumed guilty until the risk profile assumes otherwise".[49] These authors refer to the right to be presumed innocent in a broad, moral meaning rather than in a strictly legal way. As such, it may be understood as the right to be treated as trustworthy.[50]

The maximisation of control and the reversion of the presumption of innocence have an impact on the way security is perceived in society, suggesting that everybody is a potential risk.[51]

(b) Social exclusion and discrimination

The risk of social exclusion brought about by surveillance is reported often in the literature, particularly in relation to visual surveillance. It is argued that visual surveillance promotes the application of categorical suspicion: controllers tend to equate whole social categories, sorted out on the basis of appearance and visible traits such as colour, clothing, etc., with dangerous groups. This strengthens prejudices because it seems to confirm them, thus amplifying social exclusion.[52] Social sorting, i.e. the activity of sorting groups of people from others in order to treat them differently, is indeed one of the main functions of contemporary surveillance according to David Lyon.[53]

Although this risk is evident for visual surveillance, it may affect other kinds of surveillance as well because it may occur at any time that collected data may be used to categorise people on the basis of their supposed risk potential. Digital data collected through dataveillance, for example, may lead to creating a false, high-risk profile that may, in turn, influence one's chances of finding a job, thereby strengthening prejudices and social exclusion.[54]

Studies indicate also that visual surveillance in particular may have the effect of keeping particular social groups away from places where their presence is perceived by other people as disturbing. This is the case for instance of homeless or poor people and punks in shopping malls, exclusive holiday resorts or city centres.[55] Even though the studies do not explicitly describe how this effect comes

---

[48] G. Deleuze, Post-scriptum sur les sociétés de contrôle, *L'autre journal*, 1, Mai 1990. See also D. Kammerer, Bilder der Überwachung, Frankfurt am Main 2008, p. 131-142.

[49] C. Norris, G. Armstrong, The maximum surveillance society, 1999, p. 24.

[50] See SURVEILLE D4.5: Paper on the ethical risks of surveillance technologies in prevention, investigation, and prosecution of crime.

[51] PACT Summary of PACT deliverables D1.1 - D1.6, cit., p. 95.

[52] L. Hempel, E. Töpfer, URBAN EYE WP 15, cit., p.7; Chen-Yu Lin, Öffentliche Videoüberwachung, cit., p. 79 ff.; PACT Summary of PACT deliverables D1.1 - D1.6, cit., p. 94-95; M. Apelt, N. Möllers, Wie intelligente" Videoüberwachung erforschen? Ein Resümee aus zehn Jahren Forschung zu Videoüberwachung, *Zeitschrift für Außen- und Sicherheitspolitik* (2011), 4, 585–593, p. 590; D. Williams, J. Ahmed, The Relationship, cit. See also T. G.Patel, Surveillance, Suspicion and Stigma: Brown Bodies in a Terror-panic Climate, *Surveillance&Society*, 10 (2012), 3/4, 215-234.

[53] D. Lyon (ed.), Surveillance as social sorting: privacy, risk, and digital discrimination, London 2003.

[54] W. Peissl et al., Aktuelle datenschutzrechtliche Fragen, cit., p. 10.

[55] L. Hempel, E. Töpfer, The Surveillance Consensus: Reviewing the Politics of CCTV in Three European Countries, *European Journal of Criminology*, 6 (2009), 2, 157-177.

about, it may happen in two ways: either through operators directly intervening and forcing people to leave, or because the very feeling of being targeted by surveillance can be enough to make "undesired" people keep away. Such effect, at least when caused by the operators' intervention, contrasts clearly with the principle of non-discrimination, as sanctioned among others in the Charter of Fundamental Rights of the European Union.[56]

(c) Social homogenisation

This effect of surveillance derives directly from the influences on individuals' behaviour described above: the chilling effect and conformism. In the view of Daniel Solove: "Chilling effects harm society because, among other things, they reduce the range of viewpoints expressed and the degree of freedom with which to engage in political activity."[57]

At the same time, conformism may lead to societal stagnation, since deviant and dissenting behaviour is considered to be an important driving force for societal change.[58]

Both effects can impact democratic life and impede it from developing and flourishing.

(d) Decline of solidarity

This last effect of surveillance is also directly related to surveillance's influence on people's behaviour, in particular to the chilling effect described above.

I have already mentioned the fact that people may abstain from helping others when under surveillance because of being afraid to make mistakes. But beyond that, surveillance technologies may also induce people to delegate their responsibilities towards others to such technologies: "people no longer feel responsible for their fellow citizens as soon as surveillance technologies are installed. In other words: The fact that people tend to rely absolutely on surveillance technologies may lead to a decline in mutual responsibility and a lack of moral courage which may have serious consequences for the way people live together in a society".[59]

[56] Art. 21.

[57] J. D. Solove, The Digital Person, cit., p. 31, as quoted in SURVEILLE D3.1, cit. Both the chilling effect and its societal impact are also reported in W. Peissl et al., Aktuelle datenschutzrechtliche Fragen, cit., p 10-11.

[58] W. Peissl, Surveillance and Security, cit., p.8.

[59] SURVEILLE D3.1, cit.; Chen-Yu Lin, Öffentliche Videoüberwachung, cit., p. 75; S. Graham et al., Towns on the Television: Closed Circuit TV Surveillance in British towns and cities, 1995, Working Paper No. 50, University of Newcastle upon Tyne, http://www.ncl.ac.uk/guru/assets/documents/ewp17.pdf, last access August, 3rd 2015; J. Ditton, Crime an the city. Public Attitudes towards Open-Street CCTV in Glasgow, *The British Journal of Criminology*, 40 (2000) 4, 692-709, p. 707.

Effectiveness and perceptions

The relationship between perceptions and effectiveness

Tackling the question of the perceived effectiveness of surveillance technologies is a complex task. Intuitively, one might assume that the perceived and the actual effectiveness of surveillance are related, yet the very existence of such a relationship is controversial. Even if we assume its existence, it is neither unequivocal nor easy to understand.

Perceived effectiveness refers quite obviously to the question whether people think surveillance achieves the aims it is deployed for. But these differ from one technology to another, often remain implicit or are imprecisely formulated.[60] As a consequence, it is likely that people do not know the exact purposes surveillance technologies are deployed for, so the way they perceive the effectiveness of such technologies may be accordingly distorted. As we will see, most of the studies that tackle this matter consider reduction of crime and reduction of fear of crime to be the purposes of surveillance and ask people if they think surveillance technologies achieve these aims.

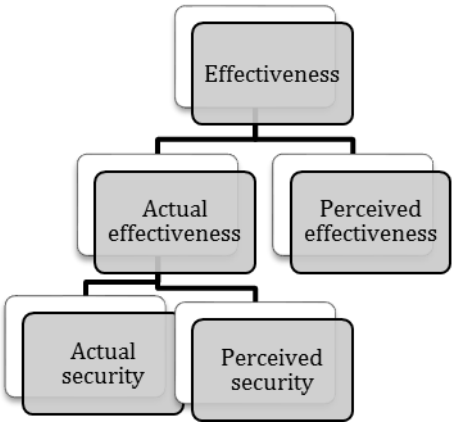
Moreover, the expression "perceived" effectiveness is somehow misleading, for it suggests that there is a subjective, variable effectiveness opposed to an "actual" effectiveness which is objective, impersonal and fact-based. This is however not the case because reducing the fear of crime or, more positively yet less precisely formulated, increasing feelings of safety are just as common priorities of surveillance as reducing crime or increasing security.[61] Actual effectiveness, therefore, has to do with perceptions and feelings too: both *actual security* (crime reduction/security improvement) and *perceived security* (reduction of fear of crime/ increase of the feeling of safety) are aspects of actual effectiveness.[62] Furthermore, as shown in the SURVEILLE Deliverable 3.4, beyond the perceptive component of effectiveness, there is currently no objective, impersonal and fact based definition of effectiveness available for surveillance technologies.

---

[60] The difficulties related to the task of assessing the effectiveness of surveillance technologies are explored in more detail in D3.4 „Design of research methodology for assessing effectiveness of selected representative surveillance systems",http://surveille.eui.eu/wp-content/uploads/2015/04/D3.4-Design-of-a-research-methodology-for-assessing.pdf, last visit August 3rd 2015.

[61] The latter is a less precise formulation than the negative one because feelings of "safety" may also include economic and social aspects which are beyond the aims of surveillance. The literature does not distinguish unequivocally and rigorously between "safety feeling" and "security feeling", so both expressions are used to refer to the same phenomenon. Although attempts to clarify the meaning of "safety" have been made (see N. Möller at al., Safety is More than the Antonym of Risk, *Journal of Applied Philosophy*, 23 (2006), 4, 419-432 and N. Möller, The Concepts of Risk and Safety, in S. Roeser, R. Hillerbrand, P. Sandin, M. Peterson (Eds.), The Handbook of Risk Theory, Epistemology, Decision Theory, Ethics, and Social Implications of Risk, Dordrecht etc. 2012) more research is needed here. This is however a task beyond the scope of this paper. This paper adopts the expression "safety feeling", except when quoting from authors doing otherwise.

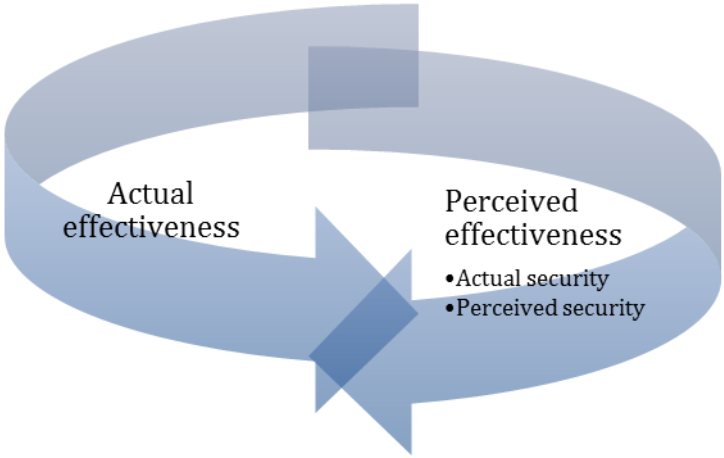
[62] PACT D1.4 Societal Impact Report, 2012, http://www.projectpact.eu/deliverables/wp1-root-branch-review/d1.4-social-impact-report, last access August 3rd 2015, p. 16.



Perceptions and effectiveness

But the matter is even more complicated, and the relationship between actual and perceived effectiveness is in part a circular one. Let us illustrate this with an example. In a parking area a CCTV system is installed in order to reduce crime (say, theft of or from vehicles and assault) and to make car users feel safer when they park there. If CCTV park users actually feel safer after the installation than before, just because they see the cameras, this may indicate that CCTV *is* effective in this respect because it achieved the goal of making people feel safer. But they may also feel safer *because they think that since the installation of CCTV crime rates in the parking area have decreased*, independently of whether they actually did or not. In this case, the increased feeling of safety may indicate that CCTV *is perceived* to be effective. So the feeling of safety can relate both to actual effectiveness (as perceived security) and to perceived effectiveness.

The picture below illustrates the overlap and interaction between the two aspects of effectiveness.



Actual and perceived effectiveness – Interaction and overlap

To sum up, although the distinction between perceived and actual effectiveness is methodologically useful and is employed in this paper, two caveats should be kept in mind: 1) despite what the expressions "perceived effectiveness" and "actual effectiveness" may suggest, perception issues are part of both actual and perceived effectiveness; 2) a clear distinction between the two is not always possible nor does authentically describe the complex role perception plays in matters related to effectiveness.

Perception aspects of effectiveness

As we have seen, the effectiveness of surveillance technologies encompasses perception-related aspects as well: surveillance technologies are effective if they increase perceived security, i.e. if they increase feelings of safety or reduce fear of crime.

The matter is twofold: on the one hand, it involves the direct relationship between surveillance and perceived security, i.e. the question whether surveillance, independently of its actual security improvements, increases perceived security; on the other hand, it refers to the relationship between actual and perceived security, i.e. to the question whether an improvement in actual security brings about an increase in perceived security.

The two points are not identical, as it is not obvious that the deployment of surveillance technologies increases actual security. Tackling such matters is beyond the scope of this paper, so it will be enough here to quickly recall that the results of several studies challenge the assumption that surveillance improves actual security.[63]

The fact that surveillance does not necessarily bring about an increase in actual security and that perceived and actual security often do not overlap opens up the possibility for what is called the "security theatre". This "covers measures taken, ostensibly in the name of security, whose value lies solely (or at least mostly) in their capacity to give the reassuring impression that *something is being done*, that *steps are being taken*, that *someone is on the case*—rather than in actually increasing security, considered from an objective standpoint. The role of security theatre is to increase *perceived* security, without necessarily having any positive effect in terms of *actual* security".[64]

Surveillance and perceived security

Does the deployment of surveillance technologies *per se* bring about an improvement in perceived security? Studies show little evidence of a causal relationship between the deployment of surveillance technologies and a reduction in fear of crime or an increase in security feelings.

A first group of studies finds little evidence and limited change to have occurred after the installation of CCTV. The URBAN EYE report and a study carried out in the German city of Regensburg, for instance, report that only a minority of those interviewed affirms to feel safer since CCTV systems have been installed.[65]

A second group of studies finds that in some cases the installation of CCTV *negatively* influences citizens' perceived security. In a study carried out in Glasgow, for instance, the percentage of those

[63] B. C. Welsh, D. P. Farrington, Home Office Research Study 252, Crime prevention effects of closed circuit television: a systematic review, 2002, http://www.popcenter.org/Responses/video_surveillance/PDFs/Welsh&Farrington_2002.pdf, last access August, 3rd 2015; and M. Gill, A. Spriggs, Assessing the impact of CCTV, Home Office Research Study 292, 2005, https://www.cctvusergroup.com/downloads/file/Martin%20gill.pdf, last access August 3rd 2015. However, few studies are available on this topic and the matter is complicated by the fact that there is no clear methodology for assessing the effectiveness of surveillance technologies. See SURVEILLE D3.4, Design a research methodology for assessing the effectiveness of selected surveillance systems in delivering improved security, September 2013, <http://surveille.eui.eu/wp-content/uploads/2015/04/D3.4-Design-of-a-research-methodology-for-assessing.pdf >, last access August 3rd 2015.

[64] PACT D1.4 Societal Impact Report, cit., p. 16.

[65] F. Helten, B. Fischer, Urban Eye WP 13, What do people think of CCTV, cit.; G. Klocke et al., Das Hintertürchen des Nichtwissens, *Bürgerrechte & Polizei*: CILIP, 69 (2001) 2, http://www.cilip.de/ausgabe/69/video.htm, last access August 3rd 2015; Chen-Yu Lin, Öffentliche Videoüberwachung, cit., p. 77; M. Apelt, N. Möllers, Wie intelligente" Videoüberwachung, cit. See also Brown, B., CCTV in Town Centres: Three case studies, Police Research Group. Crime Detection and Prevention Series; Paper No. 68, 1995, <http://www.popcenter.org/responses /video_surveillance/pdfs/brown_1995_full.pdf>, last access August 3rd 2015.

who say that they avoid the city centre has increased after the installation of CCTV.[66] The same studies find no evidence that, in general, the installation of CCTV in Glasgow has a positive impact on fear of crime. A study by Gill and Spriggs carried out in different cities in the UK also finds out that, in general, feelings of safety have little improved after the installation of CCTV. Moreover, in particular cases, an increase in the fear of crime is even registered: in two of the surveilled areas, people who are aware of the installation of CCTV worry more often about crime than those unaware of the CCTV. The authors interpret these findings as indicators that the presence of cameras can make a place appear less safe than one would have assumed.[67] I already referred to such phenomenon in section 2 as the "security dilemma".

Drawing from such studies and others, several authors point out that feelings of safety depend less on technical factors like the installation of a CCTV system and more on other elements like the actual reduction of victimization (i.e. the experience of having been the victim of a crime), familiarity with people, situations and places and the presence of other people.[68]

Actual and perceived security

In the previous sub-section, I addressed the question whether the deployment of surveillance technologies *per se* increases perceived security, independently from the question whether it also increases actual security. Now I shall assume that security technologies increase actual security and will ask whether, and if yes how, this impacts perceived security.

Intuitively, one could assume that perceived security is in a cause-effect relationship with actual security: the higher the actual crime reduction, the higher the safety feelings, and vice-versa. This is partly true, and there are surveys that indicate the existence of a link between victimization and the fear of crime. So, for instance, a study carried out in the UK finds out that people who were victim of a crime in the year before the interview are three times more likely to worry about crime than non-victims.[69]

However, the relationship between fear of crime and reduction of crime is not always so direct as the abovementioned findings would suggest.[70] On the contrary, often the objective situation and the subjective feeling do not seem to be correlated: crime rates may increase and the fear of crime may decrease, and vice versa. To describe such phenomenon scholars speak of the "fear of crime paradox".

This might derive from a misevaluation of the risks related to criminality, which in turn may be influenced by several factors. First, people may have an unrealistic perception of how likely it is that they become the victim of a crime (false perception of "personal risk"). For instance, statistics often report that women are more afraid of becoming victims of violence, although in fact men are far more often victims of violence than women.[71] Second, people may misperceive the likelihood of a particular

[66] J. Ditton, Crime an the city, cit., p. 698; Avoidance behaviour, i.e. to avoid going to certain areas (at certain times) is considered in this and other surveys as a sign of lack of safety feeling: people avoid certain places if they do not feel safe there.

[67] M. Gill, A. Spriggs, Assessing the impact of CCTV, cit., p. 48. Such findings are confirmed in D. Williams, J. Ahmed, The Relationship Between, cit.

[68] M. Gill, A. Spriggs, Assessing the impact of CCTV, cit.; M. Apelt, N. Möllers, Wie intelligente" Videoüberwachung, cit; N. Zurawski, „It is all about perceptions', cit.

[69] M: M. Gill et al., Public perceptions, cit., p. 311

[70] S. for instance H-J. Lange, M. Gasch, "Subjektives Sicherheitsgefühl", Wörterbuch zur inneren Sicherheit, Wiesbaden, 2006, p. 323.

[71] S. for instance SuSi-PLUS, Subjektives Sicherheitsempfinden im Personennahverkehr mit Linienbusse, U-Bahnen und Stadtbahnen, Auszug aus dem Abschlussbericht: Zusammenfassung und wichtigste Ergebnisse, http://www.susi-team.de/images/stories/Downloads/band7summary.pdf, 2005, last access August, 3rd 2015, p. 11-12 and the UNECE

crime being committed in general or in a particular situation (false perception of "situational risk"). Parents, for instance, are increasingly worried about their children becoming victims of sexual assault, although the number of cases is decreasing, and women are afraid of sexual violence in public spaces, although statistics show that two thirds of the cases of sexual violence take place at home or inside the family.[72]

Explanations for such a paradox have been advanced by scholars coming from sociological, psychological, evolutionistic and mixed backgrounds.[73]

Although there are many studies on the relationship between actual risk and risk perception, very little can be found dealing specifically with surveillance technologies. Apart from the study already mentioned by Gill and Spriggs, I found no survey measuring the impact of a surveillance system on actual security and on perceived security and comparing the two. A study carried out in the CPSI project, however, indirectly tackles the matter.[74] It investigates, among others, the relationship between acceptance of security interventions by the state and perceived security in seven European countries (Austria, Bulgaria, France, Germany, Italy, the Netherlands, Sweden and the United Kingdom) and, against expectations, it uncovers no evidence of the existence of such relationship. Moreover, the authors argue that political and cultural factors also play a role in shaping the relationship between actual and perceived security. On this basis they interpret the main findings of the surveys. These include uncovering discrepancies between criminal statistics and the level of fear of crime. So, for instance, the study reveals a social "overfear" of crime in Austria and an "underfear" security culture in Germany; i.e. that in Austria people are more fearful about crimes being committed than a realistic consideration of statistics on crime would suggest, while in Germany the fear of crime is low compared to actual crime rates.

Perceived effectiveness

The question to be addressed here is: "do people think surveillance is effective, typically in reducing crime and reducing the fear of crime?"

Surveys generally report a high acceptance of CCTV systems, so it is somehow puzzling to find out that, as the same studies show, most people do not think of CCTV as effective. The PRISE deliverable 5.8 reports that "approximately 70 percent of the participants in the six countries completely or partly agree to the statement that many security technologies do not really increase security, but are only being applied to show that something is being done to fight terror. The technologies are simply implemented for political reasons".[75] Studies carried out in the URBAN EYE project and in the city of Hamburg confirm such scepticism with reference to CCTV.[76] The former study reports that 55% of respondents agree with the statement that CCTV "displaces rather than reduces" crime; only 23% believe that it "prevents serious crime", and only 29% affirm that they would feel safer if more CCTV systems were installed. Similar results are found in Hamburg: almost 60% of respondents believe that

(Contd.)

(United Nations Economic Commission for Europe) statistical database at http://w3.unece.org/pxweb/database/STAT/30-GE/07-CV/?lang=1, last access 25/7/2013.

[72] M. Apelt, N. Möllers, Wie „intelligente" Videoüberwachung, cit., p. 588.

[73] Ivi; H-J. Lange, M. Gasch, "Subjektives Sicherheitsgefühl", cit.; B. Schneier, The Psychology of Security, 2008, <http://www.schneier.com/essay-155.html>, visited on August, 3rd 2015; S. Roeser, R. Hillerbrand, P. Sandin, M. Peterson (Eds.), The Handbook of Risk Theory, part 4; K. Boers, P. Kurz, Kriminalitätseinstellungen, soziale Milieus und sozialer Umbruch, in K. Boers, G. Gutsche, K. Sessar (eds.), Sozialer Umbruch und Kriminalität in Deutschland, Opladen 1997, 187-254; D., Die Entwicklung von Kriminalität und Kriminalitätsfurcht in Deutschland – Konsequenzen für die Kriminalprävention, *Deutsche Zeitschrift für Kommunalwissenschaften*, 42 (2003), 1, 31-52.

[74] CPSI Analytical Standpoint 13, Summary of CPSI Country Case Studies, 2010, http://www.esci.at/eusipo/asp13.pdf, last access August, 3rd 2015.

[75] PRISE D5.8, cit., p. 22.

[76] Urban Eye WP 15, cit., p. 9, 13, 17 and p. 45; N. Zurawski, "It is all about perceptions"', cit., p. 269.

CCTV displaces crime instead of solving it, while only 43% feel that cameras protect them against crime.

Other studies register that people's belief in the effectiveness of CCTV has declined after their installation. A study conducted by Gill and Spriggs in the UK, for instance, asks people in residential areas before and after CCTV installation whether they think that: a) people are more likely to report incidents to the police when CCTV is present; b) the police react more quickly if CCTV is installed and c) crime decreases after the installation of CCTV. In all cases, people are less prone to agree with such statements after the installation of CCTV.[77] These and similar results from other studies have been interpreted as a consequence of a more realistic attitude towards CCTV after seeing them in action: "It was not as good as they thought it would be; it was not responsible, as far as they could assess, for tackling crime".[78]

However, contrary to the findings of the abovementioned surveys, one of the available studies reports that a majority of people believe that CCTV is a meaningful tool to reduce criminality.[79]

Results

The analysis of existing studies on perceptions of surveillance shows that a negative perception of surveillance in Europe is a very context-dependent issue. Places and situations where they are deployed and national differences play a major role in shaping the perception of such technologies. As to the relationship between perception and effectiveness, it emerges from the studies presented here that this is a complex relationship, with no cause-consequence link between the two.

[77] M. Gill, A. Spriggs, Assessing the impact of CCTV, cit., p. ix-x and 57.

[78] M. Gill et al., Public perceptions, cit., p. 322.

[79] K-H. Reuband, Videoüberwachung. Was Bürger von der Überwachung halten, *Neue Kriminalpolitik*, 13 (2001), 2, 5-9, p. 9. According to this study, among the perceived aims of the deployment of CCTV are both to catch offenders and to deter potential criminals.

PART II: Methodology to incorporate perception issues in the design of new technologies

Building the methodology

Building on the results of the surveys on perceptions of surveillance presented above, this paper proposes a methodology to incorporate perception issues in the design phase of new technologies. The methodology should enable developers of new technologies to design them in a more perception-sensitive way.

As we have seen, perception issues surrounding surveillance can be divided into two broad groups: negative perceptions and perceived effectiveness. Because the two kinds of perceptions relate to two distinct frameworks, this paper develops the methodology to address each of them in two distinct parts.

However, the two parts of the methodology are based on the same basic idea and present similar structures. The common idea behind both parts of the methodology consists in the need to avoid manipulative interventions that aim at addressing perceptions only, without substantively improving the technologies. The common structure of the two methodology parts derives from their common founding idea and consists of successive steps firstly addressing the background conditions from which negative perceptions or perceptions of poor effectiveness arise and, secondly, perception itself.

After developing the two parts of the methodology, I will highlight their similarities and combine the results in common methodological guidelines.

Negative perceptions and design

As its starting point, the proposed methodology for addressing issues of negative perceptions adopts the analysis of perception-related effects and side effects of surveillance, instead of focusing primarily on technologies and their uses.

The undesirability of negative perceptions is twofold. On the one hand, in SURVEILLE, negative perception is considered to be a cost of surveillance technologies. On the other hand, as argued above, the perception-related effects and side effects of surveillance impact individuals' behaviour and society in a way that threatens the background conditions and basic principles of democracy, the rule of law and solidarity.

Addressing background conditions rather than surfaces

In looking for a methodology to incorporate perception issues in the design phase of new technologies, I take into account both aspects of such undesirability. This means that this methodology rejects approaches aiming exclusively to act on the surface of the (side)effects by improving perceptions without tackling the actual problems (which often correspond to the effects and side effects of surveillance). Such an approach would be incompatible with the basic principles of the rule of law and democracy.

The following example illustrates what I mean by interventions aiming only to cosmetically address perceptions. Take the case of a CCTV system installed in a park which raises privacy concerns within the public, which, in turn, influence peoples' perceptions of CCTV surveillance negatively. A possible way to address perception issues could include measures such as an advertising campaign presenting CCTV systems as friendly to park-visitors, painting the cameras green in order to make them blend into the scenery better, or making covert use of them in order to make park visitors unaware of their

existence. Independently of the question whether such measures would be effective in the short and long run, our approach rejects them because of their paternalistic character. They conflict with our conception of human beings as rational and autonomous persons that a democratic and rule-of-law oriented approach should adopt. Instead, I propose a methodology that takes people's concerns seriously, questions the actual problems behind them and seeks to address them effectively.

Our option for a background-oriented approach is expressed by the basic assumption of the proposed methodology:

> In order to address perception issues in a way that is compatible with fundamental rights and democratic principles, the background issues affecting negative perceptions rather than perceptions only should be tackled in the first place.

This does not mean that the background issues affecting perception negatively are always identical with the most apparent potential rationales for it. For instance, our example of CCTV reveals that the most obvious rationale for negative perceptions can be a real invasion of privacy. However, further conditions may potentially cause negative perceptions, including a lack of knowledge about the existing privacy-preserving features of the CCTV system, or a lack of transparency in the way they are communicated to the public. The rationales for negative perceptions vary for each case and are context-dependent. Identifying them is therefore a task to be carried out on a case-by-case basis.

Whatever the rationales for negative perceptions in a particular case are, the first basic assumption of the proposed methodology expresses the need of individuating, addressing and as far as possible correcting them rather than simply making the particular technology or its particular use appear "better" than it is in order to avoid or minimise negative perceptions. In our example with CCTVs, corrective measures could aim at reducing the installation of cameras to a minimum, while providing extensive information on existing protective mechanisms and/or improving communications transparency.

The three levels of intervention

Once the background conditions related to negative perceptions are identified, the proposed methodology envisages three levels of intervention. In the design phase of new technologies, measures should be taken at each of the three levels in order to effectively address the background conditions of negative perceptions and the negative perceptions themselves:

- At the first level, measures should be adopted in order to achieve "minimum harm by design" (MHbD);
- At the second level, measures should be adopted to implement transparency by design (TbD);
- At the third level measures should be adopted that aim at enhancing accountability by design (AbD).

Interventions at the first level put into effect the idea expressed in the basic assumption that it is necessary to *actually* improve the technologies and their uses in order to minimise negative perceptions and that a purely cosmetic intervention on the perception level is not sufficient. The two subsequent levels specifically address perceptions: they express the idea that, once realised, actual improvements should also be made transparent and verifiable. Only in the rare event where negative perceptions arise exclusively from a lack of transparency, from misinformation or from the wrong kinds of communication strategies can interventions take place primarily at the second and third level.

Minimum harm by design (MHbD)

Implementing MHbD for surveillance technologies implies designing them in a way which makes their negative impact on individuals, their behaviour and society as small as possible.

MHbD can be achieved, for instance, by designing the technologies in a way that makes them invade privacy as little as possible and that minimises the possibilities of misuse. A type of technology or a system can be designed to reduce its privacy impact, for example, by making it collect as little personal data as strictly necessary for achieving its goals or by making people as unidentifiable as possible, or by elaborating the collected data in a decentralised way. How this applies to each type of technology is a matter to be solved case by case, and it does not solely depend on the technical characteristics of a type of technology or system but also on its destination, the context of deployment, etc.

Existing examples of how to implement such proposals focus on mechanisms to enhance data minimisation. Pioneering proposals date back to the mid-Eighties, when David Chaum proposed a large-scale transaction system like the ones used for electronic payment, that is a system that provides security for organisations without requiring the identification of users.[80] More recently, Claudia Diaz et al. presented a system for signing electronic petitions that allows controllers to detect double signatures *and* signatories to protect their privacy through anonymity.[81] Moreover, Josep Balash et al. elaborated a prototype electronic toll pricing system that minimises the privacy impact principally by decentralising the processing of data, thus reducing the quantity of data transmitted to the central database. The presented toll pricing system is able to prove to the central system that the information transmitted is genuine without disclosing fine-grained location data that would reveal sensitive information about the users.[82] Further examples include proposals to make smart CCTV systems at airports less privacy-intrusive[83] and to encrypt by default the images of individuals collected by drones.[84]

One recurrent though not strictly necessary feature of such proposals is decentralisation: the proposals show that it is possible to leave a greater amount of information in the hands of the persons whose personal data are handled without jeopardising the functionality and security of the system. Hence, when meaningful, MHbD requires achieving as much decentralisation as possible.

Focusing on this level of intervention can be particularly effective to mitigate negative perceptions arising from side effects of surveillance such as the ones dealt with under number 1 (technologies perceived as threats), 3 (fear of misuse) and 4 (fear of insufficient protection of personal data). However, interventions at the other two levels are necessary as well.

The notion of MHbD overlaps in part with the notion of Privacy by Design (see info-box), nowadays a well-established and increasingly successful set of principles.[85]

---

[80] D. Chaum, 'Security without Identification: Transaction Systems to Make Big Brother Obsolete', *Commun. ACM*, 28 (1985), 1030–1044.

[81] C. Diaz and others, 'Privacy Preserving Electronic Petitions', *Identity in the Information Society*, 1 (2008), 203–219.

[82] J. Balasch and others, 'PrETP: Privacy-Preserving Electronic Toll Pricing', in *19th USENIX Security Symposium*, 2010, 63–78.

[83] C. Bier, P. Birnstill, E. Krempel, H. Vagts, J. Beyerer, Enhancing Privacy by Design From a Developer's Perspective, *Privacy Technologies and Policy*, 2014, 73-85.

[84] A. Cavoukian, *Surveillance, Then and Now: Securing Privacy in Public Spaces*, June 2013, http://www.privacybydesign.ca/index.php/paper/surveillance-then-and-now-securing-privacy-in-public-spaces/, accessed August 5th, 2015.

[85] For a set of principles aiming at the same purposes as PbD applied to CCTV see European Forum for Urban Security: Charter for a democratic use of video

surveillance, 2010, http://www.cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Charta/CCTV_Charter_EN.pdf and the SURVEILLE D2.3, "*Paper by local authorities end users*", http://surveille.eui.eu/wp-content/uploads/2015/04/D2.3-Paper-by-Local-Authorities-End-Users.pdf, both accessed August 5th, 2015. See also, for the increasing recognition of PbD by the EU the COMMISSION IMPLEMENTING DECISION C(2015) 102 final of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation

Although I recognise the validity of the research done in the PbD realm, I prefer, nevertheless, not to refer to PbD here and elaborate instead on the notion of MHbD for the following reasons:

- "PbD" misleadingly suggests that technologies complying with its requirements bring about an improvement of privacy. The expression "MHbD", on the contrary, signalises that surveillance technologies *always* bring about a negative impact on individuals and society and that this impact can be minimised at best but will never be completely eliminated.
- PbD focuses on information privacy, i.e. privacy regarding the collection and use of personal information. However, it is neither proven that (information) privacy is the only right threatened by surveillance, nor that threats to other rights and values necessarily depend on a previous violation of (information) privacy or that they would not take place if the invasion were to be removed. The answer to the question whether intrusions in information privacy are always the preconditions for further violations mostly depends on the definition of "privacy" adopted, which is itself a controversial matter.[86] Moreover, as the following example illustrates, whether a violation of fundamental rights and values depends on a previous privacy intrusion is a matter of perspective. Take, for example, the effect "social exclusion and discrimination" and a CCTV-surveillance scenario. In our scenario, the installed CCTV system incorporates biometrical facial recognition, which allows for the identification of the people filmed. If people are considered to be suspect on the basis of any of the data collected by the CCTV system, they are singled out for further checks. To select suspects, the operators also use categorical suspicion based on appearance. By removing biometrical identification, the system would be made less intrusive to privacy. However, the effect "social exclusion and discrimination" would not diminish unless the skin colour of a person or the way she is dressed were also concealed in the output image of the CCTV system. Of course, one could object that concealing the particular features of people filmed is also a privacy-preserving measure. However, an approach that focuses not only on privacy like the one proposed here seems able to solve such problems in a more straightforward way. By referring to a "minimum harm" rather than only "privacy" I aim not to exclusively restrict *a priori* the field of intervention into privacy-related issues.
- PbD targets whole organisations' practices instead of kinds of technologies or technology systems. PbD, for instance, does not primarily or exclusively prescribe how a licence plate recognition system should be designed in order to minimise its impact on privacy. Instead, Cavoukian's approach targets the whole context in which such a system is adopted and prescribes measures regarding, say, the code of conduct for employees handling the data, or the legislative measures limiting the uses of the data. Although such a holistic approach is meaningful and technical aspects should not be addressed in isolation from the organisational, societal, political and legal context in which they are used, I find it to be more fruitful, for analytical purposes, to keep the different stages separate. I therefore concentrate here on the *technological* aspects that a) reduce technologies' negative impact on perception through reducing the impact on basic values of solidarity, democracy and the *rule of law*; b) make it possible and meaningful to adopt further strategies at the institutional, political, legal and societal level that further reduce the impact on negative perceptions and the abovementioned values.
- As pointed out in different contributions, current definitions of "PbD" are so vague that they do not provide guidelines on how to translate its principles into engineering practices for designing

(Contd.)

deliverables for privacy and personal data protection management, <http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548#>, M530, last access August 19th, 2015.

[86] D. J. Solove, Understanding Privacy, Cambridge 2008 and J. DeCew, 'Privacy', in *The Stanford Encyclopedia of Philosophy*, ed. by E. N. Zalta, Fall 2013, 2013 <http://plato.stanford.edu/archives/fall2013/entries/privacy/>, accessed August 5th, 2015.

new technologies[87]. Given these shortcomings, PbD risks becoming a label with which to reassure consumers and the public without bringing about real improvements for privacy - exactly the opposite of our first basic assumption.[88]

INFOBOX: PRIVACY BY DESIGN

(See Cavoukian, Ann, 'Privacy by Design. The 7 Foundational Principles', August 2009, <http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf/>, accessed August, 5th 2015)

Ann Cavoukian introduced the concept of PbD in the Nineties to address the growing challenges posed by new technologies to the protection of personal information[1]. PbD aims to make privacy assurance the default mode of operation for organisations, and, according to Cavoukian, it may be attained by acting in accordance with the following seven foundational principles of PbD:

1. Proactive not reactive; preventive not remedial.

   This principle expresses the idea that PbD should act proactively, preventing privacy intrusions from happening instead of intervening after they have occurred.

2. Privacy as the default setting.

   No action should be required by users in order to protect their privacy: Personal data should be automatically protected as the default rule.

3. Privacy embedded into design.

   Privacy should be embedded into the system from the beginning; it should belong to its core functionality instead of being added after the system has already been designed.

4. Full functionality – positive-sum, not zero-sum. No trade-offs between privacy and security are necessary: in the PbD approach it is possible to have both.

5. End-to-end security – full lifecycle protection.

   Because privacy protection is embedded into the system from the design phase, it is operative before personal information is collected. This should guarantee the protection of personal information throughout the whole lifecycle of data processing.

6. Visibility and transparency – keep it open.

   This principle aims at assuring stakeholders that the system is operating in a privacy-protecting manner and is subject to independent verification.

7. Respect for user privacy – keep it user-centric.

   Users' interests should have the highest priority both in the design and operating phases.

[87] S. Gürses, C. Troncoso and C. Diaz 'Engineering Privacy by Design', https://www.cosic.esat.kuleuven.be/publications/article-1542.pdf/, last access August, 5th 2015 and C. Bier, P. Birnstill, E. Krempel, H. Vagts, J. Beyerer, Enhancing Privacy by Design, cit.

[88] S. Gürses, C. Troncoso and C. Diaz, 'Engineering Privacy by Design', cit.

Transparency by design (TbD)

Transparency by design means that technologies should be designed in a way that makes as much information as possible accessible to the public or to the persons affected by their use (typically people affected by surveillance).

The way technologies are designed should, for instance, enable the group of people targeted by surveillance to know the following:

- For what purposes the technologies were created;
- How the technologies are used and whether these uses correspond with the original/authorised purposes;
- How much and what kind of personal information is collected using the technologies, how it is used and for how long it is kept;
- Who operates the technologies and who has access to the data collected by them;
- What measures of MHbD are implemented in the technologies and what are their limits;
- What measures of AbD (see below) are implemented in the technologies and how they can make use of them;
- How they can access the information listed above.

As the list above shows, transparency should also cover, but not only, the other two levels of intervention: MHbD and AbD.

The quantity and kind of information made available and to whom varies largely depending on the technology, its particular use and the context of deployment.

In general, there are two broad categories of information about surveillance technologies: general and personal. They should be made available according to two different strategies: general information should be publicly available, whereas personal information should be made available only to the persons to whom it belongs. For instance, in the case of a licence plate recognition system on a motorway, the information available to the whole public could include: the purposes for which it was installed; the authority which authorised the installation and for what purposes and under what limitations; whether the system works in a covert, overt or opaque manner; what kinds of data are collected; how long they are kept before being definitively deleted; to whom they are communicated; who has access to them. Annual reports subjected to independent verification can be a way to make such kinds of information public.89 Clearly, the general public should not have access to the actual database – however, the persons whose data were collected should. In this case, then, the plate recognition system should be designed in a way that makes it possible for each individual to know whether her vehicle had been tracked by the system, when and where it happened, who/which organisation or agency accessed the data, what was done with the data, whether they were deleted at the right time or not and so on.

The way to access these pieces of information should be straightforward and uncomplicated; no special skills or knowledge should be expected in order to have access to them: No more, say, than the ability to use a smart phone if the technology in question is a smart phone, or no more than the ability to browse the internet if the technology in question is an internet browser. As per our example of a plate recognition system, no more skills than the ones necessary for obtaining a driving licence and carrying on the usual bureaucratic activities related to the possession of a car (such as stipulating an insurance and paying car taxes) should be necessary to access the data.

If supported by appropriate measures such as the ones suggested in the frameworks MHbD and AbD, the focus on this level of intervention can be particularly effective against side effects of surveillance

[89] A. Cavoukian, *Surveillance, Then and Now*, cit.

such as number 5 (Fear of unlimited expansion and irreversibility) and numbers 6 to 8 (self-surveillance, chilling effect, conformism and loss of autonomy). Transparency about the objectives and uses of surveillance technologies can, for instance, be effective in minimising the fear of unlimited expansion and irreversibility, while clear and precise information about where and when surveillance takes place and about the criteria for suspicion can minimise self-surveillance and the related side-effects of societal chill, conformism and loss of autonomy. These examples make the interdependence of the three levels clear: transparency, of course, can be counter-productive if the objectives of surveillance are too broad, if surveillance is ubiquitous or if the criteria for suspicion are too vague.

Accountability by design (AbD)

The claim for AbD expresses the idea that the way technologies are designed should make cases of misuse and their authors traceable, accountable and sanctionable.

Examples of misuse of surveillance technologies include the following:

- Deployment beyond the original purposes;
- Use in places or situations that are not authorised or not identical with the original ones;
- Use of the collected data for purposes that are not authorised or different from the original ones;
- Non-authorised circulation of the collected data;
- Use of the collected data beyond the authorised time-frame;
- Deployment of the technologies and/or use of the collected data in a discriminatory way.

Proposals of designs that enable accountability focus on logs registering access and handling of personal data. Such systems have been applied to e-mail service providers handling e-mail users' data, bank operators handling the personal data of bank customers, or operators accessing data collected by drones.[90] Existing literature shows that systems can be designed in a way that enables *a posteriori* checks about compliances with the data usage rules.

Even if AbD does not influence specific effects and side effects of surveillance, it seems to be the key for the effectiveness of MHbD and TbD because they may function effectively only if checks are possible.

Beyond design

The remedies foreseen by the proposed methodology are meaningful and can be effective only if backed up by a broader context in which they can actually operate. For instance, the technical features of a particular technology allowing for tracking accountability for violations and misuse are meaningful only in a context that foresees sanctions for such violations.

Pertaining to such a context, among others, are societal, institutional, political and legal settings.

Examples of measures at the legal level include mandatory, previous judicial authorisation for the deployment of surveillance technologies; strict and binding codes of conduct for surveillance operators and a mandatory two-signature protocol to access data collected by surveillance systems.[91]

---

[90] PRESCIENT, International Conference of the PRESCIENT Project, Berlin, 27-28 November 2012, Session 3: 1. Accountability by Design for Privacy, <http://prescient-project.eu/prescient/inhalte/download/prescient2012.pdf>, last visit August 5th, 2015; D. J. Weitzner and others, 'Information Accountability', *Commun. ACM*, 51 (2008), 82–87; D. Butin, M. Chicote and D. Le Metayer, 'Log Design for Accountability', in *2012 IEEE Symposium on Security and Privacy Workshops*, 2013, 1–7; A. Cavoukian, *Surveillance, Then and Now*, cit.

[91] A. Cavoukian, *Surveillance, Then and Now*, cit. For existing regulatory instrument at the European level, (in particular the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data and the Directive 2002/58/EC of

Other, non-legal measures include public discussions carried out routinely before the installation of new surveillance systems and centres for facilitating communication between individuals and institutions.[92]

Moreover, making different, practicable options available to individuals can strengthen the results attained by applying the proposed methodology. There should be options between not flying at all and letting one's biometric data be collected, or between having one's email exchange intercepted vs. having to renounce writing emails.

(Contd.)

the European Parliament and of the Council of 12 July 2002 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector) see SurPRISE D3.2, Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy, March 2013, http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE_D3.2_Report-on-regulatory-frameworks-concerning-privacy-for-final-formatting_v094.pdf, last visited August, 5th 2015.

[92] A. Cavoukian, *Surveillance, Then and Now*, cit.

Perceived effectiveness and design

The study presented in the first part of this paper pinpoints three variations of the relationship between perception and effectiveness. The first relates to the question whether surveillance, independently of its actual security improvements, increases perceived security. The second way perception and effectiveness relate to each other concerns the relationship between actual and perceived security, i.e. to the question whether an improvement in actual security brings about an increase in perceived security. The third variation of the relationship between perception and effectiveness is properly called perceived effectiveness. It relates to the question whether people think surveillance is effective, typically in reducing crime and reducing the fear of crime.

The first and the second way perception and effectiveness interact with each other seem to be determined by factors external to the use of surveillance such as social and interpersonal relationships and the actual crime rates. Hence, it seems that a meaningful intervention for addressing perception in these cases should focus on those external factors rather than on the design of new technologies.

Therefore I will concentrate here on the third way perception and effectiveness relate to each other, i.e. on perceived effectiveness.

There are many ways people may think of surveillance as being effective in reducing crime: for instance, they may refer to the prevention of crimes being committed due to the deterrence of potential offenders as well as to the identification of offenders in the prosecution phase. Respondents' perceptions of the effectiveness of surveillance vary considerably, but, unfortunately, surveys available often do not clearly distinguish between them.[93]

How can such perceptions be addressed already in the design phase of new technologies?

Addressing background conditions rather than surfaces/II

As in the case of negative perception, the proposed methodology for perceived effectiveness is based on the idea that measures aimed at addressing perceptions only are insufficient. Therefore, the basic assumption of the proposed methodology can be reformulated as follows:

> Interventions should first address the background conditions affecting perceived effectiveness rather than only focus on perceptions.

In the realm of perceived effectiveness, the basic assumption expresses the need to avoid measures inspired by the so-called "security theatre". This "covers measures taken, ostensibly in the name of security, whose value lies solely (or at least mostly) in their capacity to give the reassuring impression that *something is being done*, that *steps are being taken*, that *someone is on the case*—rather than in actually increasing security, considered from an objective standpoint. The role of security theatre is to increase *perceived* security, without necessarily having any positive effect in terms of *actual* security".[94]

In the design of new technologies, interventions inspired by the security theatre should be avoided for two reasons. First, like in the case of negative perception, manipulative interventions would contradict and threaten basic principles of democracy and the rule of law. Second, as demonstrated by the analysis of surveys carried out in part one of the paper, respondents are aware of the possibility that

---

[93] See above, part I, section 3.

[94] PACT D1.4 Societal Impact Report, 2012, <http://www.projectpact.eu/deliverables/wp1-root-branch-review/d1.4-social-impact-report>, last visit August 5th, 2015, p. 16 and B. Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, New York 2003.

measures are taken just to reassure people, without tackling the actual problems.[95] Therefore, besides being morally and politically problematic, approaches inspired by the security theatre do not seem to have good chances of success.

Two levels of intervention

After looking for the background conditions of poorly perceived effectiveness, the proposed methodology requires designing technologies in order to achieve

1. Higher effectiveness
2. TbD

The first point requires acting accordingly with the basic assumption: the first question to ask is whether the perception that technologies are poorly effective is well-grounded. If this is the case, the first step consists of improving the system's effectiveness as much as it is compatible with legal, ethical and social restraints.

Only after dealing with actual effectiveness are further measures meaningful. Efficiency and effectiveness issues have been tackled extensively in the SURVEILLE Deliverables 3.3 "*Report on system effectiveness, efficiency and satisfaction assessment"* and 3.4 "*Design of a research methodology for assessing the effectiveness of selected surveillance systems in delivering improved security.*[96]

As to AbD, at this stage of research it seems that no measures of AbD are needed for addressing issues of perceived effectiveness.

Transparency by design (TbD)

In order to achieve TbD for addressing perceptions of effectiveness, technologies should be designed in a way that keeps track of their operations. Combined with further information, this data on system operations should make it possible to document the success rate of the system.

From the collected data it should be possible to reconstruct, for instance:

1. How many cases the system analysed;
2. How many warnings the system issued;
3. How many warnings eventually led to successful interventions and how many did not;
4. Whenever possible, how many potential dangers or infractions the system failed to detect.

For instance, a metal detector used for luggage screening at airports should keep track of the number of items examined and of the number of items selected for further checks, and such data should be combined with information from the security agencies on the number of dangerous items eventually detected and, whenever possible, the number of dangerous items that went undetected through checks. An electronic plate recognition system should keep track of the number of vehicles tracked and of the number of infractions registered; these data should be combined with the number of infractions eventually sanctioned and, whenever possible, with the number of infractions that remained undetected.

Beyond design

In the case of perceived effectiveness as well, design measures should be supported by a social, political, institutional and legal context that makes them fruitful.

---

[95] See above, part I, section 3.

[96] Available at the SURVEILLE website <http://surveille.eui.eu/research/publications/>.

First, as we have seen, the data collected should be integrated and elaborated in order to gain knowledge about the actual effectiveness of the technologies considered. The data keeping track of the system functionality should be integrated with data on the number of false positives, false negatives and of the success rates. Such data should be further statistically elaborated.

Second, openness about the effectiveness of surveillance technology is needed. Both raw data and statistics should be made public. Annual reports about the effectiveness of different security technologies, including information about the strengths and limits of each technology, could also be a useful instrument for backing up TbD. Whether the further use of a technology is meaningful or not in the light of effectiveness should be a matter of public and open debate.

Third, consequences have to be drawn from the information about effectiveness. If a technology proves to be inadequate for achieving the purposes for which it was adopted, it should not be used anymore. Clearly, this presupposes that the purposes of the deployment of a particular technology should be clearly stated from the beginning.

Finally, statistical data and further information about the effectiveness of surveillance technologies should be communicated in a way that takes into account the most recent research on the perception of risk and the role of emotions in risk perception.[97] Existing psychological research shows, on the one hand, a possible link between the communication of information and the acceptance of security interventions and, on the other hand, that acceptance increases when decisions about the deployment of security technologies are perceived as fair and transparent.[98]

Combined methodological guidelines

So far the methodologies for addressing negative perceptions and perceived effectiveness have been developed separately. However, the two methodologies have a parallel structure and several similarities. It is thus possible to combine them in the following methodological guidelines.

The first step for applying the methodology is to ask if the technology to be developed may be perceived negatively and whether it will be perceived as being effective. This preliminary inquiry may rest upon surveys (existing on similar technologies or *ad hoc*) and on the basis of simulations and literature. The inquiry should aim at finding out whether the new technology, in the context for which it will be employed:

(a) potentially has the following negative perception-related effects and side effects:

1. Technologies perceived as threats;
2. Security dilemma and surveillance spiral;
3. Fear of misuse (incl. function creep);
4. Fear of insufficient protection of personal data;
5. Fear of unlimited expansion and irreversibility;
6. Self-surveillance;
7. Chilling effect;
8. Conformism and loss of autonomy;

[97] S. Röser and others, 'Handbook of Risk Theory Epistemology, Decision Theory, Ethics, and Social Implications of Risk', 2012.

[98] M. Schuler and L. Wolkenstein, 'Psychologie und Sicherheitstechnologie – Psychologische Auswirkungen von Sicherheitstechnologien auf den Menschen und die Einstellung von Menschen dieser Technik gegenüber', in H.-H. Gander, and G. Rischer (eds.), *Sicherheit und offene Gesellschaft. Herausforderungen, Methoden und Praxis einer gesellschaftspolitischen Sicherheitsforschung*, Baden-Baden 2014.

9. "Control society";
10. Social exclusion and discrimination;
11. Social homogenisation;
12. Decline of solidarity.

and

(b) may be perceived as "security theatre" or otherwise ineffective.

Once the potential (side)effects of the use of a technology in a particular context are identified and it has been ascertained that it may be perceived as poorly effective, the second step consists of identifying the actual circumstances from which such perceptions arise, according to the basic assumption of the proposed methodology.

The successive steps consist of interventions at the further levels: minimum harm, transparency and accountability by design to address negative perceptions, improvements on effectiveness and transparency by design to address perceived effectiveness.

The table reported in Annex 5 outlines the methodological guidelines for addressing both negative perceptions and perceived effectiveness.

Need for further research

Beyond the specific reported above, the research conducted also highlights trends and shortcomings of current research on perceptions of surveillance which might be useful for future studies.

As to the state of the art of European research on perceptions of visual surveillance and CCTV in particular, the following considerations regarding the relationship between the groups targeted by surveillance and the sample represented in the interviews may be advanced.

Depending on which technologies and for what purpose they are deployed, specific groups of people are more affected than others by surveillance. This is the case, for instance, with CCTV, which is most commonly deployed to address "undesired" behaviours that have little to do with (serious) crime and terrorism. With the words of Martin Gill, CCTV, for instance, is used "extensively as a means of controlling alcohol-related and other anti-social behaviour in town and city centres, monitoring and dispersing large groups of individuals and moving on what many operators termed 'undesirables', such as beggars and on-street traders".[99] Another example is technologies used for border-control, mainly deployed for keeping away another category of "undesirables", i.e. migrants. According to the EUROPOL SOCTA ("Serious and Organised Crime Threat Assessment") 2013, to combat facilitation of illegal migration should be the top priority of EUROPOL, coming even before the fight against other activities whose criminal character is more apparent like human trafficking or money laundering.[100] Moreover, surveillance's impact on migrants is huge not only because they are the first targets of European common security politics but also because they are affected in a way that often goes as far as taking their lives.[101] Further examples are surveillance technologies for which targets are selected on the basis of a risk-profiling based on, for instance, their physical appearance (visual surveillance), their physical constitution (body scanners), or their behaviour when surfing on the internet (communication surveillance).

The question arises whether existing studies elaborate strategies for recruiting interviewees that could reflect such circumstances, i.e. to adequately represent in their results the views of those who are most affected by surveillance.

The table in Annex 3 shows the recruitment strategy for the 15 studies that base their conclusions on self-conducted surveys instead of relying on pre-existing ones.

Nine out of these 15 studies use recruitment strategies or interview-media that indirectly exclude those most often targeted by surveillance, such as beggars, homeless, alcohol and drug addicts and undocumented migrants or migrants who do not manage to become residents in the EU. Seven of these nine studies (underlined in Annex 3) exclude non-resident persons (therefore homeless, undocumented migrants and migrants who attempted to come to Europe but failed) from their sample either because they address residents only or because they use means of communication presupposing residency (landline phone and mail).[102] The remaining two (in *italics* in Annex 3) specifically target, at least as a

[99] M. Gill, A. Spriggs, Assessing the impact of CCTV, cit., p. 117. See also L. Hempel, E. Töpfer, The Surveillance Consensus, cit.; L. Hempel, E. Töpfer, URBAN EYE WP 15, cit.; K-H. Reuband, Videoüberwachung, cit.; B. Brown, CCTV in Town Centres, cit., p. 40 and s. Graham et al., Towns on the Television, cit., p. 18.

[100] SOCTA 2013, "Serious and Organised Crime Threat Assessment, p. 41, https://www.europol.europa.eu/content/eu-serious-and-organised-crime-threat-assessment-socta, last visit August 19th, 2015.

[101] See http://fortresseurope.blogspot.de/2006/02/immigrants-dead-at-frontiers-of-europe_16.html and the Judgement of the European Courts of Human Rights Hirsi Jamaa et al. v. Italy, 23.02.2012, http://hudoc.echr.coe.int/sites/eng-press/pages/search.aspx#{%22display%22:[%221%22],%22dmdocnumber%22:[%22901572%22]}, both last visited on August 19th, 2015.

[102] Three of them (the PRISE studies and EUROBAROMETER 225), in addition to the approach by mail, also recruited their sample through media that do not necessarily exclude "marginal" people such as advertising in newspapers and personal

part of the sample, students, thus also contributing to overrepresent particular, non-deviant and non-marginal groups.

Six studies remain (in **bold** in Annex 3), which approach people in publicly accessible spaces such as streets, public means of transportation and shopping areas and which may also include in their sample so-called marginal and deviant people. In fact, one of them mentions three self-reportedly homeless people taking part in the interview.[103] None of these studies, however, tried actively to select their sample in a way that is representative of the people most targeted by surveillance.[104]

Since almost all the 15 studies, with the only exception of two, refer exclusively to visual surveillance, typically to CCTV, the following observations will deal with this kind of surveillance. As far as visual surveillance through CCTV is concerned, we may conclude that the perception of surveillance by its privileged targets is underrepresented and that they mostly assume an "internal" point of view with regard to the society and to Europe.

Consequently, there is a need to conduct surveys which give due weight to the points of view of those who are mostly affected by surveillance such as beggars, street-traders, alcoholics.

It remains to verify whether such conclusions apply to other surveillance areas as well, but this is a task for another day.

As to the developed methodology, the research carried out for this paper is pioneering work: as far as the authors know, no literature exists on how to specifically address perception issues in the design phase of new technologies.

Due to the initial character of such research, further developments on all the relevant topics, and in particular on MHbD, TbD and AbD is needed.

The part of the research that could rely more on existing literature is the part on MHbD. However, as we have seen, research so far has almost exclusively concentrated on PbD and related issues such as data protection. However, as argued above, the PbD approach is unsatisfactory for our purposes because its focus is both too broad and too narrow. On the one hand PbD, in spite of its name, merges different levels of intervention, not referring only to the design phase of new technologies but also targeting the whole life cycle of complex surveillance systems. On the other hand, PbD focuses only on information privacy, whereas there is a need to consider infractions of other fundamental rights and values as well, as I sought to do by introducing the notion of MHbD. Technical research in this direction, including proposals on how to design technologies in order to minimise their harm on individuals and society beyond privacy violations would be much welcome.

(Contd.)

contact. However, such changes were adopted not as a rule and not in order to compensate for the possible underrepresentation of "marginals", in this case homeless people.

[103] N. Zurawski, „It is all about perceptions', cit.

[104] The two studies from the URBAN EYE project also conducted "in depth" inteviews with "marginalised" persons and "deviants". However, this did not influence the results of their "quantitative" surveys.

References

Books and articles

- M. Apelt, N. Möllers, *Wie intelligente Videoüberwachung erforschen? Ein Resümee aus zehn Jahren Forschung zu Videoüberwachung*, Zeitschrift für Außen- und Sicherheitspolitik (2011), 4, 585–593.
- J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, I. Verbauwhede, *PrETP: Privacy-Preserving Electronic Toll Pricing*, 19th USENIX Security Symposium, 2010, 63–78.
- C. Bier, P. Birnstill, E. Krempel, H. Vagts, J. Beyerer, *Enhancing Privacy by Design From a Developer's Perspective*, Privacy Technologies and Policy, 2014, 73-85.
- K. Boers, P. Kurz, *Kriminalitätseinstellungen, soziale Milieus und sozialer Umbruch*, in K. Boers, G. Gutsche, K. Sessar (eds.), Sozialer Umbruch und Kriminalität in Deutschland, Opladen 1997, 187-254.
- B. Brown, *CCTV in Town Centres: Three case studies, Police Research Group. Crime Detection and Prevention Series*; Paper No. 68, 1995, <http://www.popcenter.org/responses /video_surveillance/pdfs/brown_1995_full.pdf>.
- D. Butin, M. Chicote, D. Le Metayer, *Log Design for Accountability*, 2012 IEEE Symposium on Security and Privacy Workshops, 2013, 1–7.
- A. Cavoukian, *Privacy by Design. The 7 Foundational Principles*, August 2009, <http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf/>.
- A. Cavoukian, *Surveillance, Then and Now: Securing Privacy in Public Spaces*, June 2013, http://www.privacybydesign.ca/index.php/paper/surveillance-then-and-now-securing-privacy-in-public-spaces/.
- D. Chaum, *Security without Identification: Transaction Systems to Make Big Brother Obsolete*, Commun. ACM, 28 (1985), 1030–1044.
- C. Diaz, E. Kosta, H. Dekeyser, M. Kohlweiss, G. Nigusse, *Privacy Preserving Electronic Petitions*, Identity in the Information Society, 1 (2008), 203–219.
- J. Ditton, Crime and the city. *Public Attitudes towards Open-Street CCTV in Glasgow*, The British Journal of Criminology, 40 (2000) 4, 692-709.
- J. DeCew, *Privacy*, in The Stanford Encyclopaedia of Philosophy, ed. by Edward N. Zalta, Fall 2013, 2013 <http://plato.stanford.edu/archives/fall2013/entries/privacy/>.
- G. Deleuze, *Post-scriptum sur les sociétés de contrôle*, L'autre journal, 1, Mai 1990.
- M. Foucault, *Surveiller et punir. Naissance de la prison*, Paris 1975.
- H.-H. Gander et al. (eds.), *Resilienz in der offenen Gesellschaft*, Symposium des Centre for Security and Society, Baden-Baden 2012.
- H.-H. Gander, *Sicherheitsethik – ein Desiderat? Mögliche Vorüberlegungen*, in: Ders. (ed.): *Resilienz in der offenen Gesellschaft*, Symposium des Centre for Security and Society, Baden-Baden 2012, 85-95.
- H.-H. Gander, G. Rischer (Hrsg.), *Sicherheit und offene Gesellschaft. Herausforderungen, Methoden und Praxis einer gesellschaftspolitischen Sicherheitsforschung*, Baden-Baden 2014.
- M. Gill et al., *Public perceptions of CCTV in residential areas: "It is not as good as we thought it would be"*, International Criminal Justice Review, 17(2007), 304-324.
- M. Gill, A. Spriggs, *Assessing the impact of CCTV*, Home Office Research Study 292, 2005, https://www.cctvusergroup.com/downloads/file/Martin%20gill.pdf.

- S. Gürses, C. Troncoso, C. Diaz *Engineering Privacy by Design*, <https://www.cosic.esat.kuleuven.be/publications/article-1542.pdf/>.
- L. Hempel, E. Töpfer, *The Surveillance Consensus: Reviewing the Politics of CCTV in Three European Countries*, European Journal of Criminology, 6 (2009), 2, 157-177.
- D. Kammerer, *Bilder der Überwachung*, Frankfurt am Main 2008.
- H-J. Lange, M. Gasch, *Subjektives Sicherheitsgefühl*, Wörterbuch zur inneren Sicherheit, Wiesbaden 2006, p. 323.
- D. Lyon (ed.), *Surveillance as social sorting: privacy, risk, and digital discrimination*, London 2003.
- M. Merleau-Ponty, *Phénoménologie de la perception*, Paris 1945.
- N. Möller at al., *Safety is More than the Antonym of Risk*, Journal of Applied Philosophy, 23 (2006), 4, 419-432.
- N. Möller, *The Concepts of Risk and Safety*, in S. Roeser, R. Hillerbrand, P. Sandin, M. Peterson (Eds.), *The Handbook of Risk Theory, Epistemology, Decision Theory, Ethics, and Social Implications of Risk*, Dordrecht etc. 2012.
- H. Münkler, *Strategien der Sicherung. Welten der Sicherheit und Kulturen des Risikos. Theoretische Perspektiven*, in H. Münkler, M. Bohlender, S. Meurer (eds.): *Sicherheit und Risiko. Über den Umgang mit Gefahr im 21. Jahrhundert*, Bielefeld 2010, 11-34.
- H. Münkler, M. Bohlender, S. Meurer (eds.): *Sicherheit und Risiko. Über den Umgang mit Gefahr im 21. Jahrhundert*, Bielefeld 2010.
- NG-Kruelle et al., *Biometrics and e-identity (e-passport) in the European Union: End-user perspectives on the adoption of a controversial innovation*, Journal of Theoretical and Applied Commerce Research, 1 (2006), 2, 12-35.
- C. Norris, G. Armstrong, *The maximum surveillance society*, Oxford 1999.
- D. Oberwittler, *Die Entwicklung von Kriminalität und Kriminalitätsfurcht in Deutschland – Konsequenzen für die Kriminalprävention*, Deutsche Zeitschrift für Kommunalwissenschaften, 42 (2003), 1, 31-52.
- A. T. O' Donnel et al., *Who is watching over you? The role of shared identity in perceptions of surveillance*, European Journal of Social Psychology, 40 (2010), 135–147.
- T. G. Patel, Surveillance, *Suspicion and Stigma: Brown Bodies in a Terror-panic Climate*, Surveillance&Society, 10 (2012), 3/4, 215-234.
- W. Peissl, *Surveillance and Security. A Dodgy Relationship*, 2002, http://www.oeaw.ac.at/ita/pdf/ita_02_02.pdf.
- K-H. Reuband, *Videoüberwachung. Was Bürger von der Überwachung halten*, Neue Kriminalpolitik, 13 (2001), 2, 5-9.
- S. Roeser, R. Hillerbrand, P. Sandin, M. Peterson (eds.), *The Handbook of Risk Theory, Epistemology, Decision Theory, Ethics, and Social Implications of Risk*, Dordrecht etc. 2012.
- B. Schneier, *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*, New York 2003.
- B. Schneier, *The Psychology of Security*, 2008, http://www.schneier.com/essay-155.html
- D. J. Solove, *The Digital Person. Technology and Privacy in the Information Age*, New York 2004.
- D.J. Solove*, I've got nothing to hide and other misunderstandings of privacy*, San Diego Law Review, 44 (2007), 745-772, p. 767.
- D.J. Solove, *Understanding Privacy*, Cambridge 2008.

- M. Schuler, L. Wolkenstein, *Psychologie und Sicherheitstechnologie – Psychologische Auswirkungen von Sicherheitstechnologien auf den Menschen und die Einstellung von Menschen dieser Technik gegenüber*, in H.-H. Gander, G. Rischer (eds.), *Sicherheit und offene Gesellschaft. Herausforderungen, Methoden und Praxis einer gesellschaftspolitischen Sicherheitsforschung*, Baden-Baden 2014.
- SuSi-PLUS, *Subjektives Sicherheitsempfinden im Personennahverkehr mit Linienbusse, U-Bahnen und Stadtbahnen*, Auszug aus dem Abschlussbericht: *Zusammenfassung und wichtigste Ergebnisse*, http://www.susi-team.de/images/stories/Downloads/band7summary.pdf, 2005.
- C. Taylor, *Sources of the Self. The Making of the Modern Identity*, Cambridge 1989.
- B. C. Welsh, D. P. Farrington, Home Office Research Study 252, *Crime prevention effects of closed circuit television: a systematic review*, 2002, http://www.popcenter.org/Responses/video_surveillance/PDFs/Welsh&Farrington_2002.pdf.
- D. J. Weitzner, H. Abelson, T. Berners-Lee, J. Feigenbaum, J. Hendler, G. J. Sussman, *Information Accountability*, Commun. *ACM*, 51 (2008), 82–87.
- L. Zedner, *Security*, London/New York 2009.
- N. Zurawski, *It is all about perceptions: CCTV, feelings of safety and perceptions of space - what the people say*, Security Journal, 23 (2010), 259-275.
- N. Zurawaski, Nils: *Kameras lösen keine Probleme*, ZEITonline, Available at: http://www.zeit.de/gesellschaft/schule/2011-11/schule-kamera-zurawski

EU-Directives and decisions

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data.
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector.
- Commission Implementing Decision C(2015) 102 final of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management, M530.

EU-Projects Deliverables and other documents

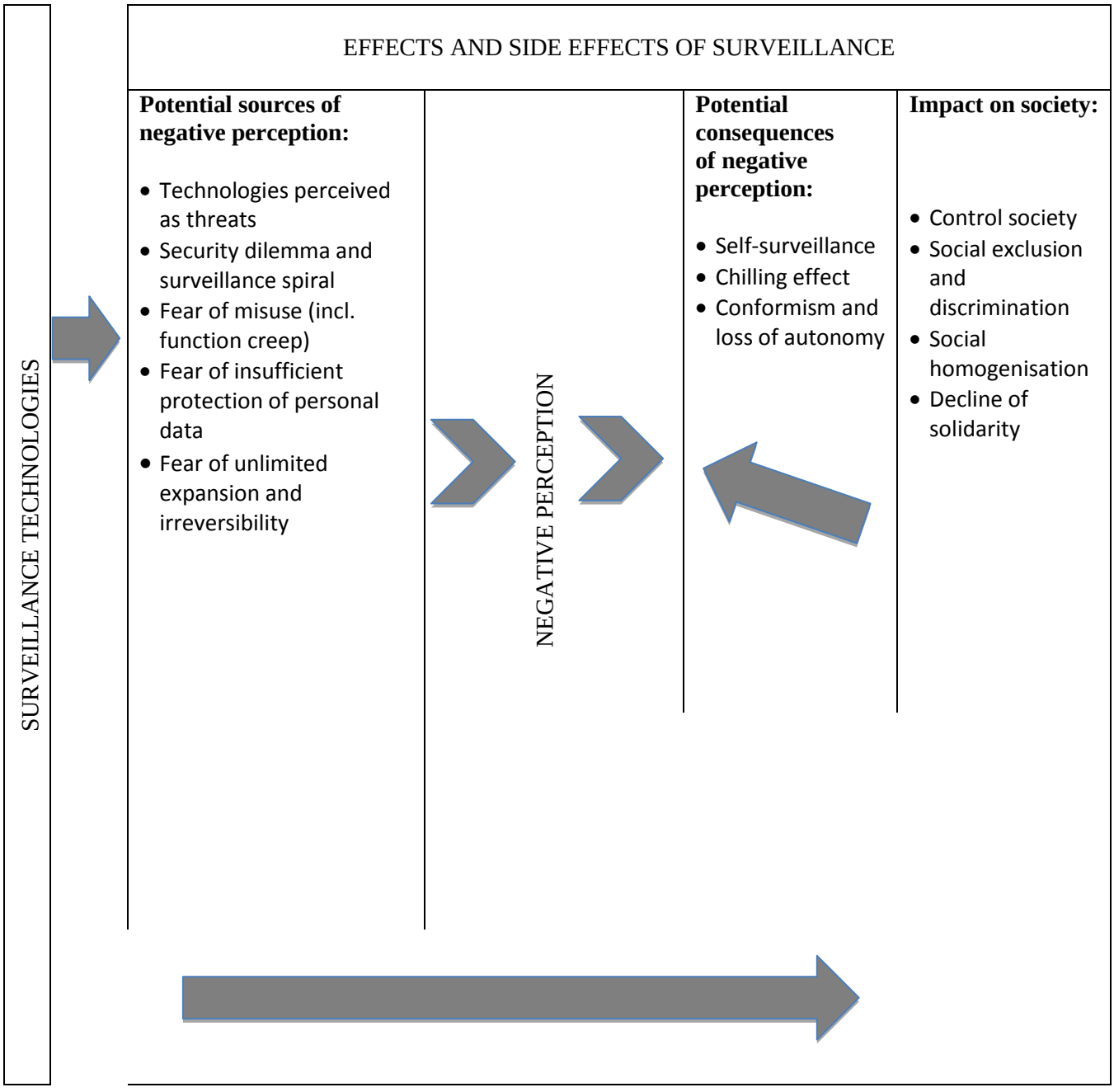
- DETECTER D 12.2.1, Quarterly Update on Technology 1, 2009, http://www.detecter.eu/index.php?option=com_content&view=section&id=7&layout=blog&Itemid=9.
- European Forum for Urban Security: Charter for a democratic use of video surveillance, 2010, http://www.cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Charta/CCTV_Charter_EN.pdf.
- PACT D1.4 Societal Impact Report, 2012, http://www.projectpact.eu/deliverables/wp1-root-branch-review/d1.4-social-impact-report.
- PRESCIENT, International Conference of the PRESCIENT Project, Berlin, 27-28 November 2012, Session 3: 1. Accountability by Design for Privacy, http://prescient-project.eu/prescient/inhalte/download/prescient2012.pdf.
- SOCTA 2013, Serious and Organised Crime Threat Assessment, p. 41, https://www.europol.europa.eu/content/eu-serious-and-organised-crime-threat-assessment-socta.

- SurPRISE D3.2, Report on regulatory frameworks concerning privacy and the evolution of the norm of the right to privacy, March 2013, http://surprise-project.eu/wp-content/uploads/2013/06/SurPRISE_D3.2_Report-on-regulatory-frameworks-concerning-privacy-for-final-formatting_v094.pdf.
- SURVEILLE Project Consortium, Description of Work of the Surveillance Project: Ethical Issues, Legal Limitations and Efficiency, 2011, internal document.
- SURVEILLE D2.3, Paper by local authorities end users, February 2013, http://surveille.eui.eu/wp-content/uploads/2015/04/D2.3-Paper-by-Local-Authorities-End-Users.pdf.
- SURVEILLE D3.1, Report describing the design of the research apparatus for the European level study of perceptions, 2012, http://surveille.eui.eu/wp-content/uploads/2015/04/D3.1-Report-describing-the-design-of-the-research-apparatus.pdf.
- SURVEILLE D3.2, Review of European level studies on perceptions of surveillance. Negative perception, effects, side effects and perceived effectiveness, September 2013, http://surveille.eui.eu/wp-content/uploads/2015/04/D3.2-Review-of-European-level-studies-on-perceptions.pdf.
- SURVEILLE D3.3, Report on system effectiveness, efficiency and satisfaction assessment, September 2013, http://surveille.eui.eu/wp-content/uploads/2015/04/D3.3-System-effectiveness-efficiency-and-satisfaction-assessment.pdf.
- SURVEILLE D3.4, Design a research methodology for assessing the effectiveness of selected surveillance systems in delivering improved security, September 2013, http://surveille.eui.eu/wp-content/uploads/2015/04/D3.4-Design-of-a-research-methodology-for-assessing.pdf.
- SURVEILLE D3.6, Report on methodology and criteria for incorporating perception issues in the design phase of new surveillance systems, December 2013, http://surveille.eui.eu/wp-content/uploads/2015/04/D3.6-Report-on-methodology-and-criteria-for-incorporating-perception-issues.pdf.

Surveys and meta-studies

See Annex 2

Annex 1: Table of effects and side effects of surveillance



Annex 2: List of studies on the perception of surveillance

Year	Project/author	Title	Publication place	P	NP	E/SE	P&E	Type of surveillance
1999	S. Graham et al.	Towns on the Television: Closed Circuit TV Surveillance in British towns and cities	http://www.ncl.ac.uk/			✓		Visual
2000	J. Ditton	Crime and the city. Public Attitudes towards Open-Street CCTV in Glasgow	The British Journal of Criminology, 40 (2000) 4, 692-709			✓	✓	Visual
2001	G. Klocke et al.	Das Hintertürchen des Nichtwissens	Bürgerrechte & Polizei: CILIP, 69 (2001) 2, http://www.cilip.de				✓	Visual
2001	K-H. Reuband	Videoüberwachung. Was Bürger von der Überwachung halten	Neue Kriminalpolitik, 13 (2001), 2, 5-9				✓	Visual
2002	B. C. Welsh, D. P. Farrington	Home Office Research Study 252, Crime prevention effects of closed circuit television: a systematic review	http://www.popcenter.org/				✓	Visual
2004	URBAN EYE	WP 15: CCTV in Europe, Final Report	http://www.urbaneye.net/		✓	✓		Visual
2004	URBAN EYE	WP 13, What do people think of CCTV. Findings from a Berlin Survey	http://www.urbaneye.net/			✓	✓	Visual
2005	M. Gill, A. Spriggs	Assessing the impact of CCTV, Home Office Research Study 292	https://www.cctvusergroup.com/				✓	Visual
2005	C. Ketzer	Securitas ex Machina. Von der Bedeutung technischer Kontroll- und Überwachungssysteme für Gesellschaft und Pädagogik	http://kups.ub.uni-koeln.de			✓		Visual

2006	NG-Kruelle et al.	Biometrics and e-identity (e-passport) in the European Union: End-user perspectives on the adoption of a controversial innovation	Journal of Theoretical and Applied Commerce Research, 1 (2006), 2, 12-35 http://www.jtaer.com/			✓		Biometrics
2006	Chen-Yu Lin	Öffentliche Videoüberwachung in den USA, Großbritannien und Deutschland – Ein Drei-Länder-Vergleich	http://ediss.uni-goettingen.de/			✓	✓	Visual
2006	EPTA	ICT and Privacy in Europe. Experiences from technology assessment of ICT and Privacy in seven different European countries	http://www.ta-swiss.ch			✓		Visual Biometrics Communication Data Location
2007	M. Gill et al.	Public perceptions of CCTV in residential areas : "It is not as good as we thought it would be"	International Criminal Justice Review 17(2007), 304-324			✓	✓	Visual
2008	Gallup Organization	EUROBAROMETER 225 – Data Protection in the European Union. Citizens' perceptions	http://ec.europa.eu/public_opinion/index_en.htm		✓			Data
2008	V. Pavone, M. Pereira	The privacy Vs security dilemma in a risk society. Insights from the PRISE project on the public perception of new security technologies in Spain	http://www.wiscnetwork.org			✓		Visual Biometrics Communication Data Location Sensors
2008	PRISE	D5.8, Synthesis Report - Interview Meetings on Security Technology and Privacy	http://www.prise.oeaw.ac.at/			✓	✓	Visual Biometrics Communication Data Location Sensors
2009	D. Williams, J. Ahmed	The Relationship Between Antisocial Stereotypes and Public CCTV Systems:	https://uhra.herts.ac.uk			✓	✓	Visual

		Exploring Fear of Crime in the Modern Surveillance Society						
2009	L. Hempel, E. Töpfer	The Surveillance Consensus : Reviewing the Politics of CCTV in Three European Countries	European Journal of Criminology, 6 (2009), 2, 157-177			✓	✓	Visual
2010	A. T. O' Donnel et al.	Who is watching over you? The role of shared identity in perceptions of surveillance	European Journal of Social Psychology, 40 (2010), 135–147	✓				Visual
2010	N. Zurawski	'It is all about perceptions': CCTV, feelings of safety and perceptions of space - what the people say	Security Journal, 23 (2010), 259-275			✓	✓	Visual
2010	CPSI	Analytical Standpoint 13, Summary of CPSI Country Case Studies	http://www.esci.at				✓	
2011	C. Bozzoli, C. Müller	Perceptions and attitudes following a terrorist shock: Evidence from the UK	European Journal of Political Economy, 27 (2011), 89-106	✓				
2011	W. Peissl et al.	Aktuelle datenschutzrechtliche Fragen der Videoüberwachung	http://epub.oeaw.ac.at/			✓		Visual
2011	M. Apelt, N. Möllers	Wie intelligente" Videoüberwachung erforschen? Ein Resümee aus zehn Jahren Forschung zu Videoüberwachung	Zeitschrift für Außen- und Sicherheitspolit (2011), 4, 585–593			✓	✓	Visual
2012	PRESCIENT	D3, Privacy, data protection and ethical issues in new and emerging technologies: Assessing citizens' concerns and knowledge of stored personal data	http://www.prescient-project.eu/	✓				Data
2012	SAPIENT	Deliverable 1.1: Smart Surveillance – State of the Art	http://www.sapientproject.eu	✓				Visual Biometrics Communication Data Location Sensors

2012	PACT	Summary of PACT deliverables D1.1 - D1.6	http://www.projectpact.eu/documents-1			✓		Visual Biometrics Communication Data Location Sensors
2012	PACT	D1.4 Societal Impact Report	http://www.projectpact.eu/			✓	✓	Visual Data
2013	PRISMS	D7.1: Report on Existing Surveys	http://prismsproject.eu	✓				Visual Biometrics Communication Data Location

P = Perception in general
NP = European Overview on negative perception
E/SE = Effect and side effects
P&E = Perception and effectiveness

Annex 3: Recruitment strategy of the studies

Year	Project/author	Title	Sample size	Recruitment strategy / Targeted people	Type of surveillance
1999	S. Graham et al.	Towns on the Television: Closed Circuit TV Surveillance in British towns and cities		Pre-existing studies	Visual
2000	J. Ditton	Crime an the city. Public Attitudes towards Open-Street CCTV in Glasgow	3.074	Street interviews with local residents	Visual
2001	G. Klocke et al.	Das Hintertürchen des Nichtwissens	120	Street interviews with residents, randomly selected	Visual
2001	K-H. Reuband	Videoüberwachung. Was Bürger von der Überwachung halten	1.568	Mail. Addresses randomly selected from the residents' (18+) register	Visual
2002	B. C. Welsh, D. P. Farrington	Home Office Research Study 252, Crime prevention effects of closed circuit television: a systematic review		Pre-existing studies	Visual
2004	**URBAN EYE**	**WP 15: CCTV in Europe, Final Report**	**1.001 resp.**	**Street interviews**	**Visual**
2004	**URBAN EYE**	**WP 13, What do people think of CCTV. Findings from a Berlin Survey**	**203**	**Street interviews outside shopping malls**	**Visual**
2005	**M. Gill, A. Spriggs**	**Assessing the impact of CCTV, Home Office Research Study 292**	**13.104**	**s. Gill 2007**	**Visual**
2005	**C. Ketzer**	**Securitas ex Machina. Von der Bedeutung technischer Kontroll- und Überwachungssysteme für Gesellschaft und Pädagogik**	**12**	**Users of public transportation**	**Visual**
2006	*NG-Kruelle et al.*	*Biometrics and e-identity (e-passport) in the European Union: End-user perspectives on the adoption of a*	*269*	*Internet survey with EU-citizens: MBA students*	*Biometrics*

		controversial innovation			
2006	Chen-Yu Lin	Öffentliche Videoüberwachung in den USA, Großbritannien und Deutschland – Ein Drei-Länder-Vergleich		Pre-existing studies	Visual
2006	EPTA	ICT and Privacy in Europe. Experiences from technology assessment of ICT and Privacy in seven different European countries		Pre-existing studies	Visual Biometrics Communication Data Location
2007	M. Gill et al.	Public perceptions of CCTV in residential areas : "It is not as good as we thought it would be"	9.121	In-home interviews with residents. Households selected through random sampling method	Visual
2008	Gallup Organization	EUROBAROMETER 225 – Data Protection in the European Union. Citizens' perceptions	27.000	Typically: Landline-telephone interviews. Also: personal interviews (15+)	Data
2008	V. Pavone, M. Pereira	The privacy Vs security dilemma in a risk society. Insights from the PRISE project on the public perception of new security technologies in Spain	25-35	Spanish citizens. For recruitment strategy s. PRISE D5.8.	Visual Biometrics Communication Data Location Sensors
2008	PRISE	D5.8, Synthesis Report - Interview Meetings on Security Technology and Privacy	158	Typically: invitation by mail for interview meetings. Also: phone; advertising	Visual Biometrics Communication Data Location Sensors
2009	**D. Williams, J. Ahmed**	**The Relationship Between Antisocial Stereotypes and Public CCTV Systems: Exploring Fear of Crime in the**	**120**	**Visitors of the central public shopping area.**	**Visual**

		Modern Surveillance Society		**Randomly selected**	
2009	L. Hempel, E. Töpfer	The Surveillance Consensus : Reviewing the Politics of CCTV in Three European Countries		Existing studies	Visual
2010	*A. T. O' Donnel et al.*	*Who is watching over you? The role of shared identity in perceptions of surveillance*	*251*	*Visitors of the city centre (16+) and students in a British University*	*Visual*
2010	**N. Zurawski**	**'It is all about perceptions': CCTV, feelings of safety and perceptions of space - what the people say**	**216**	**Visitors of the "amusement district" in the city centre. Random approach (3 homeless)**	**Visual**
2010	CPSI	Analytical Standpoint 13, Summary of CPSI Country Case Studies		Pre-existing surveys	
2011	C. Bozzoli, C. Müller	Perceptions and attitudes following a terrorist shock: Evidence from the UK		Pre-existing surveys	
2011	W. Peissl et al.	Aktuelle datenschutzrechtliche Fragen der Videoüberwachung		Pre-existing surveys	Visual
2011	M. Apelt, N. Möllers	Wie intelligente" Videoüberwachung erforschen? Ein Resümee aus zehn Jahren Forschung zu Videoüberwachung		Pre-existing surveys	Visual
2012	PRESCIENT	D3, Privacy, data protection and ethical issues in new and emerging technologies: Assessing citizens' concerns and knowledge of stored personal data		Pre-existing surveys	Data
2012	SAPIENT	Deliverable 1.1: Smart Surveillance – State of the Art		Pre-existing surveys	Visual Biometrics Communication Data Location Sensors

2012	PACT	Summary of PACT deliverables D1.1 - D1.6		Pre-existing surveys	Visual Biometrics Communication Data Location Sensors
2012	PACT	D1.4 Societal Impact Report		Pre-existing surveys	Visual Data
2013	PRISMS	D7.1: Report on Existing Surveys		Pre-existing surveys	Visual Biometrics Communication Data Location

Studies whose sample selecting strategy excludes non-resident persons.
Studies that specifically target students, at least as a part of the sample.
Studies whose sample recruitment strategy potentially includes so-called marginal and deviant people.

Annex 4: List of FP6 and FP7 projects relevant for issues on surveillance perceptions

FP6

- BITE - Biometric Identification Technologies Ethics, http://www.biteproject.org
- HUMABIO - Human monitoring and authentication using biodynamic indicators and behavioural analysis, www.humabio-eu.org

FP 7

- CPSI - Changing Perceptions of Security and Interventions, www. cpsi-fp7.eu
- DETECTER - Detection Technologies, Terrorism, Ethics, and Human Rights, http://www.detecter.eu/
- HIDE- Homeland Security, Biometric Identification & Personal Detection Ethics, http://www.hideproject.org/
- IRISS - Increasing Resilience in Surveillance Societies, http://irissproject.eu/
- PACT - Public perception of security and privacy: Assessing knowledge, Collecting evidence, Translating research into action, http://www.projectpact.eu/
- PRACTIS - Privacy – Appraising Challenges to Technologies and Ethics, www.practis.org
- PRISE - Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies, http://www.prise.oeaw.ac.at/.
- PRISMS - The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making, http://prismsproject.eu/
- RESPECT - Rules, Expectations & Security through Privacy-Enhanced Convenient Technologies, http://respectproject.eu/
- RISE - Rising Pan European & International Awareness of Biometrics & Security Ethics. For details see the project's website: http://www.riseproject.eu/
- SAPIENT - Supporting fundamental rights, Privacy and Ethics in Surveillance Technologies, http://www.sapientproject.eu/
- SMART – Scalable Measures for Automated Recognition Technologies, http://www.smartsurveillance.eu/
- SurPRISE - Surveillance, Privacy and Security. A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe, www.surprise-project.eu/

Annex 5: Table summarising methodology for incorporating perception issues in the design of new technologies

<table>
<tr><td>Domain</td><td>NEGATIVE PERCEPTIONS</td><td>PERCEIVED EFFECTIVENESS</td></tr>
<tr><td rowspan="2">BA</td><td colspan="2">BACKGROUND CONDITIONS
↓↓</td></tr>
<tr><td>Check for side-effects:
1. Technologies perceived as threats;
2. Security dilemma and surveillance spiral;
3. Fear of misuse (incl. function creep);
4. Fear of insufficient protection of personal data;
5. Fear of unlimited expansion and irreversibility.
6. Self-surveillance;
7. Chilling effect;
8. Conformism and loss of autonomy.
9. Control society;
10. Social exclusion and discrimination;
11. Social homogenisation;
12. Decline of solidarity.
↓</td><td>Is the use of technology effective in the particular context?
↓</td></tr>
<tr><td>1st level</td><td>MHbD</td><td>Effectiveness improvement</td></tr>
<tr><td>2nd level</td><td>TbD</td><td>TbD</td></tr>
<tr><td>3rd level</td><td>AbD</td><td>/</td></tr>
<tr><td>Beyond design</td><td colspan="2">Social – institutional – political- legal measures</td></tr>
</table>