Project acronym:	SAPIENT
Project title:	Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies
Project number:	261698
Programme:	Seventh Framework Programme for research and technological development
Objective:	SEC-2010.6.5-2: Use of smart surveillance systems, data protection, integrity and sharing information within privacy rules
Contract type:	Collaborative project
Start date of project:	1 February 2011
Duration:	36 months

Deliverable 1.1:
Smart Surveillance – State of the Art

Editors:	Michael Friedewald (Fraunhofer ISI), Rocco Bellanova (VUB)
Authors:	Rocco Bellanova, Matthias Vermeulen, Serge Gutwirth (VUB), Rachel Finn, Paul McCarthy, David Wright, Kush Wadhwa (Trilateral), Dara Hallinan, Michael Friedewald (Fraunhofer ISI), Marc Langheinrich, Vlad Coroama (USI), Julien Jeandesboz, Didier Bigo, Mervyn Frost (KCL), Silvia Venier (CSSC)
Dissemination level:	Public
Deliverable type:	Report
Version:	1.0
Due date:	31 August 2011
Submission date:	23 January 2012

About the SAPIENT project

The SAPIENT project that is expected 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. In addition to addressing these core research goals, the project will entail the development and validation of scenarios around future smart surveillance systems, and will apply the best elements of existing PIA (privacy impact assessment) methodologies to construct a surveillance related PIA framework.

The work of the project will lead to a practical handbook which will help policy makers, technology developers and other stakeholders to better understand how and when smart surveillance should be used, and apply criteria to assure that such systems respect the privacy of citizens.

Terms of use

This document was developed within the SAPIENT project (see http://www.sapientproject.eu), co-funded by the European Commission within the Seventh Framework Programme (FP7), by a consortium, consisting of the following partners:

- Fraunhofer Institute for Systems and Innovation Research (Fraunhofer ISI), co-ordinator,
- Trilateral Research & Consulting LLP,
- Centre for Science, Society and Citizenship (CSSC),
- Vrije Universiteit Brussel (VUB),
- Università della Svizzera italiana (USI),
- King's College London (KCL), and
- Centre for European Policy Studies (CEPS)

This document may be freely used, copied, and distributed provided that the document itself is not modified or shortened, that full authorship credit is given, and that these terms of use are not removed but included with every copy. The SAPIENT partners shall take no liability for the completeness, correctness or fitness for use. This document is subject to updates, revisions, and extensions by the SAPIENT consortium. Address questions and comments to: feedback@sapientproject.eu

Document history

Version	Date	Changes
1.0	23 January 2012	First version of deliverable

CONTENTS

INTRODUCTION 1

1 ELEMENTS FOR AN ANALYSIS OF THE HISTORY AND CONTEMPORARY TRENDS OF SURVEILLANCE IN EUROPE 5

1.1 Living in surveillance societies: surveillance as routine 6

1.2 The historicity of surveillance and the activity of governing 7

1.3 Surveillance, Panopticism and assemblages 9

1.4 Surveillance, security and normalisation 11

1.5 Dataveillance, prediction and profiling 14

1.6 Lateral surveillance: vigilantism, voluntarism, voyeurism and counter-surveillance 16

1.7 Surveillance and resistance 17

1.8 Conclusions 20

2 EMERGING SMART SURVEILLANCE TECHNOLOGIES 23

2.1 Introduction 23

2.2 Technologies and applications 23
2.2.1 Visual surveillance 23
2.2.2 Dataveillance 28
2.2.3 Biometrics 34
2.2.4 Communications surveillance 39
2.2.5 Sensors 44
2.2.6 Location determination technologies 48
2.2.7 Summary 53

2.3 Functions 53
2.3.1 Identify 53
2.3.2 Verify, authenticate and authorise 55
2.3.3 Detect/monitor 56
2.3.4 Locate/track 58
2.3.5 Collect information 59
2.3.6 Link information (profiling) 60
2.3.7 Summary 61

2.4 Stakeholders and drivers 61
2.4.1 Surveillants, surveilled and other stakeholders 61
2.4.2 Technological drivers 65
2.4.3 Economic drivers 65
2.4.4 Political drivers 66
2.4.5 Social drivers 67
2.4.6 Summary 68

2.5 Purposes 68
2.5.1 Border control 68
2.5.2 Anti-terrorism and criminal justice 69
2.5.3 Airport security 69

2.5.4 Transport access and security 70
2.5.5 Retail security and fraud prevention 70
2.5.6 Local authority/social service investigations, etc. 70
2.5.7 Entertainment (Television shows, "selling newspapers") 71
2.5.8 Summary 71

2.6 Major smart surveillance research initiatives 72
2.6.1 Foresight studies 73
2.6.2 European Security Research and Innovation Forum 74
2.6.3 Top priorities and funded projects 75
2.6.4 The ethical, social and legal aspects of EU and US surveillance research 76
2.6.5 Analysis 77

2.7 Emergent technologies and assemblages 79
2.7.1 Technologies 79
2.7.2 Future smart surveillance assemblages 80

2.8 Conclusions and critical parts 83

3 A FUNDAMENTAL RIGHTS ANALYSIS OF SMART SURVEILLANCE 85

3.1 Review of existing laws and principles applicable to surveillance 85
3.1.1 General principles on the use of surveillance technologies according to the article 8 jurisprudence of the European Court of Human rights 88
3.1.2 General principles on the use of surveillance technologies in EU law 92

3.2 Review of existing laws and principles applicable to surveillance 97
3.2.1 Fundamental rights aspects of new image analysis algorithms in smart CCTV systems 98
3.2.2 Fundamental rights aspects of new sensor systems: the case of body scanners 104
3.2.3 The Passenger Name Records System(s) 107

3.3 "Law on the Move": Current EU legislative evolutions 112
3.3.1 The revision of the Data Protection Directive 113
3.3.2 The evaluation and revision of the Data Retention Directive 118
3.3.3 Other EU developments 120
3.3.4 The CoE Committee of the Ministers on profiling 122

3.4 Conclusions: Some elements to go beyond the state of the art 124

4 CITIZENS' PERCEPTIONS ON SURVEILLANCE AND PRIVACY 129

4.1 On public opinion surveys in general 131
4.1.1 Survey Motivation 132
4.1.2 Methodology 133
4.1.3 Restriction to Use in the Policy Process 135
4.1.4 Discussion 136

4.2 What Does the Public Know about Data Protection and Privacy? 137
4.2.1 There Is More Then One 'Public' 138
4.2.2 What Does the Public Know About the Current Protection Framework? 139
4.2.3 Privacy, Data Protection and Security 141
4.2.4 Public View of the Regulatory Environment 145
4.2.5 Effectiveness of Regulation in Light of Environment 154
4.2.6 Conclusion 155

4.3 Public Perception of Surveillance Technologies 156
4.3.1 CCTV and Other Technologies 156
4.3.2 Factors Affecting Public Opinion 169

4.3.3 Public Opinion Generally Lacks Solid Understanding or a Factual Base On Technologies Themselves 171
4.3.4 Fears 173
4.3.5 Public Desires 174
4.3.6 Conclusion 175

4.4 The academic discourse on Public Perception of Privacy and Security 175
4.4.1 New technologies: Public understanding and engagement 176
4.4.2 Surveillance societies, theories of modern and post-modern governance 178
4.4.3 Theories on the Information and Risk Society 180
4.4.4 Engaging the social sciences 181
4.4.5 Theoretical insights dealing with public acceptance 183

5 DISCOURSES AND POLITICS OF SECURITY AND SURVEILLANCE, PRIVACY AND DATA PROTECTION 185

5.1 Introduction 185

5.2 Empirical and analytical parameters 186
5.2.1 Empirical focus 186
5.2.2 Analytical framework 187
5.2.3 Argument 190

5.3 Assembling security and technology 191
5.3.1 A starting point: envisaging the next steps in security research in the EU 192
5.3.2 Assembly process #1: reforming and organising the "defence-related" market 193
5.3.3 Assembly process #2: the industry and the construction of a security market 198
5.3.4 Assembly process #3: technology and the "internal security market" 203

5.4 Controversies about security, surveillance and technology 209
5.4.1 Controversies over security and the shift towards surveillance 209
5.4.2 The implications of surveillance and the question of ethics 214
5.4.3 Privacy advocates versus surveillance advocates? Controversies about privacy and data protection 219

5.5 Conclusions: Smart surveillance and its implications for freedom 223

Introduction

Rocco Bellanova (VUB-LSTS), Michael Friedewald (Fraunhofer ISI)

Smart-phones and smart-televisions, smart-weapons and smart-sanctions, smart-regulations and smart-borders: the number of elements that are becoming smart is continuously increasing. 'Smart' seems to be one of the most successful key-words, or better key-adjective, at least in terms of labelling. However, the 'smart' turn does not appear a univocal phenomenon, and often the same adjective means different things and presupposes different patterns of evolution.

Then, within such a widening and fragmented panorama, how to understand, to analyze and to assess what is becoming to be known as 'smart surveillance? Or, in other words, what is smart surveillance, and how to apprehend it?

Indeed, while the notion of smart surveillance could be seductive from an academic and a policy point of view, caution in its 'automatic use' is particularly needed, since its diffusion is still relatively recent, and little specific attention has being dedicated to it so far. In this sense, and given the crucial and sensitive role of surveillance in government, caution is also needed in order to ensure first a common ground of debate, and then discuss about possible applications and relative safeguards.

For these reasons, this deliverable is a fundamental element in the architecture of the entire SAPIENT research project, as it aims at providing a comprehensive state of the art of smart surveillance. This implies to situate smart surveillance vis-à-vis the history and trends of surveillance in Europe; to identify the main technologies and practices at stake; to assess the most relevant existing legal frameworks; to analyze citizens' perceptions; and to study the main discourses and politics of security and surveillance.

Still, as a sort of preliminary move, it has been crucial to set a common working definition, so to ensure to the consortium shared elements of reference in their researches. The output of this first collective research exercise is the following:

> **Smart Surveillance**: surveillance systems that are capable of extracting application-specific information from captured information (be it digital images, call logs or electronic travel records) in order to generate high-level event descriptions that can ultimately be used to make automated or semi-automated decisions. Smart surveillance systems inherently offer a high level of scalability, as they in turn can act as input to other surveillance systems. Smart surveillance systems contribute to social reconfigurations in ways that essentially differ from previous surveillance techniques, especially by introducing new folding processes of the spatial and temporal dimensions with the purpose to go beyond 'mere' re-action.

Such a definition works as a '*fil rouge*' through the following five chapters that compose the state of the art. All of them refer, implicitly or explicitly, to this working definition as the reference point of their specific approach, legal, ethical, sociological, politological or technological. This definition permits also to 'measure' the eventual differences and overlaps

with the ways and modes in which 'other types' of surveillance have been already, or are currently, approached and apprehended.

The **first chapter** surveys the recent history of and contemporary trends in surveillance in Europe. We dedicate particular attention to the body of literature that has explicitly taken surveillance as its core object – "surveillance studies" – and examine the conceptual assumptions, fields of inquiry and insights that have driven these investigations in recent years. In particular, we focus the discussion on the relationship between surveillance and liberties, with the aim of providing some conceptual background to SAPIENT's analysis of smart surveillance. One of the main outputs that emerge from this survey is that surveillance is embedded in the governmental practices of liberal regimes. Also, surveillance is no longer correlated solely to a disciplinary logic that entails a vertical exercise of authority, but surveillance practices currently stand in relation to a logic of normalization: they operate through freedom, rather than in negation of it.

The **second chapter** examines today's surveillance society through the lens of current and emerging technologies. Based on the review and analysis of academic articles, policy documents and reports, press stories and research projects, it identifies the different kinds of surveillance technologies prevalent in our society today and those that are emerging in the near future. Such a comprehensive exercise is crucial to present both families and specific types of surveillance technologies, and to describe their functioning. This chapter reviews also the main stakeholders and the main drivers linked to the emergence or development of these technologies. These analyses highlight the ways in which both current and emerging technologies are increasingly being organized into assemblages or "smart surveillance" systems, where surveillance systems are becoming integrated, multi-modal, automated, ubiquitous and increasingly accepted by the public.

The **third chapter** addresses smart surveillance from a legal point of view. This is a challenging task, since there is currently no proper legal definition available for what constitutes 'smart' surveillance. In order to provide a clearer idea about the legal frameworks that are relevant for the use of smart surveillance technologies, this chapter first reviews existing laws and principles that are relevant to the use of surveillance technologies in general, focusing in particular on the right to privacy and data protection. Then, these laws and principles are 'applied' or tested to a number of smart surveillance technologies in order to assess their potential intrusiveness into a range of fundamental rights, including due process and non-discrimination. Finally, as legislation in the field of data protection is currently undergoing critical changes, the chapter passes under review the most important developments from the perspective of the impact on, and development of, smart surveillance. Based on this analysis, in its conclusions, the chapter advances some elements for further reflection, *inter alia*: the crucial role of the principle of data minimization; the growing issue of discrimination; the need to ensure a consistent approach in terms of data protection over private-public surveillance partnership; the somehow paradoxical sidelining of the right to privacy from current legislative developments, in favor of the right to data protection.

The **fourth chapter** focuses on citizens' perceptions on surveillance, especially in relation to privacy. Indeed, researchers have investigated public perceptions and attitudes towards surveillance practices and surveillance technologies, and the media have duly reported their findings. Public opinion plays an increasingly role in development and deployment of surveillance technologies and in the policy planning and decision-making process, in the private and public sectors. We do not only consider findings from various studies exploring

privacy, data protection and security issues, but we also explore the difficulties, bias, methodological challenges and drivers of these studies.

The **fifth** and conclusive **chapter** focuses on discourses and politics of surveillance and security. It supplements the research efforts presented so far by providing elements for a sociological analysis of smart surveillance. Our purpose is, firstly, to examine how smart surveillance has become a pertinent item in the EU's security policies. Insofar as the 'object' of smart surveillance is sustained by references to the importance of advanced or sophisticated technologies, we take EU efforts in supporting research and development for technologies in the field of security as a starting, "local" point of investigation. We focus on the assembling of security and technology, on the different operations of translation that have assembled security technologies as a relevant object for policy, research and scholarship. At stake here is the understanding of the functional narrative that frames 'advanced' technology as a natural response to contemporary insecurities. Such a critical analysis led us to suggest that emerging references to smart surveillance should be interpreted in the light of multiple controversies over the relation between security, surveillance and technology which do not only involve technical discussions on cost-efficiency and feasibility, but also involve judgements about which contemporary developments are considered to be threatening, how they should be met, and with which implications. Finally, an important element to be highlighted is that two understandings of 'smartness' in surveillance are currently emerging: one which envisages smartness as the technical possibility in a culture of 'data-sharing by default' to sift through massive amounts of personal data to detect persons deemed to be a risk, and the other which considers smartness as the technical possibility to 'minimise' the impact of surveillance on fundamental freedoms and rights.

1 Elements for an analysis of the history and contemporary trends of surveillance in Europe

Julien Jeandesboz, Didier Bigo, Mervyn Frost (KCL)

The first chapter of this deliverable surveys the recent history of and contemporary trends in surveillance in Europe. We dedicate particular attention to the body of literature that has explicitly taken surveillance as its core object – "surveillance studies" – and examine the conceptual assumptions, fields of inquiry and insights that have driven these investigations in recent years.

We focus the discussion on the relationship between surveillance and liberties, with the aim of providing some conceptual background to SAPIENT's analysis of smart surveillance. The discussion focuses on the relationship between surveillance and liberties. How can we analyse surveillance practices in liberal regimes? How are these practices, whether they are enacted through private or public agencies, problematised in such regimes? Smart surveillance may be characterised as a more acceptable form of surveillance, as a means to avoid the totalitarian connotations associated with generalised surveillance. Yet, as the literature surveyed in the following pages makes amply clear, surveillance is embedded in the governmental practices of liberal regimes. The Orwellian framing of surveillance as a centralised, authoritarian process, then, is misleading.[1] It is only against this background of surveillance as a routine activity in liberal societies – a view encapsulated in scholarly arguments under the notion of "surveillance societies" – that smart surveillance makes sense.

To make such an argument, we need to alter our understanding of surveillance. Surveillance has traditionally been framed, following in particular the work of Michel Foucault on punishment, as a hierarchical process informed by a disciplinary logic of tutoring and improvement. Persons under surveillance are viewed as the metaphorical inmates of Bentham's Panopticon, upon which Foucault comments at length in his classic work *Discipline and Punish*. The analysis of surveillance in panoptic terms, however, has been increasingly criticised over the past decade. Surveillance, some scholars argue, should be regarded as rhizomatic rather than panoptic, as a heterogeneous and contested process involving sometimes disjointed assemblages of technologies and practices, subject to contests, controversies, struggles and resistance. Contemporary trends in surveillance practices, they further argue, should be understood less in relation to the political technology of discipline than in relation to security. The distinction, here, involves Foucault's later work on security and normalisation, which accounts for the part that Foucault plays both in the literature on surveillance and in the present section. While discipline is associated with *normation* – the detailed administration of persons, including through their bodies and minds, according to a pre-established norm – security is tied with *normalisation*, that is, the idea that the "natural"

[1] "Orwellian", here, refers more to the use that surveillance studies have made of the work of Orwell, particularly *1984*, than to the political thinking of this writer. *1984*, one could argue, is more a discussion of and parable on the mechanisms of obedience and of the complacency of the British middle class of Orwell's time towards established patterns of order than it is about the totalitarian exercise of power.

processes at work within a human collective should be regulated from within, rather than administrated from outside and above. Surveillance as a rhizomatic process of normalisation still allows for the "plugging-in" of the logics of sovereignty and discipline, but these are no longer the predominant rationality of rule at work in contemporary European societies. The correlation of surveillance with security and normalisation, in turn, accounts for the growing focus of contemporary surveillance practices on the electronic processing of personal data, a trend coined in the literature as "dataveillance". It is also reflected in the growing emphasis on practices of "lateral" surveillance, on self-surveillance and mutual surveillance among subjects to be governed.

1.1 LIVING IN SURVEILLANCE SOCIETIES: SURVEILLANCE AS ROUTINE

The shaping of "surveillance societies" in Europe is a concern shared by scholars, public bodies and civic organisations alike.[2] As a preliminary working definition, surveillance can be understood following the terms of David Lyon as

> the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction. Surveillance directs its attention in the end to individuals (even though aggregate data, such as those available in the public domain, may be used to build up a background picture). It is focused. By systematic, I mean that this attention to personal details is not random, occasional or spontaneous; it is deliberate and depends on certain protocols and techniques. Beyond this, surveillance is routine; it occurs as a 'normal' part of everyday life in all societies that depend on bureaucratic administration and some kinds of information technology. Everyday surveillance is endemic to modern societies.[3]

Describing our current societies as surveillance societies implies here that surveillance is a banal, normal, routine experience in our daily lives as citizens, consumers, patients, travellers or workers.[4] Surveillance as routine sustains a key point in surveillance studies, namely the dismissal of Orwellian interpretations of surveillance as a manifestation of totalitarian authority and as the antithesis of the tenets of liberal regimes, a question to which we will return.

The preliminary definition proposed by Lyon suggests three additional points. First, surveillance is hardly a recent development but is intimately related to the formation of our modern societies. In this sense, the idea that we are currently living in "surveillance societies" can be misleading. The question would rather seem to be what it is in contemporary surveillance practices that leads some scholars to insist upon this notion. Second, surveillance is ultimately tied with how we behave in the roles outlined above. In other words, surveillance is driven by prescriptions about normal and abnormal behaviours and how these behaviours are to be steered. Surveillance, then, relates to the activity of governing, the exercise of

---

[2] Lyon, David, *The Electronic Eye: The Rise of Surveillance Society*, University of Minnesota Press, Minneapolis, 1994, and Surveillance Studies Network, *A Report on the Surveillance Society*, Information Commissioner's Office, Wilmslow, UK, 2006.

[3] Lyon, David, *Surveillance Studies: An Overview*, Polity, Cambridge, 2007, p. 15.

[4] Bellanova, Rocco, Paul De Hert and Serge Gutwirth, "Variations sur le thème de la banalisation de la surveillance", *Mouvements*, No. 62, 2010, pp. 46-54; Lyon, David, "Surveillance, power and everyday life", in R. Mansell, C. Anti Avgerou, D. Quah and R. Silverstone (eds.) *The Oxford Handbook of Information and Communication Technologies*, Oxford University Press, Oxford, 2007, and Murakami Wood, David, "Beyond the Panopticon? Foucault and Surveillance Studies", in J. W. Crampton and S. Elden (eds.), *Space, Knowledge and Power: Foucault and Geography*, Ashgate, London, 2007.

authority and the logics of rule. Third, because surveillance practices are related to the activity of governing, they establish categories of governed individuals, and enable action (coercion, but also education or incitation) upon them. As such, surveillance in so-called liberal regimes raises ethical and political issues relating to the question of liberties and their limitation. In liberal regimes, the exercise of authority is premised upon the notion that the subjects of the activity of governing "are individuals whose freedom, liberty and rights are to be respected by drawing certain limits to the legitimate scope of political and legal regulation".[5] With regard to privacy, which seeks to limit and/or prohibit the exercise of surveillance and, as a legal right in a context of "smart" surveillance, "should be conceived essentially as an *instrument* for fostering the specific yet changing *autonomic capabilities* of individuals"[6], the main question that we need to address is how we should understand the relation between surveillance and liberties. More precisely, if surveillance is considered a routine experience, if it is regarded as having historically contributed to the shaping of contemporary liberal societies and of the ways in which liberal regimes are governed, can we consider surveillance practices as opposing liberal rationalities of rule?

1.2 THE HISTORICITY OF SURVEILLANCE AND THE ACTIVITY OF GOVERNING

Addressing the above-mentioned issue requires a discussion of the intellectual background of contemporary scholarly studies of surveillance. Surveillance is sometimes framed as the expression of a totalitarian streak in European societies and as antithetic to the fundamental values of liberal regimes. In his attempt to rescue liberal societies from critiques inspired by both Karl Marx and Michel Foucault, Anthony Giddens famously argued that "the expansion of surveillance in the hands of the state can support a class-based totalitarianism of the right (fascism); but it can also produce a strongly developed totalitarianism of the left (Stalinism)".[7] Surveillance, in this view, is opposed to liberalism and can lead to various forms of totalitarianism. In another vein, some contemporary analyses of surveillance draw from Italian philosopher Giorgio Agamben's examination of the state of exception[8] to develop a similar notion: that surveillance is fuelled by a separate, illiberal rationality of rule which negates the values of liberal regimes[9]. The question of exception has become a crucial stake in recent debates on security and surveillance, to which we will return later in this section.

A different view is that surveillance both supports and is produced by liberal regimes. Historically, it has played a key role in the formation of the modern state and the search for legal-rational, impersonal forms of rule as a counterpoint to monarchic absolutism.[10] Several

[5] Rose, N., "Governing 'advanced' liberal democracies", in A. Sharma and A. Gupta (eds.), *The anthropology of the state: a reader*, Blackwell Publishing, Malden, MA, 2006, p. 150.

[6] Rouvroy, A., and Y. Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy", in S. Gutwirth, Y. Poullet, P. De Hert, C. de Terwangne and S. Nouwt (eds.), *Reinventing Data Protection*, Springer, Dordrecht, 2009, p. 46.

[7] Giddens, Anthony, *A Contemporary Critique of Historical Materialism, Vol.1: Power, property and the state*, University of California Press, Berkeley, 1981, p. 175.

[8] Agamben, Giorgio, *Homo Sacer: Sovereign Power and Bare Life*, Stanford University Press, Stanford, 1998 and Agamben, Giorgio, *State of Exception*, Zone Books, New York, 2005.

[9] Douglas, J., "Disappearing Citizenship: surveillance and the state of exception", *Surveillance & Society*, Vol. 6, No. 1, 2009, pp. 32-42; Salter, Mark B., "When the exception becomes the rule: borders, sovereignty and citizenship", *Citizenship Studies*, Vol. 12, No. 4, 2008, pp. 365-80, and Stenson, K., "Surveillance and Sovereignty", in M. Deflem (ed.), *Surveillance and Governance: Crime Control and Beyond*, Emerald Group Publishing, Bingley, 2008.

[10] Dandeker, C., *Surveillance, Power and Modernity*, Polity Press, Cambridge, 1990.

contributors highlight, for instance, how techniques of census and the establishment of "paper identities" through the delivery of identity cards and passports have contributed to establish the distinction between citizens and foreigners, thus reinforcing the authority claims of states over the former.[11] Surveillance of things (in the case of the "police of provisioning") and of people, argues Mark Neocleous, was also a fundamental component of the development of techniques of policing and of the "police state" from the 15th century onwards.[12] In a related development, surveillance practices have also been central to the shaping of industrial capitalism. Karl Polanyi, for example, has shown how the development of economic and political liberalism in the United Kingdom from the onset of the 19th century, particularly the demise of the "Speenhamland system", cannot be dissociated from the invention of the poor as a social category and of surveillance techniques targeting this category such as that of the "workhouse".[13] Building on these historical surveys, we suggest that surveillance practices are not so much the reflection of a logic of rule that opposes liberalism (authoritarianism or totalitarianism) as an expression of the "liberal government of unfreedom", whereby the resort to illiberal practices "far from being a simple matter of liberal hypocrisy, of denying its commitment to liberties… is a necessary consequence of the liberal understanding of that commitment".[14] Liberal regimes have historically and routinely limited the liberties of a variety of populations and continue to do so today, and surveillance practices have played an important role in such operations. This does not preclude, however, that the rationale, or rationalities, of such limitations have not evolved and, returning to Lyon's definition above that the purpose of surveillance has not evolved over time.

One problem in the literature is how the original analysis of surveillance spelled out by Michel Foucault in his classic volume *Discipline and Punish* ("*Surveiller et Punir*" in French, literally "*To Watch and Punish*") and introduced to surveillance studies in particular by Zuboff and Gary T. Marx, has been interpreted.[15] Giddens suggests the discussion on surveillance inspired by Foucault requires that a distinction be made between two intimately correlated dimensions of the notion: "the accumulation of 'information' – symbolic materials that can be stored by an agency or a collectivity", on the one hand, and "the supervision of the activities of subordinates by their superiors within a collectivity"[16], on the other. Foucault analyses the correlation between these two dimensions in his examination of the transformation of punishment from a spectacularly and personalised manifestation of violence in the name of the sovereign's authority to the anonymous exercise of correction upon bodies (and minds). The key figure used by Foucault is Jeremy Bentham's "Panopticon", a model internment institution made up of a tower placed in the centre of a circular building composed of identical cells. Tower and cells are pierced with windows, making it possible for a warden placed in the former "to see constantly and recognise immediately".[17] The panopticon is a

[11] Piazza, P., *Histoire de la carte nationale d'identité*, Odile Jacob, Paris, 2004; Caplan, J., and J. C. Torpey (eds.), *Documenting Individual Identity: The Development of State Practices in the Modern World*, Princeton University Press, Princeton, 2001; Torpey, J., *The Invention of the Passport: Surveillance, Citizenship and the State*, Cambridge University Press, Cambridge, 2000, and Noiriel, G., *La Tyrannie du national. Le droit d'asile en Europe (1793-1993)*, Calmann-Lévy, Paris, 1991.

[12] Neocleous, Mark, *The Fabrication of Social Order: A Critical Theory of Police Power*, Pluto Press, London, 2000.

[13] Polanyi, Karl, *The great transformation*, Octagon Books, New York, 1975 [1944].

[14] Hindess, B., "The Liberal Government of Unfreedom", *Alternatives : global, local, political*, Vol. 26, No. 2, 2001, p. 94.

[15] Zuboff, S., *In the Age of the Smart Machine: the Future of Work and Power*, Basic Books, New York, 1988 and Marx, Gary T., *Undercover: Police Surveillance in America*, University of California Press, Berkley, 1988.

[16] Giddens, op. cit., 1981, p. 169.

[17] Foucault, Michel, *Discipline and Punish: The Birth of the Prison*, Random House, New York, 1978, p. 200.

modality of visibility and more acutely of visibilisation, and it serves a specific purpose: to ensure the supervision of the inmates' behaviours in order to amend them, and eventually to foster an internalisation of this "gaze" among supervised persons and substitute "self-discipline" for external disciplinarisation. For Giddens, however, Foucault places too much emphasis on supervision, and too little on the accumulation of information; and excessively insists on the exercise of discipline within enclosed spaces (the prison, the barrack, the clinic, the factory, the school) and too little on how "[t]he everyday life of capitalism, organised via commodified time, is smoothed of those interruptions" constituted by the encounters with deviance, madness, illness or death.[18] This comment arguably misses the point of Foucault's evolving reflection on discipline. The "Panopticon" is an illustration of a process otherwise examined by Foucault in his on-going work at the time, supported by other examples such as the relation between the "city of lepers" and the "city of plague" used in *Discipline and Punish* as well as in his lectures on the "abnormals": namely, the spread of disciplinary mechanisms beyond closed institutions such as the prison, the barracks or the factory into the daily activity of governing and the correlated making of discipline into a "technology of power".[19] Discipline as a technology of power or political technology is used "to describe how knowledge is inscribed within the practical exercise of power, authority and rule" at a given moment and place.[20] Surveillance constitutes a dimension of the exercise of rule, correlated to specific modes of knowledge and specific purposes – namely, the shaping and correction of human behaviours according to established norms, an activity that Foucault labels at this stage "normalisation". What matters here is not enclosure and supervision *per se*, but how such techniques fit within a broader problematisation of human behaviour and correction.

1.3 SURVEILLANCE, PANOPTICISM AND ASSEMBLAGES

Foucault's inscription of surveillance into the political technology of discipline has been central both to the critique of Foucault by Giddens and (perhaps more acutely) by others such as Michel De Certeau, as well as to subsequent analyses of surveillance .[21] The figure of the Panopticon is at the heart of current scholarly discussions and disagreements over the understanding of contemporary surveillance practices in surveillance studies.[22] For some, the fact of living in surveillance societies today implies that one is subjected to the same disciplinary rationality, albeit updated and transformed through the use of a range of new techniques. The "Panopticon" is the yardstick that enables these scholars to examine life in surveillance societies: the "gaze" is now electronic, but the disciplinary rationality remains, limiting liberties either externally or through self-discipline in the name of the conformity to behavioural norms.[23] The Panopticon, accordingly, is either electronic for David Lyon, "super-panoptic" for Mark Poster or Zygmunt Bauman or "synoptic" for Thomas Mathiesen.[24]

---

[18] Giddens, op. cit., 1981, p. 173.

[19] Elden, S., "Plague, Panopticon, Police" *Surveillance & Society*, Vol. 1, No. 3, 2003, pp. 240-53.

[20] Dean, M., "Putting the technological into government", *History of the Human Sciences*, Vol. 9, No. 3, 1996, p. 50.

[21] De Certeau, Michel, *The Practice of Everyday Life*, University of California Press, Berkley, 1984.

[22] For an overview see Murakami Wood, op. cit., 2007.

[23] Lyon, op. cit., 1994.

[24] Bauman, Zigmunt, *Globalization: The Human Consequences*, Polity, Cambridge, 1998; Mathiesen, Thomas, "The Viewer Society: Michel Foucault's 'Panoptique' Revisited", *Theoretical Criminology*, Vol. 1, No. 2, 1997, pp. 215-34 and Poster, Mark, "Database As Discourse: Or, Electronic Interpellations", in D. Lyon and E. Zureik (eds.), *Computers, Surveillance and Privacy*, University of Minnesota Press, Minneapolis, 1996.

Others, however, warn against the risk of reification and oversimplification that follow from maintaining the Panopticon as a central figure (albeit by actualising it) in studies of surveillance. Superficially, these disagreements concern the organisation of surveillance practices and broadly speaking, their spatialisation.[25] As an analytical device, the "Panopticon" is criticised for supporting an over-centralised, over-hierarchical understanding of surveillance (the central tower looming over the cell blocks and the population of inmates), to the detriment of observations which suggest that contemporary practices of oversight espouse a more horizontal, multicentred and reticular set-up. In a classical contribution to the critique of Panopticism in surveillance studies, Kevin Haggerty and Richard Ericson hence borrow liberally from Gilles Deleuze and Felix Guattari's notion of the "assemblage", in order to, firstly, instil heterogeneity and instability in the otherwise bounded and stable understanding of surveillance provided by Panopticism and secondly, criticise the Orwellian vista that informs mainstream debates of this issue.[26] Their "surveillant assemblage" brings into question the hierarchical, institution-bound view of surveillance they see as characterising panoptic analyses. Of particular interest here is their insistence that surveillance practices operate through the "assembling" of heterogeneous components whose effects are not only cumulative, but involve something more than the sum of the assemblage's parts:

> The analysis of surveillance tends to focus on the capabilities of a number of discrete technologies or social practices. Analysts typically highlight the proliferation of such phenomena and emphasize how they cumulatively pose a threat to civil liberties. We are only beginning to appreciate that surveillance is driven by the desire to bring systems together, to combine practices and technologies and integrate them into a larger whole. It is this tendency which allows us to speak of surveillance as an assemblage, with such combinations providing for exponential increases in the degree of surveillance capacity. Rather than exemplifying Orwell's totalitarian state-centred Oceana, this assemblage operates across both state and extra-state institutions.[27]

Analysed through its logic of assembling, as an assemblage or a set of assemblages, surveillance accordingly appears as a rhizomatic system. Whereas arborescent plants grow from deep roots and, despite their apparent multiplicity, are organised by the vertical axis of a trunk ("pseudo-multiplicities", according to Deleuze and Guattari)[28], rhizomatic plants rely on a horizontal, interconnected root system with bulbs as nodal points. The rhizome is not dependent upon one specific node, since each one of them is susceptible of growing offshoots and furthering the development of the plant. Understanding surveillance as rhizomatic enables us to envisage the circulation of surveillance practices between different agencies and locations, the changing uses of specific surveillance devices and technologies, or the transfers of data between private and public organisations, for instance, without taking institutional or technical boundaries for granted. Surveillance as rhizome also points out to forms of surveillance that are not organised hierarchically. Following Mathiesen's above-mentioned notion of synopticism, Haggerty and Ericson consider the possibility of "bottom-up" forms of surveillance, whereby the many (and assumedly weak) watch the few (and assumedly powerful). However, this notion involves the fact of "watching one another" through practices

---

[25] Salter, Mark B., "Surveillance", in J. P. Burgess (ed.), *The Routledge Handbook of New Security Studies*, Routledge, London, 2010 and Salter, Mark B., "The Global Airport: Managing Space, Speed and Security", in M. Salter (ed.), *Politics at the Airport*, University of Minnesota Press, Minneapolis, 2008.

[26] Haggerty, Kevin D., and Richard V. Ericson, "The Surveillant Assemblage", *British Journal of Sociology*, Vol. 51, No. 4, 2000, pp. 605-22.

[27] Ibid., p. 610.

[28] Deleuze, Gilles, and Felix Guattari, *A Thousand Plateaus: Capitalism and Schizophrenia*, University of Minnesota Press, Minneapolis, 1987, p. 8.

of vigilantism, voluntarism or voyeurism as much as it concerns the question of resistance to surveillance.

Underpinning the debate over Panopticism and assemblages, however, is a debate of an altogether different magnitude that involves the correlation between techniques of surveillance and the political technology of discipline.[29] As David Murakami Wood suggests, there are in this regard two simultaneous debates on the issue of surveillance: one involves moving "beyond Panopticism" and the other "beyond *Discipline and Punish*".[30] Is surveillance inevitably tied with discipline and the "normalising" and authoritarian exercise of authority associated with this technology of power? Surveillance studies should be wary of "the desire to conceptualise surveillance *tout court*", writes Kevin Haggerty in this regard, and should rather "examine how specific systems of visibility are deployed in the framework of specific governmental ambitions".[31] Exploring this interrogation involves discussing the conceptual link between surveillance and security, and the distinction that Foucault introduced in his work shortly after the French publication of *Discipline and Punish* between disciplinary normalisation or "normation" and security normalisation.

1.4 SURVEILLANCE, SECURITY AND NORMALISATION

One critique of Foucault's take on surveillance, including those scholars who pay at least nominal heed to the analytical centrality of the Panopticon, is that *Discipline and Punish* has very little to say about contemporary forms of surveillance. In his seminal 1993 article on the electronic panopticon, David Lyon highlights that Foucault did not comment upon the relevance of panoptic discipline in a context where state bureaucracies, starting from the 1960s, have become increasingly reliant on computerised systems of data processing[32]; nor did he investigate how private organisations have been using surveillance in the organisation of consumption. Drawing from Zygmunt Bauman's analysis of consumerism as seduction, whereby modern societies are ordered through market dependency and the distinction between the "seduced" majority whose social and economic capitals enable them to consume, and the "repressed" minority who are unable to partake in consumption and therefore submitted to disciplinary procedures of control[33], Lyon suggests that the panoptic does not yield a complete picture of surveillance.[34] If electronic monitoring involves what Giddens called "the everyday life of capitalism", then

> those utilizing the concept have often failed to see how the Panopticon had already 'done its work', contributing to modernity's elimination of alternative powers and the creation of dependency, before being electronically enhanced. If it is correct to see consumerism as

[29] Hier, Sean P., "Probing the Surveillance Assemblage: on the dialectics of surveillance practices as processes of social control", *Surveillance & Society*, Vol. 1, No. 3, 2003, pp. 399-411 and Haggerty and Ericson, op. cit., 2000.

[30] Murakami Wood, op. cit., 2007, pp. 252-5.

[31] Haggerty, K.evin, D. "Tear down the walls: on demolishing the panopticon", in D. Lyon (ed.), *Theorizing Surveillance: The Panopticon and Beyond*, Willan Publishing, Portland, OR, 2008, p. 41.

[32] Lyon, David, "An electronic panopticon? A sociological critique of surveillance theory", *The Sociological Review*, Vol. 41, No. 4, 1993, p. 659.

[33] Lyon, David, "Liquid Surveillance: The contribution of Zygmunt Bauman to Surveillance Studies", *International political sociology*, Vol. 4, No. 4, 2010, pp. 325-38 and Bauman, Zigmunt, *Legislators and interpreters: on modernity, post-modernity and intellectuals*, Polity Press, Cambridge,1989.

[34] Lyon, op. cit., 1993, p. 671.

> creating social order, providing integration, identity and the grounds of social inclusion, then burgeoning electronic surveillance must be analysed in relation to that.[35]

This interpretation, however, does not pay enough tribute to the fact that *Discipline and Punish* constituted a specific consolidation of Foucault's work, which was still on-going at the time. While the discussion of the peculiarities of Foucault's historical work and his project of a "history of the present" fall outside of the scope of this state-of-the-art overview[36], two points are worth mentioning. To reiterate a suggestion developed above, firstly, the panopticon was hardly the only modality examined by Foucault in relation to surveillance and discipline: it operates alongside discussions on medicine epidemics and urban organisation via the cases of the "plague town" and the "leper town" as well as on the question of police. A number of contributions in surveillance studies and beyond, secondly, have emphasised the importance of Foucault's later work on security, particular of his 1977-1978 lectures on *Security, territory and population.* In these lectures, Foucault confronts his own argument (the very one criticised by Giddens) that discipline can be read as the political technology of modernity. With the study of security another understanding emerges of authority and rule in liberal regimes, articulated around the notions of *laissez faire* and *laissez circuler*, which contradicts the interpretation of political modernity as the dissemination of disciplinary mechanisms across society. Security as a technology of power operates through liberties, through statistical reasoning and calculation but also through risk analyses and profiling.[37] The first aspect would become the main line of enquiry in the lectures when Foucault leaves the discussion of security "fallow"[38] to pursue the investigation of governmentality and biopolitics. The question of risk and profiling, however, would remain underplayed. One motive commentators identify is that the analysis of the security *dispositifs* contradicts the work Foucault had just published on discipline:

> The dispositif of security is not sovereignty, or the power to punish and deliver death, but is nevertheless tied to it. It is, and it is not, about order, justice and punishment, which he has just studied. It is, and it is not, about the 'police state' and its panopticon. It is, and it is not, about discipline as it bears upon the body of the individual. It is, and it is not, about the regime of surveillance.[39]

Security, as outlined in the course's first lecture, does not relate to space and time in the same way as sovereignty and discipline. It is not about ruling a territory, or exercising authority on bodies within closed boundaries, but about controlling populations without disrupting the "natural" processes that characterises them, and in fact to prevent such disruptions. Security is related to normality, but not in the normative outlook implied by discipline. Discipline operates on the basis of pre-established norms of behaviour, towards which conducts must be directed through the detailed administration of bodies and minds: it reflects a logic of improvement that James Scott, for example, singles out as "authoritarian high modernism".[40] This logic is singled out as "normalisation" by Foucault in *Discipline and Punish*, but he

---

[35] Lyon, op. cit., 1993, p. 675.

[36] But see Dean, M., *Critical and effective histories: Foucault's methods and historical sociology*, Routledge, London, 1994, and Veyne, P., *Comment on écrit l'histoire*, Seuil, Paris, 1978.

[37] Elden, S., "Governmentaliy, calculation, territory", *Environment and Planning D: Society and Space*, Vol. 25, No. 4, 2007, pp. 562-80.

[38] Bigo, Didier, "Security: A Field Left Fallow", in M. Dillon and A. W. Neal (eds.), *Foucault on Politics, Security and War*, Palgrave Macmillan, Houndmills, Basingstoke, 2008.

[39] Bigo, op. cit., 2008, p. 96.

[40] Scott, James, *Seeing Like a State: How Certain Schemes to Improve the Human Condition Have Failed*, New Haven, Yale University Press, 1998.

returns to the idea in *Security, territory and population* and distinguishes between disciplinary normalisation, that he renames "normation", and security normalisation that retains the label. Normalisation is a fundamental notion for an understanding of the contemporary politics of surveillance, their relation to security and freedom. It is through normalisation that one can understand how liberal regimes deploy practices of surveillance as a routine operation in the activity of governing, and not as some kind of exceptional politics. Where sovereignty seeks to rule through decrees on what is forbidden and what is authorised, where discipline seeks to improve through the detailed administration and disposition of things and persons, security as a technology of power seeks to optimise both the processes considered natural among a given population and the exercise of governing, which is expected to get as little as possible in the way of these natural processes. In other words, security as a technology of power does not negate or cancel out freedom, but operates through it. This does not entail, of course, that the operations involved in the technologies of sovereignty and discipline have disappeared. In his 1977-1978 lectures, Foucault establishes clearly that sovereignty, discipline and security work in a triangle: the tip of this triangle might shift, but as security becomes the predominant rationality of rule, sovereignty and discipline remain, albeit in a more discrete fashion.

These insights have informed a number of contributions in the field of security studies[41], including on EU affairs in the field of border control and migration[42]. It has also been taken on board by students of "governmentality". Valverde and Mopas, following the work of criminologist David Garland, have documented the correlation between the rise of the "new penology" and the "dream of targeted governance", i.e. the growing reliance on risk management techniques and risk profiles to govern populations considered deviant in a way that is premised to limit both the overall intervention of criminal justice institutions in the society, and the scope of that intervention.[43] In the field of surveillance, this trend has been espoused by some scholars in the wake of "post-panoptic" arguments and has seen a shift in the intellectual sources of the field - broadly speaking, from Foucault's *Discipline and Punish* to Deleuze's *Societies of Control*.[44] It has been further nurtured by the increasing centrality in practices of surveillance of the processing of electronic data, as will be discussed in the following pages.

---

[41] Balzacq, T., T. Basaran, D. Bigo, E-P. Guittet and C. Olsson, "Security Practices", in R. A. Denemark (ed.), *The International Studies Encyclopedia*, Blackwell Reference Online, Blackwell Publishing, 2010; Basaran, T., *Security, Law and Borders: At the Limits of Liberties*, Routledge, London, 2010; Bigo, Didier, "Exception et ban: à propos de l'"Etat d'exception"", *Erytheis*, No. 2, 2007, pp. 115-45; Bigo, Didier, "Pro-activity, profiling and prevention", Paris, Unpublished manuscript, 2007; Bigo, Didier, "Protection: security, territory and population", in J. Huysmans, A. Dobson and R. Prokhovnik (eds.), *The Politics of Protection: Sites of insecurity and political agency*, Routledge, London, 2006 and Huysmans, J., *The politics of insecurity: fear, migration and asylum in the EU*, Routledge, London, 2006.

[42] Jeandesboz, Julien, "Beyond the Tartar Steppe: EUROSUR and the ethics of European border control practices", in J. P. Burgess and S. Gutwirth (eds.), *Europe under threat? Security, migration and integration*, Brussels, VUB Press, 2011; Bigo, D., J. Jeandesboz, F. Ragazzi and P. Bonditti, "Borders and security: the different logics of surveillance in Europe", in S. Bonjour, A. Rea, and D. Jacobs, D. (eds.), *The Others in Europe*, Presses de l'Université de Bruxelles, Brussels, 2010; Neal, A.W., "Securitization and Risk at the EU Border: The Origins of FRONTEX", *Journal of Common Market Studies*, Vol. 47, No. 2, 2009, pp. 333-56; Huysmans, op. cit., 2006 and Bigo, Didier, "Security and Immigration: Toward a Critique of the Governmentality of Unease", *Alternatives : global, local, political*, Vol. 27, Special Issue, 2002, pp. 63-92.

[43] Valverde, M., and M. Mopas, "Insecurity and the dream of targeted governance", in W. Larner and W. Walters (eds.), *Global Governmentality: Governing international spaces*, Routledge, London, 2004 and Garland, D., *The culture of control: crime and social order in contemporary society*, Chicago University Press, Chicago, 2002.

[44] Deleuze, Gilles, "Postscript on the Societies of Control", *October*, Vol. 59, 1992, pp. 3-7.

1.5 DATAVEILLANCE, PREDICTION AND PROFILING

Having established that surveillance is intrinsic to the practices of liberal regimes as well as an evolving activity of governing associated with different rationalities of rule, the question we address here is of the specificity of contemporary surveillance practices. A driving argument in the literature is that this specificity is tied to the growing reliance on the processing of electronic data.[45] Gary T. Marx has consistently argued that electronic technologies supported the advent of a "new surveillance", a process that Oscar Gandy, David Lyon or Mark Poster tied in more specifically with the processing of personal information for purposes of social sorting.[46] Contemporary practices of surveillance are thus better understood as "dataveillance", a term coined in 1988 by Roger Clarke and defined as "the systematic use of personal data systems in the investigation and monitoring of the actions or communications of one or more persons".[47]

While practices of dataveillance have become the focus of a number of studies dealing with the activities of security agencies and bodies, for example in the context of counter-terrorism policies[48], they are not limited to security purposes, nor are they the sole remit of public authorities. Dataveillance is a routine commercial practice for companies that process the information knowingly or unknowingly submitted by their customers, for instance to devise so-called targeted advertisements. Such practices have supported the development of entire business models, for example search engines such as Google, and provide additional income to online vendors such as Amazon with its recommendation lists. The divide between data processing by private and public agents, in the meantime, is not clearly delineated. The multiple developments of the SWIFT/TFTP case in the EU, for instance, highlight how public agencies and bodies tap into the personal data held by private organisations (in this case the SWIFT company) for security purposes.[49]

Specific instances of dataveillance, however, share a number of common points. As mentioned earlier, commercial practices of dataveillance seek to determine customer preferences based on the analysis of patterns of consumption in order to predict future behaviours and develop more targeted advertisement activities through the extraction of data from large sets of information (so-called data-mining). Pattern recognition and prediction are equally present in data processing schemes set up for policing purposes, and increasingly so since the significant hardening of security policies experienced in North American and European countries following the events of 11 September 2001.[50] It has further become a characteristic of the criminal justice system in a number of these countries, particularly in the United States and the United Kingdom, through the promotion of notions such as

[45] Lyon, op. cit., 1994.

[46] Poster, op. cit., 1996; Lyon, op. cit., 1994 and Gandy, Oscar H., *The panoptic sort: a political economy of personal information*, Westview Press, Boulder, CO, 1993.

[47] Clarke, Roger, "Information Technology and Dataveillance", *Communications of the ACM*, Vol. 31, No. 5, 1988, pp. 498-512.

[48] Bigo, D., and A. Tsoukala (eds.), *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*, Routledge, London, 2008, and Amoore, L., and M. De Goede (eds.), *Risk and the War on Terror*, Routledge, London, 2008.

[49] Amicelle, A., "The Great (Data) Bank Robbery: Terrorist Finance Tracking Program and the 'SWIFT Affair'", *CERI Research Questions*, No. 36, 2011 and De Goede, M. (forthcoming in 2011), "The SWIFT Affair and the Constitution of the European Security Community", *Journal of Common Market Studies*, 2011.

[50] Amoore, L. and M. De Goede (eds.), *Risk and the War on Terror*, London, Routledge, 2008 and Gandy Jr, Oscar, "Data Mining, Surveillance and Discrimination in the Post 9/11 Environment", in K. Haggerty and R. Ericson (eds.), *The New Politics of Surveillance and Visibility*, University of Toronto Press, Toronto, 2006.

"intelligence-led policing".[51] The emphasis on "pro-active" or "pre-emptive" policing is a core component of internal security activities supported in the European governmental arenas, as exemplified by recent strategic documents such as the Stockholm programme for the European area of freedom, security and justice[52], the European Internal Security Strategy[53] or the European Information Management Strategy for internal security[54]. Access to personal data and to data processing schemes, accordingly, has become a tug of war for EU security agencies in their dealings with national authorities as well as with the European Commission and Parliament[55] and of the INEX project, in particular[56]. Pattern recognition, more commonly referred to as profiling, has also emerged as a key component of these activities, albeit one that is never explicitly embraced in the EU context.

We will come back to the specific "assembling" of smart surveillance in the European governmental arenas in the fourth section of the deliverable, but it is important to emphasise further the analytical relevance of profiling. Profiling is arguably one of the most significant ways in which dataveillance departs from earlier practices of surveillance. "Computers, Gary Marx argued already at the end of the 1980s, qualitatively alter the nature of surveillance - routinizing, broadening, and deepening it. Rather than focusing on an isolated individual at one point in time and on static demographic data, such as date of birth, surveillance increasingly involves complex transactional analysis, interrelating persons and events".[57] Profiling should be understood in relation to two other notions, pro-activity and prevention.[58] Pro-activity involves following traces, particularly electronic ones, left by persons and/or groups that are targeted by surveillance, and prevention is the ultimate goal, whereby "the idea is not to recover from an event or to respond to it, or even to be protected from it by previous measures, but to assess a future threat and to prevent the event from happening".[59] Profiling is the set of techniques through which data is assembled in a pre-determined analytical setting. Profiling, of course, is a variegated practice[60], but it becomes particularly problematic when it is expected to act upon the future, and support actions against specific persons or groups in the name of the behaviour they are expected to have.

---

[51] Harcourt, B., *Against prediction: Profiling, policing, and punishing in an actuarial age*", University of Chicago Press, Chicago, 2007, and Valverde, M., and M. Mopas, "Insecurity and the dream of targeted governance", in W. Larner and W. Walters (eds.), *Global Governmentality: Governing international spaces*, Routledge, London, 2004.

[52] Council of the European Union, *The Stockholm Programme - An open and secure Europe serving and protecting citizens*, Brussels, 5731/10, 2010.

[53] Council of the European Union, *Draft Internal Security Strategy for the European Union: Towards a European Security Model*, Brussels, 5842/2/10, 2010.

[54] Council of the European Union, *Draft Council Conclusions on an Information Management Strategy for EU internal security*, Brussels, 16637/09, 2009.

[55] See the results of the CHALLENGE project, in particular, Bigo, Didier, "Security: A Field Left Fallow", in M. Dillon and A.W. Neal (eds.), *Foucault on Politics, Security and War*, Palgrave Macmillan, Houndmills, Basingstoke, 2008, and Bigo, D. and A. Tsoukala (eds.), *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*, Routledge, London, 2008.

[56] Bigo, D., P. Bonditti, J. Jeandesboz and F. Ragazzi, *Security technologies and society: A state of the art on security, technology, borders and mobility*, PRIO INEX Deliverable D.1.1, Oslo, 2008.

[57] Marx, op. cit., 1988, p. 208.

[58] Bigo, et al., op. cit., 2008, pp. 24-5 and Bigo, op. cit., "Pro-activity, profiling and prevention", 2007.

[59] Bigo, op. cit., "Pro-activity, profiling and prevention", 2007, p. 11.

[60] Gonzalez Fuster, G., S. Gutwirth and E. Ellyne, *Profiling in the European Union: A high-risk practice*, Brussels: CEPS, 2010 and Hildebrandt, Mireille, and Serge Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer, Dordrecht, 2008.

1.6 LATERAL SURVEILLANCE: VIGILANTISM, VOLUNTARISM, VOYEURISM AND COUNTER-SURVEILLANCE

Following the previous discussion of the correlation between surveillance, security and normalisation, it is important to emphasise that contemporary surveillance practices do not rely exclusively on coercive, hierarchical modalities for obtaining and processing personal data. Surveillance, it has been argued, can operate "laterally".[61] In the case of policing, persuasion, calls for inclusiveness, emphasis on the individual's responsibility as a member of a community are modalities for enrolling individuals in their own surveillance or in the surveillance of others.[62] In order to investigate the riots following the defeat of the Vancouver Canucks in the Stanley Cup final on 15 June 2011, for instance, the Vancouver police not only used the information provided by social media such as Twitter or Facebook to identify and arrest suspects, but also called upon users of social networks to turn in any information they might have come across that might provide leads on persons involved in violence. The same practices are currently enacted in the Metropolitan Police's on-going investigation of the events that have taken place in London's inner cities in August 2011: the "trawling" of online data, including of social media, is combined with calls to participation from the public, for example, to identify persons suspected of involvement in cases of looting out of CCTV footage. Intelligence services are putting increasing emphasis on mining "open source intelligence", that is, information made available on the Internet through blogs, social media and press sources, to predict future trends. The possibilities of such an approach, illustrated by the 2009 Google Flu Trends project, will be explored by the U.S. intelligence research agency DARPA through its newly established Open Source Indicator Program.

Lateral surveillance has different facets. In the above-mentioned examples, it relates to the promotion of forms of vigilantism and to reliance on voluntarily provided information (voluntarism). A number of scholarly contributions in surveillance and media studies have insisted, in this regard, on the role played by representations of surveillance in popular culture (through advertisement, books, movies and various other artistic performances) in generating familiarity and even fascination with surveillance, and ultimately enhancing the reach of surveillance practices.[63] They build on Bauman's argument of the displacement of the panoptic logic of surveillance by the logic of seduction of the market, and on Thomas Mathiesen's notion of the "viewer society", which enables him to revise some of the insights proposed by Foucault on surveillance in disciplinary societies.[64] Foucault demonstrates how the economy of punishment has shifted from a spectacular and theatrical logic whereby the many watch the few (being punished). Mathiesen argues that today's mass media are contributing to the shaping of a synoptic logic that both turns surveillance into a daily and generalised activity and familiarises us with its exercise.[65] A typical example of this process

[61] Andrejevic, Mark, "The Work of Watching One Another: Lateral Surveillance, Risk and Governance", *Surveillance & Society*, Vol. 2, No. 4, 2005, pp. 479-97.

[62] Marx, Gary T., "Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information – 'Hey Buddy Can You Spare a DNA?'", in Torin Monahan (ed.), *Surveillance and Security: Technological Politics and Power in Everyday Life*, Routledge, London, 2006.

[63] For an overview, see Lyon, David, *Surveillance Studies: An Overview*, Polity, Cambridge, 2007, pp. 139-58.

[64] For an illustration on what he terms "post-panopticism", see Boyne, R., "Post-Panopticism", *Economy and Society*, Vol. 29, No. 2, 2000, pp. 285-307.

[65] Mathiesen, op. cit., 1997.

which has been commented at length in the literature, is so-called reality TV and particularly the "Big Brother" show and its various spin-offs.[66]

Familiarity with surveillance also follows from the growing availability of some technologies to the general public. One of the best documented cases[67], here, concerns the use of private webcams and the fact that such devices enable persons to make themselves visible voluntarily, in some cases to a very large group of persons.[68] Personal webcams and the practices of voyeurism and exhibitionism that they support, argues Hille Koskela, draw attention to what she terms "the other side of surveillance". Surveillance can be "experienced as pleasurable"[69], but organising one's own visibility can also be a way to exercise control over one's image and representation in the context of Mathiesen's viewer society. The point can be extended to a number of other devices beyond webcams in a context of so-called ambient intelligence and pervasive computing systems. The use of telephone handsets with inbuilt GPS receivers, cameras and Internet access (so-called "smart phones") has, for example, encouraged the use of geolocalisation services, enabling users to "check in" specific locations, notify their relatives of their presence in a given area, indicate a spot of interest or search for acquaintances in their physical vicinity.[70]

The discussion of vigilantism, voluntarism and voyeurism in surveillance practices draws our attention to the key debates in surveillance studies on the relation between surveillance and freedom, particularly with regard the issue of domination and agency. By pointing out that surveillance does not have to involve the forcible extraction of information from reticent subjects for purposes of overseeing, some surveillance studies hint at the multiple forms of agency that operate within contemporary surveillance societies. As summarised by David Lyon, "[t]he persons surveilled are not merely subject to surveillance but subjects of surveillance".[71] While surveillance has traditionally been equated with domination[72], recent directions adopted in the study of this matter also point out to the fact that in certain contexts, surveillance can be regarded as desirable (e.g., in the medical field), or can foster practices of appropriation and empowerment, as well as "counter-conducts" or practices of resistance.

1.7 SURVEILLANCE AND RESISTANCE

There are two sides to contemporary examinations of counter-conducts and resistance towards surveillance in a context where growing emphasis is placed on the electronic processing of

[66] Andrejevic, Mark, *Reality TV: The Work of Being Watched*, Rowman & Littlefield, Lanham, MD, 2004; McGrath, John E., *Loving Big Brother: Performance, Privacy and Surveillance Space*, Routledge, London, 2004, and Pecora, V., "The culture of surveillance", *Qualitative Sociology*, Vol. 25, No. 3, 2002, pp. 345-58.

[67] Whose attractiveness to surveillance scholars undeniably lies in the fact that it involves one of the most notorious symbols of surveillance in popular culture, the video camera.

[68] Bell, D., "Surveillance is Sexy", *Surveillance & Society*, Vol. 6, No. 3, 2009, pp. 203-12; Koskela, Hille, "Webcams, TV Shows and Mobile Phones: Empowering Exhibitionism", *Surveillance & Society*, Vol. 2, No. 2/3, 2004, pp. 199-215 and Tabor, P., "I Am a Videocam", in I. Borden, J. Kerr and J. Rendell (eds.), *The Unknown City: Contesting Architecture and Social Space*, MIT Press, Cambridge, MA, 2001.

[69] Koskela, Hille, "'The other side of surveillance': webcams, power and agency", in David Lyon (ed.), *Theorizing Surveillance: The Panopticon and Beyond*, Willan Publishing, Portland, OR, 2008, p. 173.

[70] Goggin, G., *Cell Phone Culture: Mobile Technology in Everyday Life*, Routledge, London, 2006, and Koskela, op. cit., 2004.

[71] Lyon, op. cit., *Surveillance Studies: An Overview,* 2007, p. 159.

[72] Gilliom, John, *Overseers of the Poor: Surveillance, Resistance and the Limits of Privacy*, University of Chicago Press, Chicago, 2001.

personal data. A number of contributions, firstly, highlight that "the potential of a technology for harm needs to be kept distinct from its realization.… Control systems are not usually as effective and efficient as their advocates claim and they often have a variety of unintended consequences".[73] One needs to distinguish, in other words, between the "programmatic" logic of surveillance (what it is expected or supposed to do) and the practices through which it is effectuated. A growing body of work[74] has addressed what Murakami Wood terms the "technological fetishism"[75] of some students of surveillance. Kirstie Ball, for instance, mobilises so-called Actor Network Theory approaches (ANT, see below 4.1.1.) to support her claim that "we should analyse surveillance in a socio-technical manner, privileging neither the technology nor its social 'effects' in analysis"[76], but that technology in its biases and dysfunctions should be included equally in examinations of surveillance.

Secondly, surveillance is constantly challenged through a wide array of practices, operating at different levels of scale. Such challenges range from more collective processes involving struggles over fundamental freedoms and rights, to personal tactics mobilised in everyday life. Concerning the latter, Gary T. Marx identifies 11 everyday ways of engaging with surveillance practices, ranging from "discovery moves" (which involve finding out whether surveillance is in operation or not) to explicit counter-surveillance moves (currently made easier by the growing accessibility of counter-measure equipment for private citizens), and including distorting (manipulation of the data collection process), blocking (physically preventing the collection) or masking (providing misleading information) moves.[77] Such tactics thus do not always involve a frontal confrontation with surveillance practices, nor can they be considered as the sole resort of "victims" of surveillance.

As far as collective processes are concerned, struggles over privacy and data protection have been, in view of the increasing use of electronic devices and computer systems, a long-standing concern of surveillance scholars.[78] As a recent debate organised by the journal *Surveillance & Society* (Issue 4 of 2011) on the question demonstrates, there is a degree of disagreement over the adequacy of the notion. On the one hand, concerns with data protection and privacy are seen as too narrow, too closely associated with liberal discourses on a rights-based approach to freedom. Privacy and data protection are challenged as a possible "antidote to privacy", as they are often seen as enabling, rather than preventing or blocking surveillance.[79] Privacy is also regarded as too excessively centred on the individual and its right to self-determination (the "right to be let alone", in particular) at the expense of

[73] Marx, Gary, T., "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance", *Journal of Social Issues*, Vol. 59, No. 2, 2003, p 371.

[74] Murakami Wood, D., and S. Graham, "Permeable Boundaries in the Software-Sorted Society: Surveillance and the Differentiation of Mobility", in M. Sheller and J. Urry (eds.), *Mobile Technologies of the City*, Routledge, London, 2006; Donaldson, A., and D. Murakami Wood, "Surveilling Strange Materialities: The Evolving Geographies of FMD Biosecurity in the UK", *Environment and Planning D: Society and Space*, Vol. 22, No. 3, 2004, pp. 373-91. Ball, Kirsty, "Elements of surveillance: A new framework and future directions", *Information, Communication & Society*, Vol. 5, No. 4, 2002, pp. 573-90.

[75] Murakami Wood, op. cit., 2007, p. 256.

[76] Ball, op. cit., 2002, p. 586.

[77] Marx, op. cit., 2003, p. 374-84.

[78] See Bennett, Colin J., *The Privacy Advocates: Resisting the Spread of Surveillance*, MIT Press, Cambridge, MA, 2008, and Bennett, Colin J. and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge, MA, 2006.

[79] Stalder, F., "Opinion: Privacy is not the antidote to surveillance", *Surveillance & Society*, Vol. 1, No. 1, 2002, pp. 120-124.

considerations of the broader social effects of surveillance practices.[80] On the other hand, privacy is a useful conceptual and practical umbrella that contributes to keeping surveillance studies relevant to contemporary policy developments. Bennett maintains in his contribution to the debate organised by *Surveillance & Society* that none of the above-mentioned criticisms provides a comprehensive case against privacy as a central notion in surveillance studies. Privacy, in his view, is a useful descriptor of a number of actors, regimes of practices and policy tools involved in challenging surveillance. While practices such as the enforcement of fair information principles are limited when it comes to curtailing surveillance, in other words, "skepticism about privacy tends to promote a certain passivity and reluctance to engage in the messy debates over the rules, and the implementation and enforcement of those rules".[81] Voicing the opposite perspective, John Gilliom objects to Bennett that the point is not to challenge the validity of privacy and the concerns that it expresses, but rather to question its standing as the "organizing matrix of the field" of surveillance studies.[82] Weakening the intellectual monopoly of privacy, he argues, would nonetheless enable students of surveillance to take stock of the complexity of current surveillance practices, of the limited successes that the "privacy advocates" analysed by Bennett in his most recent volume have encountered, and ultimately avoid the biases which would result from a dialectical interpretation of the relation between surveillance and privacy.

This discussion leads to the key analytical move that is shared by most current reflections on resistance to surveillance: the rejection of a normative perspective that would pit "bad" surveillance against "good" resistance. This owes in part to the Foucauldian inspiration underpinning the majority of contributions to surveillance studies. Foucault, in no small part due to his intellectual relationship to Marxism, refused the view that domination and resistance were two opposing forces or essences: he saw them as intertwined processes that could not exist without one another, and whose relations generated effects of power (rather than power being the explanatory variable of domination and resistance). This understanding of resistance informs the most recent developments in the study of surveillance. Some scholars, for instance, have sought to develop further and more fully the notion of surveillant assemblages initially proposed by Ericson and Haggerty. This is the purpose, for example, of what William Bogard evocatively terms, following Deleuze and Guattari, "lines of flight". The notion, he argues, offers the possibility to encompass the transformation of surveillance practices under the joint influence of practices of resistance and of attempts at re-asserting control: "Flight refers to how assemblages change as an effect of their own organisation […] In a crucial sense, assemblages as a whole are lines of flight. Older organisations of punishment, such as torture or the spectacle, deterritorialize on the panopticon. The panopticon is a line of flight or resistance in relation to these organized forms […] What we have called rhizomatic surveillance is a convergence of resistance lines that develop immanently within panoptic assemblages (specifically resistant to limits on the recording imposed by space and time, the need for centralized, hierarchical control, etc.)".[83] Such proposals highlight the importance of approaching surveillance as a heterogeneous set of

[80] Bennett, Colin J., "In Defence of Privacy: The concept and the regime", *Surveillance & Society*, Vol. 8, No. 4, 2011, pp. 485-96; Regan, Priscilla, "Response to Bennett: Also in Defence of Privacy", *Surveillance & Society*, Vol. 8, No. 4, 2011, pp. 497-9; Lyon, David, *Surveillance Society: Monitoring Everyday Life*, Open University Press, Buckingham, 200,1 and Regan, Priscilla, *Legislating Privacy: Technology, Social Values and Public Policy*, University of North Carolina, Chapel Hill, 1995.

[81] Bennett, op. cit., 2011, p. 494.

[82] Gilliom, John, "A response to Bennett's 'In defence of privacy'", *Surveillance & Society*, Vol. 8, No. 4, 2011, p. 500.

[83] Bogard, W., "Surveillance assemblages and lines of flight", in D. Lyon (ed.), *Theorizing Surveillance: The Panopticon and Beyond*, Willan Publishing, Portland, OR, 2008, pp. 107-108.

practices, involving various sets of actors (including, in the case of ANT-informed approaches, non-human actors), diverging tactics and struggles over the extent and limits of their exercise.

1.8 CONCLUSIONS

This state-of-the-art review offers five key insights for the study of smart surveillance and the reflection on how an innovative privacy impact assessment methodology can be devised.

First, surveillance has to do with the activity of governing. Far from the popular, Orwellian representation of surveillance as an authoritarian and anti-liberal practice or as a romanticised cape-and-dagger activity, it is a routine and long-standing practice for public administration, law-enforcement and security bodies as well as for the private sector. The notion that we live in "surveillance societies" might be an oversimplification, but it does convey the view that there is nothing exceptional to surveillance, and that in any case, it is by no means alien to liberal regimes.

The second, arguably more central point concerns the relation between surveillance and freedom. What current discussions among students of surveillance reflect is that it is no longer correlated solely to a disciplinary logic that entails a vertical exercise of authority. Surveillance practices currently stand in relation to a logic of normalisation: they operate through freedom, rather than in negation of it. A key implication of this insight in the current EU context is that the image of a "balance" between security/surveillance and freedom cannot be considered an adequate representation of the policy challenges involved in devising privacy-oriented methodologies.

Third, the main area of concern regarding contemporary surveillance trends is the generalisation of dataveillance. However, the use of electronic data should not be regarded just as an enhancement of previous surveillance practices. Dataveillance operates in relation with pro-activity and profiling, with the ultimate goal, particularly in security policies, of prevention. It is this trend towards prediction and its corollaries, including the increasing reliance on data-mining and the processing of "bulk" data, which should be placed at the forefront of discussions on privacy.

Fourth, it is important to take on board the notion that surveillance is not a homogenous process. The politics of surveillance involve various forms of resistance, combining collective and individual attitudes. In some cases furthermore, surveillance will be considered as desirable, or will call upon the active participation of individuals. Surveillance is thus dynamic and evolves through struggles and controversies. This is an important issue with regard to the discussion on privacy and data protection. Privacy and data protection should not be considered ramparts against surveillance. In some cases, they authorise surveillance by limiting its scope to proportions considered more acceptable. The point is not to deny the significance of privacy and data protection, but to emphasise that they operate in relation to other rights that might be challenged by surveillance, and in broader social configurations that are dynamic and changing.

Finally, the analysis of "smart surveillance" and the correlated devising of a PIA methodology, which constitutes the objective of SAPIENT, should embed the more technical aspects of this discussion with an overall analysis of the legal and political struggles unravelling around the issue of surveillance. This supports the layout of the present

deliverable, and the combination of more technology-focused section (as in the following chapter) and legal, sociological and public opinion analyses (chapters 3,4 and 5).

2 EMERGING SMART SURVEILLANCE TECHNOLOGIES

Vlad Coroama, Marc Langheinrich (USI); Rachel Finn, David Wright, Kush Wadhwa (Trilateral); Silvia Venier, Emilio Mordini (CCSC)

2.1 INTRODUCTION

This chapter examines today's surveillance society through the lens of current and emerging technologies. It uses a review and analysis of academic articles, policy documents and reports, press stories and research projects to identify the different kinds of surveillance technologies prevalent in our society today and those that are emerging in the near future. In particular, we address surveillance technologies with security relevance ("the critical parts"). We begin in section 2.2 by describing surveillance technology families (visual surveillance, biometrics, sensors, etc.) and individual technologies within those families, (i.e., CCTV, iris recognition, etc.). For each technology, we examine how it works, the applications associated with it, where and how has it been implemented, the users of the technology and finally who the surveilled are in relation to the technology. We particularly review security projects in the field of border/immigration control, security for public spaces and critical infrastructures. Section 2.3 begins by setting out a taxonomy of surveillance technologies by their different functions, in which we examine factors such as intrusiveness, comfort and speed. Section 2.4 then identifies the stakeholders and drivers associated with the implementation of surveillance systems. In section 2.5, we explore current technologies as surveillance assemblages or systems, and describe how they are used to fulfil specific purposes such as border control or airport security. Section 2.6 looks forward by analysing major European and U.S. research initiatives and programmes, in order to discuss the extent to which emergent technologies will be organised into "smart" assemblages (section 2.7).

2.2 TECHNOLOGIES AND APPLICATIONS

The technology-focused section of this deliverable begins with a taxonomy of surveillance technologies. In order to fully understand the implications of surveillance systems, we offer a brief examination of how each of these technologies work, the applications associated with the technologies, where and how they have been implemented and who the surveyors and surveilled are in relation to each technology. This specific information will assist in the analysis of the legal and sociological impacts of surveillance technologies in later chapters of the report. This taxonomy divides surveillance technologies into the following technology families: visual surveillance, dataveillance, biometrics, communication surveillance, sensors and location determination technologies, and discusses individual technologies within each.

2.2.1 Visual surveillance

We group existing visual surveillance technologies into five areas: photography, CCTV, UAVs, imaging scanners, and satellites.

Photography (cameras, mobile phones, mobile video)

The original form of visual surveillance was the portable camera, where images of individuals could be taken that would place them in particular spaces. Today, in addition to portable still cameras, mobile phone cameras and mobile video devices such as mobile phones with video capabilities offer a portable way to collect and record images of individuals, sometimes with information that places them in particular places and particular times. Photographic images can be used to identify unknown individuals if their image has been stored on a database or in other files. In addition to photographs of people, images may also be of cars or other objects. For example, photographic technology can be linked with sensors that detect speed or the encroachment into particular places at particular times, and/or to issue fines to the owners of particular vehicles. Although state or other authorities use this equipment to target the less powerful, these systems may be more democratic than other surveillance systems. Relatively non-powerful individuals can use this equipment to capture images of powerful individuals such as police, celebrities and/or state officials in a synoptic surveillance framework.[84]

Some applications of this technology include the surveillance of suspected or known criminals, passport holders and car drivers by the police, the surveillance of the powerful by non-authoritative individuals (such as filming incidents of alleged police brutality), surveillance of celebrities or other famous individuals for entertainment, or peer surveillance such as individuals taking photos of one another. These systems have been implemented both in public and private space. For example, in the UK a judge ruled that the photographing and subsequent storage of images of a protester was unlawful and breached the protester's human rights.[85] Photographic surveillance is also used for identification purposes by the state including, but not limited to mug shots, passports, driving licenses and other identity documents. Police or other authorities may also use this surveillance to monitor traffic offences such as speed cameras, red light cameras, bus lane cameras, etc. Finally, this surveillance system may be used for less conventional forms of surveillance such as photographing celebrities or "happy slapping" by young people.

CCTV

Closed circuit television, or CCTV as it is commonly called, generally refers to "all semi permanently installed video equipment...[and includes cameras that are] primarily used to monitor places or behaviour" usually by the police or other state or public authorities.[86] Such surveillance, according to Webster is "considered ubiquitous, a normal part of everyday life, with citizens willingly acquiescing as surveillance subjects, and perfectly happy to forgo some personal privacy in return for greater levels of personal safety and security."[87] However, in our definition we also include other types of cameras, such as web-cameras, and other types of authoritative viewing such as store owners, private security, home owners, school authorities and private property owners. Cameras may be actively monitored in "real time", where those monitoring the cameras can provide a response to incidents, they may be passively monitored, in that they may only record data which can be later referred to if an incident occurs, or they may be non-active, such as dummy cameras which are meant to act as

[84] Mathiesen, op. cit., 1997.

[85] Taylor, Matthew, and Paul Lewis, "Surveillance of Protesters Ruled Illegal", *The Guardian*, 21 May 2009. http://www.guardian.co.uk/uk/2009/may/21/police-surveillance-ruling-andrew-wood

[86] Nouwt, Sjaak, Berend R. de Vries and Dorus van der Burgt, "Camera Surveillance and Privacy in the Netherlands", *Social Studies Research Network*, 2005, p. 2. http://ssrn.com/abstract=849205

[87] Webster, C.W.R., "CCTV policy in the UK: reconsidering the evidence base", *Surveillance & Society*, Vol. 6, No. 1, 2009, pp. 11-12. http://www.surveillance-and-society.org

a visual deterrent.[88] Some actively monitored systems may also record and store data for later reference. Cameras can also be fitted with microphones or loud speakers to enable those monitoring the cameras to listen, or speak to those who are being observed. CCTV systems which are operated by police or other authorities generally must provide notice to the shoppers or other individuals who are being surveilled that cameras are in operation, although some systems in some locations may be covert. Cameras are often used within the criminal justice system to prevent and detect crime, but they may also contribute to citizens feeling safer and more secure in public or semi-public space.

Some examples of applications of CCTV systems include, but are not limited to, the protection of private property, national security, counter-terrorism, road traffic monitoring (associated with automatic number plate recognition), identification of individuals, monitoring for criminal or anti-social behaviour, behaviour or pattern recognition, border control and employee monitoring. Examples of places in which camera systems have been deployed are public spaces such as streets and town centres, motorways, casinos, housing association houses/estates, workplaces (including the home as a workplace as in "nanny cams"), shopping malls, convenience stores, banks, transport systems, airports and schools. CCTV cameras have also been fitted to drones, helicopters and cars/vans. Cameras are more popular in some states than others, for example, the US is only beginning to invest heavily in CCTV surveillance of public space, whereas there are already an estimated 4.2 million cameras in the UK[89].

UAVs (drones)

Unmanned aerial vehicles (UAVs) or unmanned aircraft systems (UASs) can generally be defined as a "device used or intended to be used for flight in the air that has no onboard pilot"[90] that include "multiple pieces of ancillary equipment, such as vehicle control equipment, communications systems, and potentially even launch and recovery platforms"[91]. These devices are sometimes referred to as drones, which are programmed for autonomous flight and remotely piloted vehicles which are flown remotely by a ground controlled operator.[92] Current generations of UASs "can be as small as an insect or as large as a charter flight".[93] They can be launched from a road or a small vehicle, but are often large enough to accommodate cameras, sensors or other information gathering equipment.[94] UASs have a range of capabilities making them useful not only for military applications, but also the bourgeoning field of civil applications. Specifically, UASs have a "niche" in performing the three Ds: dull, dirty and dangerous work, thereby protecting human pilots from fatigue and

[88] Biale, Noam, "Expert Findings on Surveillance Cameras: What Criminologists and Others Studying Cameras Have Found", ACLU White Paper, 25 June 2008. http://www.aclu.org/images/asset_upload_file708_35775.pdf and Webster, op. cit., 2009.

[89] Biale, op. cit., 2008

[90] Quoted from Aviation Safety Unmanned Aircraft Programme Office, 2008, in McBride, Paul, "Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations", *Journal of Air Law and Commerce*, Vol. 74, 2009, p. 628.

[91] McBride, op. cit., 2009, p. 629. See also Directorate of Airspace Policy, *CAP 722: Unmanned Aircraft System Operations in UK Airspace – Guidance*, Civil Aviation Authority, 6 Apr 2010.

[92] Bolkcom, Christopher, *Homeland Security: Unmanned Aerial Vehicles and Border Surveillance*, Congressional Research Service Report for Congress, 28 June 2004.

[93] Eick, Volker, *The Droning of the Drones: The increasingly advanced technology of surveillance and control*, Statewatch Analysis, No. 106, 2009, p. 1. http://www.statewatch.org/analyses/no-106-the-droning-of-drones.pdf

[94] McCormack, Edward D., *The Use of Small Unmanned Aircraft by the Washington State Department of Transportation*, Washington State Transportation Center, June 2008.

various environmental hazards. UASs fitted with electro-optical sensors "can identify an object the size of a milk carton from an altitude of 60,000 feet".[95] Microdrones, such as the SkySeer, can also be fitted with video cameras, thermal imaging devices, radiation detectors, mobile-phone jammers and air sampling devices.[96] Some have also discussed the possibility of putting weapons on UASs used for policing.[97] One of the main advantages from UASs is that they are almost undetectable to the person(s) or target(s) being surveilled[98] and can operate almost in silence[99].

Unmanned aircraft systems have been used extensively in military applications, primarily by the USA and the UK, however they also have applications in policing, border control, emergency response and for monitoring environmental hazards. Police forces in the UK, Netherlands, Switzerland, Belgium, France, Italy and Germany have all used UAS devices to monitor individuals such as festival-goers, squatters, undocumented workers, demonstrators and hooligans.[100] Austria, the UK and Frontex, the European border agency, have also demonstrated or used UASs for border surveillance.[101] According to Wilson, drones were so effective in the Gulf War that "Iraqi troops began to associate the sound of the little aircraft's two-cycle engine with an imminent devastating bombardment", which he says led to "the first instance of human soldiers surrendering to a robot".[102]

Imaging scanners

We define imaging scanners as systems which detect non-visible waves on the electro-magnetic, sonar, heat or other spectrums and use these to produce a visible image. Examples include infrared scanners, sonar imaging, thermal imaging, x-ray imaging, radiation or millimetre wave imaging. Some of the most common surveillance deployments of imaging scanners include the recent use of body scanners in airports and the use of thermal imaging to find crime suspects or identify criminal activity (such as indoor marijuana cultivation). Hiranandani also identifies electromagnetic radiation imaging as a source of concern, as these devices can be easily made and can reproduce the images on a computer screen through walls from across a street.[103] Some imaging scanners are portable, and can be attached to drones or helicopters. Other imaging scanners, such as x-ray backscatter and passive or active millimetre wave scanners primarily installed in airports, are fixed in place. However, some portable passive millimetre wave scanners have appeared on the market. Each of these body-scanning systems uses the distinctions between the chemical components of a human body and other substances to detect when an individual is carrying concealed weapons on their

[95] *The Economist*, "Unmanned aircraft: The fly's a spy", 1 Nov 2007.
http://www.economist.com/displaystory.cfm?story_id=10059596

[96] Bowcott, Owen, and Paul Lewis, "Unmanned drones may be used in police surveillance", *The Guardian*, 24 Sept 2010. http://www.guardian.co.uk/uk/2010/sep/24/police-unmanned-surveillance-drones

[97] "A.I.R. (Ariel Intelligence and Response) to Help Law Enforcement", *WLTX*, 22 Mar 2011. http://www.wltx.com/news/article/129337/2/From-Toy-to-Life-Saving-Tool

[98] Lewis, Paul, "CCTV in the sky: police plan to use military-style spy drones", *The Guardian*, 23 Jan 2010. http://www.guardian.co.uk/uk/2010/jan/23/cctv-sky-police-plan-drones

[99] OPARUS, "Concept and Approach", 2010. http://www.oparus.eu/index.php/concept-a-approach

[100] Eick, op. cit., 2009.

[101] Eick, op. cit., 2009.

[102] Wilson, J.R., "UAVs: A Worldwide Roundup", *Aerospace America*, June 2003.
https://www.aiaa.org/aerospace/Article.cfm?issuetocid=365&ArchiveIssueID=39

[103] Hiranandani, V., "Under-Explored Threats to Privacy: See-Through-Wall Technologies and Electro-Magnetic Radiation", *Surveillance & Society*, Vol. 8, No. 1, 2010, pp. 93-98.

person. Some of these systems also incorporate privacy enhancing technology (PET) elements, such as remote operator work stations or software filters that blur sensitive areas of the body[104]. Yet, these PETs are only effective if they are guaranteed to be installed by default and if they cannot be switched off.[105]

While infrared, thermal and other types of portable imaging scanners have been available to law enforcement agencies for some time, the use of body scanners in airports and other locations is relatively recent, but increasingly widespread. The deployment of body scanners in airports has primarily been concentrated in the USA, and the Transportation Security Administration (TSA) claims on its website that there are currently 486 scanners at 78 US airports[106]. Airports in the European Union represent another major site of body scanning technology. Schiphol airport in Amsterdam became one of the first major international airports to introduce body scanners in May 2007.[107] Rapiscan x-ray backscatter systems have also been deployed at Manchester Airport and London's Heathrow Airport since February 2010. Hamburg Airport began a six-month trial of two body scanners in September 2010[108] and France has begun a three-year trial of body scanners in "areas of airports not freely accessible to the public" in Paris Roissy and Charles de Gaulle airports[109]. *Jaunted* web-magazine has also reported the use of body scanners in Rome's Leonardo da Vinci airport[110] and L-3 Communications report the use of their body scanners in Madrid Barajas International Airport[111]. Canada[112], Russia[113] and Nigeria[114] have also deployed body scanners in their airports. The Australian government announced its intention to deploy scanners in late 2011 as has Japan, India, South Africa and Kenya,[115] while the European Commission reports that China (including Hong Kong) and South Korea are interested in the technology.[116] In addition to airports, body scanners are being deployed in other contexts, such as border

---

[104] Rapiscan Systems, "Backscatter/ Rapiscan Secure 1000 Dual Pose", 2011. http://www.rapiscansystems.com/rapiscan-secure-1000.html

[105] Mordini, Emilio, *Whole Body Imaging at airport checkpoints: the ethical and policy context, HIDE and RISE Projects*, POLICY Report N° 2010/01, Feb 2010.

[106] Transportation Security Administration, "Advanced Imaging Technology (AIT)", 2011.

http://www.tsa.gov/approach/tech/ait/index.shtm

[107] United Press International (UPI), "Airliner attack re-ignites scanner debate", 29 Dec 2009.

http://www.upi.com/Top_News/Special/2009/12/29/Airliner-attack-re-ignites-scanner-debate/UPI-98181262114910/

[108] *Privacy International, Germany - Privacy Profile*, 26 Jan 2011.

https://www.privacyinternational.org/article/germany-privacy-profile

[109] Privacy International, *France - Privacy Profile*, 22 Jan 2011.

https://www.privacyinternational.org/article/france-privacy-profile

[110] JetSetCD, "Updated: What Airports Have Full-Body Scanners Right Now", *Jaunted*, 2 Mar 2010. http://www.jaunted.com/story/2010/3/1/232031/9854/travel/Updated%3A+What+Airports+Have+Full-Body+Scanners+Right+Now

[111] L-3 Communications, "TSA to Test L-3 Millimeter Wave Portals at Phoenix Sky Harbor Airport", 11 Oct 2007. http://www.l-3com.com/news-events/pressrelease.aspx?releaseID=1061924

[112] European Commission, Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports COM(2010) 311/4 , Brussels, 2010.

[113] Ibid.

[114] Associated Press, "Dutch to use full body scanners for U.S. flights", *MSNBC.com*, 30 Dec 2009. http://www.msnbc.msn.com/id/34630097/ns/us_news-airliner_security/

[115] European Commission, op. cit., 2010.

[116] Ibid.

crossings and for security checks at US courthouses, jails and other government facilities[117] to check for weapons, drugs or other prohibited materials.[118] Although not related to surveillance, body scanners have been recently installed in retail settings to assist with fittings and tailoring.[119] Thermal and infrared imaging scanners may also be used for disaster relief or emergency response (searching for survivors) and by various government, law enforcement and security authorities to search for suspects or gather information about the number and location of occupants in a building. In these contexts, the surveilled include passengers, those who visit courtrooms, inmates in prisons and criminal suspects.

Satellites (earth observation, "keyhole" satellites)

Earth observation, communication, keyhole and other satellites have been orbiting the earth since the beginning of the space programme. Initially, these satellites were used for military reconnaissance and to provide weather information to assist meteorologists. More recently, such satellites have become more powerful and been used for a number of military and civilian applications. Aquilina notes that satellites have assisted law enforcement in intercepting or obtaining information about various types of signals from mobile phones, radio transmissions, mobile data links, emails, IP addresses, file transfers, virtual private networks and messages sent to websites.[120] Satellites also assist the military and other state authorities in reconnaissance operations, and can take static photographs or video of places or people.[121] Some satellites have an imaging resolution of 0.6 metres[122] and US government satellites, such as keyhole satellites, are thought to be even more powerful. Satellites are also operated by private firms, and provide services such as location based services for mobile phones, satellite navigation services for cars or other vehicles, vehicle location tracking and recovery services, tracking of individuals (children[123], shoppers[124], etc.), emergency services, environmental management (such as erosion tracking), disaster response services and images for entertainment. The surveilled can include almost anyone, but drivers, employees, those with smart phones and others who use location services are most affected.

2.2.2 Dataveillance

The term "dataveillance" denotes surveillance based on the electronic data traces typical for the modern world. Roger Clarke, who coined the term back in 1988, observed the increasing pervasiveness of such day-to-day data traces: "trends include the integration with EFTS [Electronic Funds Transfer System] of air-travel systems and telephone charging; road traffic monitoring, including vehicle identification, closely integrated with ownership and driver's-

[117] L-3 Communications, "TSA to Test L-3 Millimeter Wave Portals at Phoenix Sky Harbor Airport", 11 Oct 2007.

[118] airport-technology.com, "Cook County Selects L-3 ProVision™ Whole Body Imaging Solution for Deployment across Large Prison Complex", 10 Feb 09. http://www.airport-technology.com/contractors/security/l-3_security/press22.html

[119] Unique Scan, "Custom clothing and apparel", 2011. http://www.uniquescan.com/

[120] Aquilina, Kevin, "Public security versus privacy in technology law: A balancing act?", *Computer Law & Security Review*, Vol. 26, 2010, pp. 130–143.

[121] Ibid.

[122] Satellite Imaging Corporation, "Using Google Earth to Plan High-Resolution Satellite Image Data", 2011. http://www.satimagingcorp.com/google_earth.html

[123] Johnson, Bobbie, "GPS wristwatch helps parents track children", *The Guardian*, 12 Jan 2009.

http://www.guardian.co.uk/technology/2009/jan/12/num8-gps-wristwatch-child-security

[124] Richards, Jonathan, "Shops track customers via mobile phone", *Times Online*, 16 May 2008. http://technology.timesonline.co.uk/tol/news/tech_and_web/article3945496.ece

license records; computerization and integration of court records, criminal records, fingerprint records, and criminal-investigation systems; ... and homes wired for reasons of employment, security, entertainment, and consumerism".[125]

Electronic traces have since become ubiquitous: Employers can monitor employees' calls, e-mails and even computer keystrokes[126]; cellular phone companies have access not only to the calls but also the whereabouts of their customers; credit card companies know their clients' online and offline shopping habits; Internet service providers can inspect their subscribers' data traffic; operators of electronic highway tolls know when and where their subscribers drive. Clarke himself noted in 2003 the broadening and continuous sophistication of electronic data traces – and thus, of potential dataveillance sources – in the 15 years that had passed since 1988 when he coined the term. Among (then) newly emerged technologies, he identified "loyalty" schemes, person location and tracking, digital signature technologies and PKIs (public-key infrastructures), Internet tracing, spyware (i.e., software that calls home), highway tolls, digital rights management, and biometrics.[127]

Clarke distinguishes between "personal dataveillance", the monitoring of the data of one specific person, and "mass dataveillance", the systematic investigation or monitoring of groups of people via their data traces.[128] *Personal dataveillance* represents the act of monitoring a specific targeted individual via his or her data. The data gathered for personal dataveillance may include credit card usage, shopping patterns (via loyalty schemes for physical shopping, or access to the databases of Internet shops for online shopping), or monitoring the surveilled's e-mail and Internet usage (e.g., via his or her Internet service provider). To some extent, personal dataveillance can also reveal the surveilled's whereabouts. The location can be inferred, for example, from the monitoring of financial transactions (by knowing when and where a credit or debit card has been used), or from electronic toll collection systems installed in the target's car. Despite some overlaps with the information that can be gained from physical surveillance (e.g., the physical location) and communication surveillance (e.g., the subject's phone calls), the information from personal dataveillance is typically complementary to these. Its advantage is that while other types of surveillance can only partly (or not at all) be automated, dataveillance is essentially computer-based, and thus relatively cheap to deploy and easily scalable. *Mass dataveillance* monitors the data traces of large groups of people in order to identify individuals with a specific profile (e.g., individuals considered potentially dangerous): "mass dataveillance is concerned with groups of people and involves the generalized suspicion that some (as yet unidentified) members of the group might be of interest".[129]

Data mining and profiling

The main method deployed for mass dataveillance is data mining. Definitions vary slightly, but *data mining* is usually understood as the "nontrivial extraction of implicit, previously

[125] Clarke, Roger, "Information Technology and Dataveillance", *Communications of the ACM*, Vol. 31, No. 5, 1988, pp. 498-512.

[126] Wright, David, Michael Friedewald, Serge Gutwirth, Marc Langheinrich, Emilio Mordini, Rocco Bellanova and Paul De Hert, "Sorting out smart surveillance", *Computer Law & Security Review*, Vol. 26, No. 4, 2010, pp. 343-354.

[127] Clarke, Roger, "Dataveillance – 15 Years On", *Privacy Issues Forum,* Wellington, New Zealand, 2003, pp. 15-18.

[128] Clarke, op. cit., 1988.

[129] Ibid.

unknown and potentially useful information from data"[130], or a "procedure by which large databases are mined by means of algorithms for patterns of correlations between data"[131].[132] Such correlations indicate a relation between the data, without necessarily establishing causes or reasons – data mining is thus sometimes referred to as a discovery-driven approach as opposed to the more traditional assumption-driven approach.[133] Various types of algorithms can be deployed for data mining, and the field is being constantly expanded. The individual algorithms come from fields such as complex algorithms, artificial intelligence, neural networks, and genetic-based modelling.[134]

Mass dataveillance is thus also closely related to *profiling*. Profiling is "a means of generating suspects or prospects from within a large population and involves inferring a set of characteristics of a particular class of person from past experience, then searching data-holdings for individuals with a close fit to that set of characteristics".[135] The main application domains of profiling are the targeted assessment of consumer behaviour, risk assessment for insurances, and criminal profiling. Data mining is typically the first step in this process, as it defines the classes ("suspects or prospects") that users can then be profiled into. Profiling then attempts to predict, or at least pre-empt, individual future behaviour by relying on the stereotypes learned during the data mining step, ultimately classifying individuals as potential risks or commercial windfalls.

Companies, however, look already into research that goes beyond stereotype building, into individually understanding each client's needs (reaching thus highly individualised 'profiles' of a single individual). Wal-Mart, for example, acquired Kosmix (now called @WalMartLabs) in order to connect people, places, and things through people's online social media conversations (e.g., tweets).[136] The system might catch a text such as "Went to Bellevue movie centre to see Spiderman2", and from this connects the poster's identity to the particular movie theatre and the movie. They call the resulting graph the "social genome". The closest Wal-Mart store might then decide to stock more Spiderman DVDs in anticipation of increased sales of the movie prequel.

---

[130] Frawley, W.J., G. Piatetsky-Shapiro, and C. J. Matheus, "Knowledge Discovery in Databases : An Overview", *AI Magazine*, Vol. 13, No. 3, 1992, pp. 57-70.

[131] Hildebrandt, Mireille, "Defining Profiling: A New Type of Knowledge?", in Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer, New York / Heidelberg, 2008, pp. 17-46.

[132] Dependent on the context, "data mining" can refer either to the entire field of research, or a particular method within the field. Sometimes, the field has also been called "knowledge discovery in databases" (KDD), most notably by Frawley et al., *op. cit*., 1992 and Fayyad, U., G. Piatetsky-Shapiro and P. Smyth, "From Data Mining to Knowledge Discovery in Databases", *AI Magazine*, Vol. 17, No. 3, 1996, pp. 37-54. In this view, data mining is just one step of the KDD process, which comprises data preparation, data selection, data cleaning, data aggregation, (data mining), and interpretation of the results. Due probably to the catchiness of the "mining for data" image, as well as the fact that all the other steps in this view are not by far as challenging and interesting as data mining, this view has not become prevalent and "data mining" typically denotes the entire process and is thus a (much more commonly used) synonym for KDD.

[133] Hildebrandt, op. cit., 2008.

[134] Zarsky, T.Z., "Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion", *Yale Journal of Law & Technology*, Vol. 5, 2003, pp. 1-56.

[135] Clarke, Roger, "Profiling: A Hidden Challenge to the Regulation of Data Surveillance", *Journal of Law and Information Science*, Vol. 4, No. 2, 1993, pp. 403-419.

[136] Roush, Wade, "Inside WalmartLabs: How the Former Kosmix Team Plans to Help the World's Largest Retailer Get Social and Mobile", *Xconomy.com*, 1 Aug 2011. http://www.xconomy.com/san-francisco/ 2011/08/01/ inside-walmartlabs-how-the-former-kosmix-team-plans-to-help-the-worlds-largest-retailer-get-social-and-mobile/

Databases, data retention

The amount of (digital) information processed every day is staggering. Google was reported to handle over 20 petabytes of data each day back in 2008, while Twitter's 140-character tweets required four petabytes of storage per year in 2010. Facebook's recent data centre move required the migration of 30 petabytes of data,[137] and Ebay, a popular online auction site, is said to handle more than 80 petabytes (80 000 terabytes, or 80 million gigabytes) of data every day.[138,139] The National Security Agency (NSA) began construction of a new cyber intelligence centre in Utah in 2011,[140] with an envisioned storage measured in "hundreds of petabytes", if not "yottabytes".[141] According to a 2011 IDC report, the amount of digital information created in the world in 2010 for the first time exceeded a "zettabyte" (1 trillion gigabytes).[142] Cisco, one of the world's largest communications technology providers, expects that by 2015 the Internet will carry a zettabyte of data (cf. Figure 2.1) per year.[143]

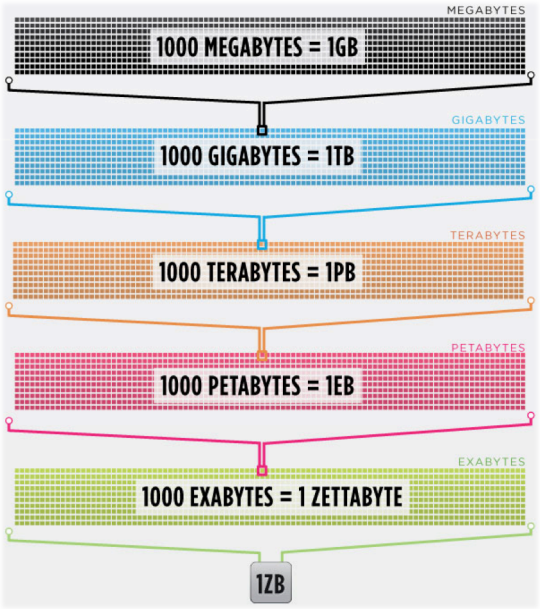


Figure 2.1: From megabytes to zettabytes
(Image source: http://blogs.cisco.com/news/the-dawn-of-the-zettabyte-era-infographic/)

---

[137] Watters, Audrey, "Strata Week: How Facebook moved 30 petabytes of Hadoop data", *O'Reilly Radar*, 28 July 2011. http://radar.oreilly.com/2011/07/facebook-hadoop-nebula-libraries.html

[138] Ratzesberger, Oliver, LinkedIn personal page. http://www.linkedin.com/in/oliverratzesberger

[139] Monash, Curt, "eBay followup — Greenplum out, Teradata > 10 petabytes, Hadoop has some value, and more", Personal Blog, 6 Oct 2010. http://www.dbms2.com/2010/10/06/ebay-followup-greenplum-out-teradata-10-petabytes-hadoop-has-some-value-and-more/

[140] Storm, Darlene, "Shadowy eyes and ears of NSA to modernize with cloud and crypto centers", *Computerworld Blogs*, 26 May 2011.

http://blogs.computerworld.com/18363/shadowy_eyes_and_ears_of_nsa_to_modernize_with_cloud_and_crypto_centers

[141] Coldewey, Devin, "NSA to store yottabytes of surveillance data in Utah megarepository (update: not so much)", 2009. http://techcrunch.com/2009/11/01/nsa-to-store-yottabytes-of-surveillance-data-in-utah-megarepository/

[142] Gantz, John, and David Reinsel, "The 2011 Digital Universe Study: Extracting Value from Chaos. IDC iView", 2001. http://idcdocserv.com/1142 for the print version; http://www.emc.com/collateral/demos/microsites/emc-digital-universe-2011/index.htm for the video.

[143] Cisco, "Entering the Zettabyte Era", 2011. http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/VNI_Hyperconnectivity_WP.pdf

Traditional Database Management Systems (DBMS) that use online storage (i.e., spinning disks) supporting real-time data access are typically able to handle databases up to a few petabytes of storage. Combining several such instances, online storage company EMC forecasts that by 2012 it will have the first customers with more than thousand petabytes of storage (an exabyte).[144] Not all data requires the transactional processing power of traditional DBMS. For example, searching a huge index of Web pages (e.g., Google) requires fast lookups but can tolerate slow, batch triggered updates. Such so-called "big data" datasets typically use parallel processing techniques to make working with them feasible. The Apache Hadoop Framework[145] is a popular example of such a system: it offers distributed, reliable data storage combined with high-performance parallel data processing, using a technique called "MapReduce". Hadoop runs on a collection of regular servers, without the need for any special high-performance hardware. It is open-source and actively used by virtually all major Internet services companies, such as Google, Facebook, Amazon, and Yahoo.[146]

Data integration: data warehouses, data marts and data federation

DBMS and parallel data processing frameworks like Hadoop are typically used for *transactional data*, i.e., data that is frequently updated in order to provide a current snapshot of information. Historic data, i.e., the development of transactional data over time, has different requirements regarding size and speed of access/update. Long-time retention of data is handled in so-called "data warehouses", that allow so-called "data marts" to analyse the development of data over time.

Data warehouses (DWs) target analytical needs, not operational needs.[147] DWs integrate all available data in an enterprise – in particular data development over time (historic) – to support managerial decision making process. Data in DWs is typically never updated, but just added to (contrast this with an inventory database that is constantly updated to show current inventory levels). DWs form the basis for data marts (DMs) that extract derived data from the primitive (raw) data stored in the DW. DWs have typically fewer constraints on response time (response times of up to 24 hours may still be ok) and on the number of users/concurrent accesses.

A data federation (DF) is the combination of several distributed DBMS, DMs, and DWs into a single, unified data access.[148] They are typically used in situations where specific queries need to be performed on current data that is held in multiple systems. DF is also sometimes called "data virtualization" or "distributed queries". In contrast to a data warehouse, data federations are quicker to setup yet have higher requirements regarding system availability, computing resources, and underlying data quality. In order to combine multiple data sources into such a unified view, all heterogeneities between their data models must be resolved, i.e., conflicting names, concepts, cardinalities, attributes, etc. must be properly mapped to allow for data integrity in the resulting DF.

---

[144] Hollis, Chuck, "EMC's Record Breaking Product Launch", *Chuck's Blog – an EMC insider's perspective on information, technology, and customer challenges*, 14 Jan 2011. http://chucksblog.emc.com/chucks_blog/2011/01/emcs-record-breaking-product-launch.html

[145] The Apache Software Foundation, "Welcome to Apache Hadoop!", 2011. http://hadoop.apache.org/

[146] Hadoop Wiki, "Powered by Hadoop", 2011. http://wiki.apache.org/hadoop/PoweredBy

[147] Inmon, W.H., *Building the Data Warehouse*, 4th edition, Wiley, Indianapolis, 2005.

[148] Heimbigner, Dennis, and Dennis McLeod, "A Federated architecture for information management", *ACM Transactions on Information Systems,* Vol. 3, No. 3, 1985, pp. 253–278.

Cyber surveillance

The term *cyber surveillance* typically refers to the tracking of online behaviour, which in most cases is synonymous with browser activity (i.e., Web surfing). In a broader sense, however, it can also include the monitoring of all Internet traffic, i.e., including e-mail, peer-to-peer connections, VoIP, remote logins, file download (FTP), or instant messaging (IM). While the surveillance of computer-based communication between two humans will be covered below (i.e., in the "communication surveillance" section), here we refer both to the generic concepts of cyber surveillance and the specific surveillance of Web surfing.

Maybe the simplest and most limited, but probably the most prevalent form of cyber surveillance is represented by the so-called cookies. Cookies were originally developed to cope with a drawback of the HTTP (Web surfing) protocol. HTTP is a stateless protocol, which means that visits with a web browser to the same webpage are by and large isolated events; there is no memory of previous visits – i.e., there is no state. While this feature contributed to HTTP's simplicity and quick spreading, it also represents a downside for Web applications. A virtual shopping cart, e.g., must "remember" all items placed in it, no matter how long the user continues to browse the different pages of a web shop, and no matter how long the pauses between those page visits are. Cookies are small pieces of text, typically name-value pairs, which a web server can place on the client's computer to store precisely such data. Whenever the user subsequently visits (i.e., requests) one of the web pages of the same web site, the browser will send the previously stored cookie along with the request. In the above example, the state of the virtual shopping cart is stored inside a cookie; at any new visit (even after a browser or computer restart), the cart's previous state is still available. While the basic functionality is innocuous enough, the fact that web pages can be combined with elements (e.g., images) from many different web sites allows a single site to track users across a range of different sites. Many companies have since specialized in tracking users in such a fashion using so-called "tracking cookies" or "web bugs" across two or more seemingly unrelated websites to learn about the user's surfing preferences.[149] Overall, though, while they have been largely debated in the media, the surveillance potential of cookies is rather limited.

More powerful surveillance opportunities lie with Internet service providers (ISPs). In many countries, ISPs are already required by law to record so-called "traffic data", i.e., the individual connections made from each connected computer, for several months. Aside from webpage URLs, these connections include, for example, e-mail headers, FTP connections and VoIP calls. These will be discussed in more detail in section "communication surveillance" below. ISPs can also use a technique called "deep packet inspection" (DPI), which analyses each data packet passing between their customers and the Internet in order to extract its semantic content. While DPI can be used for non-surveillance purposes (such as network management or Internet statistics),[150] it can also be used as a censorship tool, for example, by blocking certain application types. Anyone with an Internet connection is subject to surveillance via the storage of traffic data.

[149] Symantec, "Tracking Cookie", 2009. http://www.symantec.com/security_response/writeup.jsp?docid=2006-080217-3524-99

[150] See, for example, iPoque's study about the relative weight of different Internet applications: Schulze, Hendrik, and Klaus Mochalski, "Internet Study 2008/2009", 2009. http://www.ipoque.com/sites/default/files/mediafiles/documents/internet-study-2008-2009.pdf

Independently of ISPs, there is a plethora of so-called "parental control" software that locally monitors computer activity, including text-based communication.[151] Once installed, such software – usually advertised for the monitoring of children's or employees' online actions – exhaustively monitors all activity on the computer, such as the content of sent and received e-mails and IM chats, social network activity, visited websites and more. All keystrokes are registered and the surveillant receives hidden, complete reports at an e-mail of choice, with an adjustable frequency of 30 minutes to 24 hours. Without administrator's rights, the average user has little chance to find out that such sniffing software is installed, and even with administrator access, the software is difficult to discover.[152] Furthermore, once installed, the software can be remotely administrated, so the surveillant does not need to gain access to the computer again to modify its settings.[153] If not even a first access to the computer can be guaranteed, more refined versions of such software can be sent via a Trojan horse, for example as part of an email – if the target opens the e-mail, the sniffing software installs automatically. The German government developed and deployed such a "government Trojan" for the surveillance of suspected terrorists[154]; the lack of transparency of its deployment policies, as well as its weak security mechanisms, which might allow third parties access to the collected data, recently spurred a significant amount of controversy.[155]

Finally, more subtle types of cyber surveillance are emerging. In 2007, Google patented the creation of "psychological profiles" from playing online games: "User dialogue (e.g. from role playing games, simulation games, etc) may be used to characterize the user (e.g. literate, profane, blunt or polite, quiet, etc.). Also, user play may be used to characterize the user (e.g., cautious, risk-taker, aggressive, non-confrontational, stealthy, honest, cooperative, uncooperative, etc)."[156] It recently launched games on its social network "Google Plus" that require significant access to one's friendship "circles" and other personal data.[157]

2.2.3 Biometrics

Biometrics refers to the use of measurements and analysis of human body characteristics to distinguish between individuals. In general, biometrics relies upon pattern recognition, where individuals are enrolled in the system, and the image of the biometric is converted into a binary code using an algorithm.[158] There are two types of biometrics: physical characteristics such as fingerprint, face or iris patterns and behavioural characteristics such as voice,

---

[151] Naraine, R., "First Look: Sentry Remote and eBlaster 6.0", *PC World*, 2007.
http://www.pcworld.com/article/139460/first_look_sentry_remote_and_eblaster_60.html

[152] Greene, T. C., "eBlaster spyware has Achilles heel", *The Register*, 16 June 2003.
http://www.theregister.co.uk/2003/06/16/eblaster_spyware_has_achilles_heel/

[153] Bradley, T., "eBlaster 6.0 Review", *about.com*.
http://netsecurity.about.com/od/readproductreviews/gr/eBlaster6.htm

[154] Steinhäuser, M., "Gegenangriff auf Schäuble", *Zeit Online*, 2007.
http://www.zeit.de/online/2007/35/bundestrojaner-reaktionen/

[155] Der Spiegel, "CCC findet Sicherheitslücken in Bundestrojaner", 9 October 2011. http://www.spiegel.de/netzwelt/netzpolitik/0,1518,790756,00.html

[156] Adam, David, and Bobbie Johnson, "Google may use games to analyse net users", *The Guardian*, 12 May 2007. http://www.guardian.co.uk/media/2007/may/12/newmedia.news

[157] Spoerry, Paul, "Google+ Games – Watch your privacy", *PlusHeadlines.com*, 13 Aug 2011. http://plusheadlines.com/google-games-watch-your-privacy/1024/

[158] Zureik, Elia, and Karen Hindle, "Governance, Security and Technology: The Case of Biometrics", *Studies in Political Economy*, Vol. 73, Spring/Summer 2004, pp. 113-137.

signature or gait patterns.[159] Biometrics can be used for identification, where an individual's pattern is matched to many records, or authentication, where an individual's pattern is checked against the one stored in their record. Zuriek and Hindle caution, however, that "the idea here is not to confirm that people are who they say they are, but to check if the temporary template is present in the stored files of reference templates."[160]

Fingerprints

Fingerprints are one of the oldest biometric technologies. While fingerprints were once checked manually, currently they are digitised and loaded onto databases for "instant, remote and automatic checking".[161] Therefore, fingerprint checking now requires a range of information technology accompaniments, such as a scanning device, software, a database and, often, encryption. Adkins explains that scanned fingerprints are examined for unique features and then stored as a mathematical template.[162] An algorithm is generated from the template and stored to compare against later scans. She continues, "law enforcement officials rely upon a score indicating the closeness of the presented biometric to the stored template using the help of a predefined number or algorithm to determine whether the images are sufficiently close enough to be considered a match".[163] However, depending upon the sensitivity of the authentication scheme, false negatives (i.e. rejection of authorised individuals) and false positives (i.e. false identification of individuals) may occur.

As stated above, fingerprinting systems are used to either identify or verify. They are being used in an increasing number of applications, including national identity systems, criminal justice systems, immigration and border control, public transport, commercial applications (such as CitiBank's new fingerprint authentication system for bank accounts)[164], in schools and to prevent duplicate claims in immigration and asylum seeking in Europe as well as social assistance systems in some countries. These applications are also becoming interlinked, where, for example, the FBI has announced two major initiatives on biometrics: Next Generation Identification, which will build the largest database in the world of biometrics, and Server in the Sky, which will allow the FBI to cooperate with law enforcement agencies in other countries, such as the UK, Australia and Canada.[165] While most associate fingerprinting with criminal suspects, fingerprinting is increasingly being used in other contexts as an access control mechanism. Lyon concludes his discussion of biometrics by pointing out that,

> If we take Canada and the USA, for example, contemporary biometric identification has been developed for crime control (law enforcement), social assistance (welfare recipients) and border control (passport issuance) purposes. In each case, already marginalized or disadvantaged persons – criminals, the poor and people of colour –

[159] Wei, Gang, and Dongge Li, "Biometrics: Applications, Challenges and the Future", in Katherine J. Strandburg and Danela Stan Raicu (eds.), *Privacy and Security Technologies: An Interdisciplinary Conversation*, Springer, New York, 2006, pp. 135-150.

[160] Zureik and Hindle, op. cit., 2004.

[161] Lyon, David, "Biometrics, Identification and Surveillance", *Bioethics*, Vol. 22 No. 9, 2008, p. 500.

[162] Adkins, Lauren D., "Biometrics: Weighing Convenience and National Security Against Your Privacy", *Michigan Telecommunications Technology Law Review*, Vol. 13, 2007, pp. 541-555. http://www.mttlr.org/volthirteen/adkins.pdf

[163] Ibid., p. 542.

[164] Lyon, op. cit., 2008.

[165] Lyon, op. cit., 2008.

> are in view and the aim of these systems is to distinguish between those that should be included or excluded, trusted or not and so on.[166]

However, some countries are considering universal fingerprint databases linked with passports, thus mitigating some of the focus on marginalised populations as subject to this surveillance practice.

DNA

DNA fingerprinting was first introduced by Prof. Alec Jeffreys at the University of Leicester in 1984. According to Van Camp and Dierickx, "it is currently considered the most accurate identification tool available to law enforcement agencies".[167] DNA fingerprinting often uses a profiling technique whereby *short tandem repeats* (STRs) are analysed. These STRs are repeated sequences of DNA, the lengths of which are thought to be unique for every individual. This means they can be used for forensic purposes. But, using an STR technique, there is a slight chance that even when a match is established, it is a false positive, because the technique selects certain repeating sequences to analyse rather than an individual's entire DNA sequence. As such, Van Camp and Dierickx caution that DNA matching is probabilistic. When DNA samples are degraded, another technique called mitochondrial DNA analysis is often used. However, this technique cannot distinguish between individuals born from the same mother. Even close matches using STR might actually be the result of a sibling or other close relative match rather than the individual tested.[168]

Like other biometric techniques, DNA profile matching relies upon a database of known individuals, and DNA identification is only successful if the sought individual is on the database, or if it can be matched to a known suspect. Williams and Johnson argue that the ability to digitally represent DNA profiles and to store and search them in a computerised database has greatly expanded the role for DNA profiling in criminal investigations as well as other applications.[169] The FBI in the USA and the European Union have sought to take advantage of this potential in the criminal justice system to link up and enable cross-jurisdictional searching of DNA profiles. Other applications include the identification of remains for military personnel and the identification of family relationships for immigration purposes. In fact, the first use of Jeffreys' research methods was to test the truthfulness of a claim to family relationship in a UK immigration case.[170] DNA profiling for matching has been implemented in the context of criminal justice throughout Europe, in the USA, Canada and Australia, as well as many other countries. While the UK has the largest criminal justice DNA database, the USA is thought to have the largest military DNA database.[171] Austria, Germany, France and the Netherlands all introduced criminal justice DNA databases in 1998,

---

[166] Lyon, op. cit., 2008, p. 505.

[167] Van Camp, Nathan, and Kris Dierickx, "The Expansion of Forensic DNA Databases and Police Sampling Powers in the post-9/11 Era: Ethical Considerations on Genetic Privacy", *Journal of the European Ethics Network*, Vol. 14, No. 3, 2007, p. 238.

[168] Hibbert, Michelle, "DNA Databanks: Law Enforcement's Greatest Surveillance Tool", *Wake Forest Law Review*, Vol. 34, 1999, pp. 767-825.

[169] Williams, Robin, and Paul Johnson, "Inclusiveness, Effectiveness and Intrusiveness: Issues in the Developing Uses of DNA Profiling in Support of Criminal Investigations", *Journal of Law and Medical Ethics*, Vol. 33, No. 3, 2005, pp. 545-558.

[170] Williams and Johnson, op. cit., 2005.

[171] Nelkin, Dorothy, and Lori Andrews, "DNA identification and surveillance creep", *Sociology of Health & Illness,* Vol. 21, No.5, 1999, pp. 689–706.

while Finland and Belgium introduced them in 1999 and Denmark introduced one in 2000.[172] Later criminal justice databases included the introduction of the Spanish database in 2008[173] and the Republic of Ireland database in 2010[174]. In criminal justice databases, samples can be taken from a range of different types of offenders. In some jurisdictions, only violent criminals convicted of serious crimes can be included on a DNA database, whereas in other contexts, DNA samples can be taken, and stored, for anyone arrested. Consent emerges as a serious issue in that some police forces, such as those in the UK, are able to use reasonable force to take a DNA sample from arrested individuals, and military personnel in the USA are only able to refuse to submit a DNA sample for serious religious reasons.[175] Furthermore, in addition to criminals, suspects and military personnel, victims, volunteers, and even the family members of people already on DNA databases may potentially make up the population of the surveilled.

Facial recognition

Like other biometric systems, facial recognition technology works by matching an image of a person with an image stored on a database. Facial recognition technology involves capturing a still image of a person's face, or multiple still images of a person's face, and then using computer software to measure the distance between a number of nodal points on the individual's face.[176] Thus, like fingerprints, the individual's face is transformed into a mathematical template. The digitised image is then loaded onto a database, which enables computerised searching and matching to faceprints already on file.[177] A number of researchers have pointed out that facial recognition technology is not particularly effective at identifying faces in a crowd, and works best when individuals voluntarily enrol and then cooperate with the identification system.[178] Zureik and Hindle also point out that as of 2004, changes in appearance such as hairstyle, a new beard or glasses will cause problems for facial recognition systems.[179]

Facial recognition technology has a number of applications. It has been used "to verify identification for access to weapons, biohazards, nuclear materials, money, or criminal evidence", it has been used by Casinos "to identify card counters and other 'undesirables'" and the State of Virginia's Department of Motor Vehicles has been using it since 1998 "to check for duplicate and false driver's license registrations".[180] Facial recognition technology has also been used in new identity documents such as passports and more recently Facebook has implemented a facial recognition programme to enable users to more easily identify

[172] Van Camp and Dierickx, op. cit., 2007.

[173] "Spanish DNA database has helped solve 7,500 crimes", *The Olive Press*, 26 Apr 2011. http://www.theolivepress.es/spain-news/2011/04/26/dna-database-has-helped-solve-7500-crimes-in-spain/

[174] "An Irish law for a DNA Database", *EDRi-gram*, No. 8.1, 13 Jan 2010.

http://www.edri.org/edrigram/number8.1/irish-law-dna-database

[175] Nelkin and Andrews, op. cit., 1999.

[176] Stefani, John A., "Finding Waldo", in Katherine J. Strandberg and Danela Stan Raicu (eds.), Privacy and Security Technologies: An Interdisciplinary Conversation, Springer, New York, 2006, pp. 173-188.

[177] Ibid.

[178] Zureik and Hindle, op. cit., 2004 and Introna, Lucas D., and Helen Nissenbaum, *Facial Recognition Technology A Survey of Policy and Implementation Issues*, The Center for Catastrophe Preparedness & Response, New York University, New York, 8 Apr 2009.

[179] Zureik and Hindle, op. cit., 2004.

[180] Stefani, op. cit., 2006, p. 179.

photos of their friends.[181] Police in the USA may also begin using a hand-held facial recognition technology device to identify stopped suspects who refuse to identify themselves.[182] Those potentially surveilled by this technology include, but are not limited to, criminal suspects, employees, suspected or known terrorists, drivers, social network users and passport holders.

Iris recognition systems

Iris recognition systems have consistently performed as the most reliable biometric identification technology. These systems work by converting an image of the iris into a sequence of 1s and 0s.[183] Once this sequence is collected, an IrisCode is used to represent the pattern, and an individual's identity is verified when two IrisCodes are compared.[184] Adkins further explains that "iris recognition is based upon the failure of [the comparison] test. "Failure" occurs when less than one third of the bytes in the codes differ. When images of the same iris are compared, they fail the test. Hence, a score of zero would indicate a perfect match".[185] Iris recognition has been used primarily for air travel. Schiphol airport in Amsterdam was the first airport to introduce an iris scanning fast track system for passengers in 2002.[186] Similar systems were also installed in UK airports in 2005, and allowed "trusted travellers" to bypass immigration queues by enrolling in the system.[187] Iris scanning can also be used as an access control system for workplaces, homes or other sites.

Behavioural biometrics

Soft biometrics refers to biometric measurements that are behavioural and/or otherwise subject to change. Two often cited examples of soft biometrics include voice recognition systems and gait recognition systems. According to Wei and Lee, voice recognition systems work by capturing the voice of a person through a microphone and extracting certain features of their voice from the signals produced by their speech. These signals are then compared to known persons in a database.[188] While this method is most commonly used for access control, it has also been used in the UK to check whether known offenders are complying with the terms of their curfew orders[189] or to check if football hooligans are at home during match times[190]. Yet, Wei and Li point out that problems such as background noise and people's sensitivity about having their speech recorded will likely prevent wide-spread roll out of this technology.[191]

Gait recognition is a soft biometric technology which has been explored over the last 10-15 years. It involves people being identified through a computer analysis of the way they walk.

---

[181] Williams, Christopher, "Facebook facial recognition system criticised", *The Telegraph*, 8 June 2011. http://www.telegraph.co.uk/technology/facebook/8563464/Facebook-facial-recognition-system-criticised.html

[182] Steel, Emily, and Julia Angwin, "Device Raises Fear of Facial Profiling", *Wall Street Journal*, 13 July 2011.

[183] Wei and Li, op. cit., 2006.

[184] Adkins, op. cit., 2007.

[185] Adkins, op. cit., 2007, p. 545.

[186] Lyon, op. cit., 2008.

[187] McFerran, Ann, "Immigration in the Blink of an Eye", *The Sunday Times*, 14 Aug 2005.

[188] Wei and Li, op. cit., 2006.

[189] "Joyrider, 14, is first tagging guinea pig", *The Times*, 17 July 2001.

[190] Fay, Joe, "Dutch give football thugs a good talking to", *The Register*, 2 Sept 2005.
http://www.theregister.co.uk/2005/09/02/dutch_hooligans/

[191] Wei and Li, op. cit., 2006.

Wei and Li note that people can often recognise friends from a distance based on how they walk, and current research is developing an automatic gait-based person identification method.[192] Although the accuracy of gait recognition has not yet been optimised, the technology has created quite a bit of interest because it has the potential to identify individuals at a distance, it can make use of low resolution images and it can identify people without their cooperation.[193] Gait recognition works by measuring step length, hip, knee and foot joint angles and speed. Often images from CCTV cameras are used to provide forensic evidence in bank robberies or other, similar crimes where an individual has concealed his or her face.

2.2.4 Communications surveillance

Since ancient times, remote communications have been prone to interception: "Couriers have been waylaid, seals have been broken, and letters have been read".[194] Electronic communication forms are no exception; efforts towards their interception are as old as the communication technologies themselves: "Almost as soon as the telegraph appeared so did wiretapping and the same holds for efforts to intercept every new form of communication".[195] In the context of surveillance, the following technologies are relevant.

Wiretapping (electronic eavesdropping)

Electronic eavesdropping is "the act of electronically intercepting conversations without the knowledge or consent of at least one of the participants".[196] Strictly speaking, *wiretapping* defines a specific subset of electronic eavesdropping, where an actual wire is involved in the communication, "to tap a telephone or telegraph wire in order to get information".[197] Although encyclopaedias have not always caught up, the term is usually used for both wired and wireless communication, both by academia[198] and by the media[199]. It thus includes, next to landline telephony, the interception of mobile telephony and calls using the Voice-over-Internet-Protocol (VoIP).[200]

---

[192] Wei and Li, op. cit., 2006.

[193] Rani, M. Pushpa, and G. Arumugam, "An Efficient Gait Recognition System for Human Identification Using Modified ICA", *International Journal of Computer Science and Information Technology*, Vol. 2, No. 1, Feb 2010. http://airccse.org/journal/jcsit/0210ijcsit4.pdf

[194] Diffie, Whitfield, and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, 2nd ed., Vol. 17, MIT Press, Cambridge, MA, 2007, p. 2.

[195] Marx, Gary T., "What's New About the 'New Surveillance'? Classifying for Change and Continuity", *Surveillance & Society*, Vol. 1, No. 1, 2002, p. 20.

[196] Britannica. Electronic Eavesdropping, *Encyclopædia Britannica*, 2011.

http://www.britannica.com/EBchecked/topic/183788/electronic-eavesdropping

[197] Merriam-Webster, "wiretapping", *Merriam-Webster*, 2011. http://www.merriam-webster.com/dictionary/wiretapping

[198] Diffie, Whitfield, and Susan Landau, "Communications Surveillance: Privacy and Security at Risk", *Communications of the ACM*, Vol. 52, No. 11, 2009, pp. 42-47.

[199] *The Economist*, "Internet Wiretapping: Bugging the Cloud", 6 March 2008.

http://www.economist.com/node/10789393

[200] While wiretapping in this wider sense refers to the interception of any form of electronically-supported communication, wired or wireless, it is not exactly synonymous to "electronic eavesdropping". Unlike the latter, it does not include the electronic interception of non-electronic communication, such as the usage of hidden tape recorders, parabolic microphones or laser interferometers to intercept a conversation out of earshot. It is in this broader sense of wiretapping, but not entirely eavesdropping, that we use the term.

Common to all these forms of communication is that they could, in principle, be intercepted at numerous points along the path: in one of the devices used by the communication partners, as well as at various locations along the way. For a classic phone call, for example, this means inside one of the telephones themselves, in a junction box, a phone closet, on a telephone pole, or in the telephone company's central office.[201] Understanding the possible paths for each type of communication, along with specific attributes for each leg (e.g., a possible encryption of the signal) is thus vital in analysing the technological possibilities of interception.

Telephone lines

Starting in the 1970s and throughout the 1980s and 1990s, telephony gradually underwent fundamental technological shifts. The most important were threefold: i) the replacement of analogue signals through digital ones; ii) the substitution of fibre optics for both the former continental copper cables and intercontinental communication satellites[202], and iii) the transition from electromechanical circuit switching to computer-based switching.[203] These shifts also changed the nature of wiretapping, making it both easier in some aspects, and more difficult in others. In the old days, a telephone wiretap would have to be placed close to the telephone of the person of interest[204], before it started to be switched through the PSTN (Public Switched Telephone Network), which assigned a specific circuit to each call that lasted only for the duration of the call.[205] Furthermore, the presence of the wiretap could be detected by the small power drain at the target's phone.[206]

Digital wiretaps work remotely – they are typically installed in the telephone company's switch – and are not detectable by the surveilled.[207] Public telephone networks do not foresee encryption in their default configuration. When the digitised voice travels unencrypted over the telephone line, wiretapping is the trivial act of copying a bit stream – and the switches of telephone companies have the capability already built in.[208] As the voice travels in digitised form, though, users can use end-to-end encryption devices.[209] When strong end-to-end cryptography is used, the conversation cannot be wiretapped along the line – the only possibility lies in wiretapping either the telephone itself, or within the target's organisation before the device that encrypts the signal.

Mobile phones

[201] Diffie and Landau, op. cit., 2009.

[202] Marx, op. cit., 2002.

[203] Diffie and Landau, op. cit., 2008.

[204] Marx, op. cit., 2002.

[205] Landau, Susan, *Surveillance or Security?: The Risks Posed by New Wiretapping Technologies*, MIT Press, Cambridge, MA, 2011, p. 360.

[206] Diffie and Landau, op. cit., 2009.

[207] Diffie and Landau, op. cit., 2009.

[208] Marsan, C. D., "Internet community debates wiretapping", *CNN.com*, 1999.

http://edition.cnn.com/TECH/computing/9910/19/ietf.wiretap.idg/

[209] These come in numerous flavours, from rather home-brewed devices that can only be used in pairs by both parties and that use unknown, possibly unsafe algorithms (e.g., http://www.pimall.com/nais/voicekeeper.html) to enterprise-scale devices that use state-of-the-art encryption algorithms with a new key for every conversation (e.g., http://www.cisco.com/en/US/products/ps5853/index.html).

For GSM mobile phones, secure communication has been an aim from the outset: the protocol includes several security measures, such as challenge-response authentication, frequency hopping and the strong A5/1 encryption algorithm.[210] As a result, the over-the-air transmission of GSM signals has been considered secure for almost two decades since the system's launch in 1991. A first weakness was revealed in 2003: through a man-in-the-middle attack, the tampering entity can make the mobile phone use the weak A5/2 algorithm instead of A5/1.[211] Since 2009, A5/1 can also be broken.[212] The more recent A5/3 algorithm, the standard encryption in UMTS networks, has already been proven unsafe.[213] Breaking both A5/1 and A5/3 nowadays, though, still requires strong computation resources, which are unlikely to be used for trivial criminal investigations.

As argued above, however, understanding the entire path of communication is paramount for an analysis of surveillance opportunities. Even if intact, GSM's encryption algorithm does not work end-to-end. The communication, rather, is encrypted between the mobile phone and the base station it uses; it then travels unencrypted through the mobile provider's core network, to be encrypted again between the other telephone and its respective base station.[214] Means for so-called "lawful interception" (court-ordered wiretaps) are being built into the mobile networks equipment by its manufacturers. A so-called "Interception Management System (IMS)" sets up and manages lawful interception.[215] The challenge is not the wiretap (which consists of the technologically trivial creation of a copy of an unencrypted bit stream inside one of the network's switches), but to repel abuse. Despite various controls and safety features, the Greek case from 2004-2005, when the cellular phones of over 100 high-ranking government and military officials (including the prime minister) have been illegally wiretapped for over half an year, has plainly shown the perils of the technology.[216]

Voice-over-IP

The "Voice over Internet Protocol" (VoIP) is a collection of communication protocols that define how audio or audio-video conversations can use the Internet as communication medium instead of telephone lines. There are two major differences between telephony over the Internet and classic telephony: i) the communication is packet-based instead of circuit-switched[217]; and ii) in VoIP, the mechanisms for setting up and ending the conversation can be entirely different from the mechanisms used during the actual call[218]. For the actual

---

[210] Quirke, J., *Security in the GSM system*, Perth, Australia, 2004.

http://web.archive.org/web/20040712061808/www.ausmobile.com/downloads/technical/Security+in+the+GSM+system+01052004.pdf

[211] Barkan, E., E. Biham and N. Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", *Proceedings of the 23rd Annual International Cryptology Conference (Crypto2003)*, Springer, Santa Barbara, CA, 2003, pp. 600-613.

[212] Bradley, T., "GSM Encryption Cracked, Showing Its Age", *PC World*, 2009. http://www.pcworld.com/businesscenter/article/185552/gsm_encryption_cracked_showing_its_age.html

[213] Dunkelman, O., N. Keller and A. Shamir, "A Practical-Time Related-Key Attack on the KASUMI Cryptosystem Used in GSM and 3G Telephony", *Proc. of the 30th Annual International Cryptology Conference (Crypto 2010),* Santa Barbara, USA: Springer, 2010, pp. 393-410.

[214] Prevelakis, V., and D. Spinellis, "The Athens Affair", *IEEE Spectrum*, July 2007, pp. 18-25.

[215] Ibid.

[216] Ibid.

[217] Diffie and Landau, op. cit., 2008.

[218] Porter, T., *H.323 Mediated Voice over IP: Protocols, Vulnerabilities & Remediation*, 2009.

http://www.symantec.com/connect/articles/h323-mediated-voice-over-ip-protocols-vulnerabilities-amp-remediation

communication, often the "normal" RTP (real-time transport protocol) is used[219]: the data stream encoding the voice is cut in small packets, which are routed over the Internet to the communication partner. There is no fixed circuit for the duration of the call and – as with any Internet data transfer – no guarantee that the packets will be routed over the same path to their destination. This fact, obviously, poses a challenge to wiretapping VoIP calls.

The standard protocol for the set-up, management, and termination of a call is H.323.[220] While the voice signal is not necessarily encrypted, native encryption is possible and foreseen in the standard H.235.6.[221] H.235.6 defines an end-to-end encryption scheme with strong encryption algorithms, and it is thus safe from wiretapping along the line. As in this "interconnected VoIP"[222] model, though, for the initial key exchange the two partners communicate over a central instance, interception can be done with a man-in-the-middle attack at the VoIP provider – this is the mechanism foreseen for lawful interception.

The most popular VoIP software, nonetheless, works differently. Skype uses a proprietary, decentralised protocol. The central instance is needed just for the initial authentication of the communication partners and the subsequent exchange of IP addresses. Both the key exchange for the conversation and the conversation itself are done in a peer-to-peer manner among the communication partners. The key exchange uses RSA public/private key pairs of 1536 or 2048 bits; the actual conversation is encrypted according to the "Advanced Encryption Standard" (AES) with the maximally foreseen key length of 256 bit.[223] As both technologies are considered unbreakable, Skype is impossible to be eavesdropped upon along the line. The only possibility of wiretapping is before the voice signal has been encrypted by the Skype software; that is, on one of the communication partners devices (computers, smartphones).

Call logging

Once the prerogative of powerful organisations, strong encryption of telecommunications is now widely available[224], and easily usable if the communication terminal has the computing capabilities of a smartphone or a computer. Eavesdropping into a communication along the line is thus difficult and expensive, and often outright impossible.[225] Call logging is the cheaper and easier alternative – it records the time and duration of the conversation, as well as the identities of the communicating parties, albeit not the content.[226]

---

[219] Ibid.

[220] ITU-T, *H.323 : Packet-based multimedia communications systems*, 2009. http://www.itu.int/rec/T-REC-H.323/en/

[221] ITU-T, *H.235.6 : H.323 security: Voice encryption profile with native H.235/H.245 key management,* 2009. http://www.itu.int/rec/T-REC-H.235.6/en/

[222] Diffie and Landau, op. cit., 2008.

[223] Skype.com Support, "Does Skype use encryption". https://support.skype.com/en-us/faq/FA31/Does-Skype-use-encryption

[224] Marx, op. cit., 2002.

[225] Danezis, G., and R. Clayton, "Introducing Traffic Analysis", in A. Acquisti, S. Gritzalis, C. Lambrinoudakis and S. di Vimercati (eds.), *Digital Privacy: Theory, Technologies, and Practices,* Auerbach Publications, New York, 2007, pp. 95-116.

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.156.952&rep=rep1&type=pdf

[226] Petersen, J.K., *Understanding Surveillance Technologies: Spy Devices, Privacy, History & Applications* (2nd ed.), Auerbach Publications, Boca Raton, FL, 2007.

Analysing who is communicating with whom, when the content is not accessible, has military roots. British intelligence, for example, after intercepting (but not decoding) German Air Force transmissions in 1941, was able to infer that a unit was composed of nine and not twelve planes as previously assumed, leading to a reassessment of the German Air Force's overall strength.[227] More recently, using such communication patterns has been proposed as a technique for the identification of the key figures within a terrorist group[228], or within criminal organisations[229].

To allow such investigations, but also more benign aims such as statistical analyses, the Directive 2006/24/EC (better known as the "Data Retention Directive") regulates the call logging duties of telecommunication providers within the EU. According to the Directive, all telephony providers but also Internet Service Providers (for the VoIP calls) have to store, and provide upon request to the authorities, for each individual call and for a period of between six months and years, the following data: the calling telephone number (for VoIP calls: user ID) along with the name and address of the subscriber, the called telephone number along with the name and address of the receiving subscriber, as well as the date, time and duration of the conversation. For mobile telephony, additionally, the International Mobile Subscriber Identity (IMSI) of the SIM card is to be stored along with the cell ID from where the call has been effectuated.[230]

Monitoring text-based communication

So far, this subsection has discussed remote, electronically supported, voice communication. With the rapid spreading of Internet usage, though, increasingly daily communication is text-based, such as via instant messaging (IM) or e-mail.[231]

As for voice communication, text-based messages can also be intercepted either in one of the end-user devices (computers or smartphones) or along their path. Interception on one of the communication devices is typically accomplished via so-called "parental control" programs. This type of software, which monitors and reports all activity on a computer, down to individual keystrokes, and includes the content of e-mails and IM chats, has been discussed above, in the "cyber surveillance" section. As of 2011, such "parental control" software became available for smartphones as well, monitoring even more types of data: in addition to the attributes revealed about the activity on computers, the smartphone version also reports the GPS coordinates of the phone and possible pictures taken by its camera.[232]

---

[227] Herman, M., *Intelligence Power in Peace and War*, Cambridge University Press, Cambridge, 1996.

[228] Carley, K. M., J. S. Lee and D. Krackhardt, "Destabilizing Networks", *Connections*, Vol. 24, No. 3, 2001, pp. 79-92.

[229] Klerks, P., "The Network Paradigm Applied to Criminal Organisations: Theoretical nitpicking or a relevant doctrine for investigators? Recent developments in the Netherlands", *Connections*, Vol. 21, No. 3, 2001, pp. 53-65 and Sparrow, M. K., "The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects", *Social Networks*, Vol. 13, No. 3, 1991, pp. 251-274.

[230] European Parliament and the Council, Directive 2006/24/EC of 15.03.2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, Brussels 2006.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:EN:NOT

[231] Hancock, J.T., C. Landrigan and C. Silver, "Expressing Emotion in Text-based Communication", *Proceedings of the SIGCHI conference on Human factors in computing systems (CHI 2007)*, San Jose, USA, 2007, pp. 929-932.

[232] Rubenking, N.J., "eBlaster Mobile for Android", *PC Magazine*, 2011.

http://www.pcmag.com/article2/0,2817,2381450,00.asp

Intercepting text-based communication (or any other form of data exchanged among computers) along the communication path (instead of one of the end-user devices) poses similar challenges to the VoIP interception presented above. So-called "packet sniffers" – programs that intercept the packets passing the network[233] – can be installed either inside the local network or further along the Internet. Their installation requires physical access to the subject's network or the Internet node, respectively. However, a packet sniffer is not useful in revealing a packet's content if strong encryption is used. The easiest form of packet sniffing intercepts the communication to and from public, non-encrypted WiFi access points. Packet sniffing in this case is trivial – the corresponding software is freely available and at anyone's reach.[234]

2.2.5 Sensors

Sensors represent another type of surveillance technology, with a growing market in relation to security, law enforcement and commercial applications. Sensors can range from traditional retail security systems at store entrances and exits or metal detectors to complex, recently developed explosives "sniffing" or behavioural sensors. Although each type of sensor often performs only one specific task, these sensing systems can be combined to consolidate a comprehensive, multi-modal system.

Explosive and drug "sniffers"

There are two main categories of explosive and drug discovery methods: bulk detection and trace detection.[235] Bulk detection involves non-olfactory methods to sense significant quantities of the targeted material. The technologies used for bulk detection of explosives or drugs are the same as the imaging scanners discussed in the section on "imaging scanners", i.e., x-ray backscatter imaging, millimetre wave imaging, and terahertz imaging.[236] Thus, this section focuses on systems for chemical trace analysis, so-called "chemical sniffers" or "electronic noses".[237] These are systems designed to detect and identify residual traces that indicate either the presence of, or someone's recent contact with, certain chemicals, such as drugs or explosives. There are three phases to the chemical trace analysis: i) the sample collection, ii) the sample analysis, and iii) the comparison of results with known standards.[238] "Electronic noses" are deployed in the second analysis step. Methods commonly used in this step include separation and detection technologies, such as mass spectrometry, gas chromatography, chemical luminescence, and ion mobility spectrometry, with the latter being the most commonly used in current equipment.[239] The first chemical trace sampling step is commonly referred to as "sniffing". The most widespread sniffing method is based on a portal

[233] Connolly, K.J., *Law of Internet Security and Privacy,* Aspen Law & Business, New York, 2001, p. 394.

[234] Pogue, D., "How Secure Is Your Wi-Fi Connection?", *The New York Times*, 4 Jan 2007. http://pogue.blogs.nytimes.com/2007/01/04/04pogue-email/

[235] Settles, G. S., "Sniffers: Fluid-Dynamic Sampling for Olfactory Trace Detection in Nature and Homeland Security – The 2004 Freeman Scholar Lecture", *Journal of Fluids Engineering*, Vol. 127, No. 2, 2005, pp. 189-218.

[236] Shea, D. A., and D. Morgan, *Detection of Explosives on Airline Passengers: Recommendation of the 9/11 Commission and Related Issues*. *Science,* Washington, DC, USA: DTIC Document, 2007, pp. 1-6.

[237] Gardner, J. W., and P. N. Bartlett, *Electronic Noses: Principles and Applications*, Oxford University Press, Oxford, 1999.

[238] National Research Council, *Configuration Management and Performance Verification of Explosives-Detection Systems*, National Academy Press, Washington, DC, 1998.

[239] Shea and Morgan, op. cit., 2007.

approach (similar to traditional x-ray scanners or millimetre wave imagers) that accomplishes all steps at once: it collects, analyses and identifies the residues on a person or an object. For the sniffing step, the portals designed for persons might rely on the persons' own body heats to volatilise traces of chemicals from their bodies. Often, however, they use puffs of air to dislocate particles from the person or object under scrutiny. A more precise but also more intrusive sniffing technique deploys a small handheld vacuum 'wand' to collect the chemical sample. A less precise but cheaper and quicker technique is to analyse an object handled by the person under scrutiny, such as the boarding pass at airports.[240]

In the decade after 2000, several US airports had introduced portals for trace detection of explosives. The TSA had planned to acquire 434 such machines. However, only 95 have been installed.[241] Efforts focus now more on bulk detection and on the more generic millimetre wave scanners and backscatter x-ray scanners.

Metal detectors

Metal detectors are electromagnetic devices able to detect the presence of metals in their vicinity. There are two main techniques used by metal detectors: 'very low frequency' (VLF) and 'pulse induction' (PI).[242] Both types create electromagnetic fields, and detect either the presence of a magnetic response field created by conductive objects, or the altering of the decay pattern of the original field due to the presence of metal close-by.[243] Metal detectors come either as portable units or walk-through gates. The portable detectors, usually using the VLF technique, are used by archaeologists and hobby treasure hunters to locate metal in the ground, geologists to detect the metallic composition of soil and rock formations, or by security staff as handheld metal detectors. Walk-through metal detection portals use the pulse induction technique and are typically installed in points of access to zones where an increased level of security is needed. Traditionally, they have been placed in airports delimiting the public from the passenger-only zones, and at the entrance to some governmental buildings. Over the last years, they are increasingly seen at entrances to railway stations, museums, football stadiums, outdoor music festivals, and political rallies. Although relatively uncommon, metal detecting portals have been used at some US schools for over 20 years in an effort to hinder pupils carrying knives or firearms.[244] After a series of knife crimes in early 2008 in the UK, there has been some discussion about introducing metal detectors in some UK schools as well;[245] however, the idea was later abandoned.

Audio sensors

"Sound ranging" describes the techniques used to determine the position of a sound source that can be heard but not seen. Sound ranging originates in World War I, when scientists from various countries started to devise systems for the location of the enemy's artillery positions.

---

[240] Shea and Morgan, op. cit., 2007.

[241] Frank, Thomas, "TSA puts security technology to the test", *USA Today online*, 2 Oct 2007. http://www.usatoday.com/money/industries/travel/2007-10-01-security-tech_N.htm

[242] Tyson, Jeff, "How Metal Detectors Work", *howstuffworks*. http://electronics.howstuffworks.com/gadgets/other-gadgets/metal-detector.htm

[243] Yamazaki, S., H. Nakane and A. Tanaka, "Basic Analysis of a Metal Detector", *IEEE Transactions on Instrumentation and Measurement*, Vol. 51, No. 4, 2002, pp. 810-814.

[244] Morris, Nigel, "Teachers back metal detectors for schools", *The Independent*, 21 Jan 2008. http://www.independent.co.uk/news/education/education-news/teachers-back-metal-detectors-for-schools-771385.html

[245] BBC, "Metal detectors plan for schools", 21 Jan 2008.

http://news.bbc.co.uk/2/hi/uk_news/education/7198633.stm

While the simplest such systems would rely on seeing the flash produced by the shot (thus knowing the direction of the gun; and through the measurement of the time between the flash and the sound also the distance), more sophisticated systems quickly emerged that relied on audio information only.[246] These systems were using the triangulation technique, which determines an unknown position by measuring the distances to a set of points of known location.[247] Thereby, n+1 points of reference are needed to determine an n-dimensional position. To determine a position on a surface, hence, three points of reference are needed, and in order to determine a three-dimensional position, four such points are required. The sound ranging systems of WWI were using four to six (for higher accuracy and redundancy) microphones in known positions, which were all connected through wires to a command point. By measuring the time differences between the arrival of sound to each microphone location (a technique called time-difference-of-arrival, or TDOA, which will be presented in more detail in the next section), the location of the artillery fire could be located by triangulating between the known positions of the microphones.

Military sound ranging has evolved considerably, and today includes acoustic arrays that can directly sense the sound's direction of arrival, more complex arrays that can also sense the shockwave of a bullet while it travels at supersonic speed (and can thus locate the shooter from a single position), and networks of such arrays that can achieve an astonishing precision.[248] Since the mid-1990s, simpler civilian systems have emerged that rely on the original idea of triangulating the sound's time of arrival, combined – as they are meant to work 24/7 in city neighbourhoods – with filters that can distinguish the sound of a firearm from all the other city sounds.[249] These systems aim at the surveillance of neighbourhoods that are considered dangerous. The sensors are small (can-sized) and placed on rooftops or light poles, and are virtually undetectable. They are typically linked directly to a police station, where they raise an instantaneous alarm as soon as a firearm has been fired, pinpointing the location with a precision of a few metres. By mid-2008, such systems were installed in 30 US cities; in Washington DC, one of the early adopters, 16 of the city's 68 square miles were covered.[250] In Europe, Birmingham was the first city to install such a system in late 2010.[251] Connecting such sound ranging systems to surveillance CCTV cameras, if available, and having them almost instantaneously pointing to the direction of the gunshot, would mean more timely information for law enforcement and possibly evidence; corresponding efforts are on their way.

Heat sensors

There are two main types of heat sensors: passive infrared sensors and infrared cameras. Passive infrared sensors are small devices with a pyroelectric sensor (i.e., a sensor that

[246] Bateman, H., "Mathematical Theory of Sound Ranging", *Monthly Weather Review*, Vol. 46, No. 1, 1918, pp. 4-11.

[247] Strictly speaking, 'triangulation' denotes a similar technique, which determines the position by measuring the *angles* between the unknown location and several points of reference (of known location). Using *distances* would thus be called 'trilateration'. The term 'triangulation', however, is commonly used to denote either of the two methods.

[248] Kaplan, L.M., T. Damarla and T. Pham, "QoI for Passive Acoustic Gunfire Localization", *Proc. of the 5th IEEE International Mobile Ad Hoc and Sensor Systems Conference (MASS 2008),* 2008, pp. 754–759.

[249] ShotSpotter, "The ShotSpotter Gunshot Location System". http://www.shotspotter.com/technology

[250] Klein, Allison, "District Adding Gunfire Sensors", *The Washington Post*, 5 July 2008. http://www.washingtonpost.com/wp-dyn/content/article/2008/07/04/AR2008070402356.html

[251] BBC, "How Birmingham's gunshot sensor system pinpoints location", 9 Dec 2010. http://www.bbc.co.uk/news/uk-11954987

creates, through its material characteristics, a small electrical potential when its temperature changes) connected on an integrated circuit board to a small relay. When a temperature changes, the sensor induces a current that closes a second circuit, which then performs a function. The most common usage of passive infrared sensors is to sense human heat in relation to burglar alarms.

Infrared (or thermographic) cameras are more complex devices. Their purpose is to sense the levels of infrared radiation (invisible to the human eye) in their field of sight and to transform them into a visual representation. They typically use either a colour scheme, where low levels of infrared are represented in cold colours and high levels of radiation in increasingly warmer colours, or a black and white representation where low radiation is dark and increasing levels of infrared become gradually lighter.

Infrared cameras are applied in numerous domains, many of which are unrelated to surveillance. Firefighters use them to assess the structure of a fire, find possible victims in darkness or behind smoke, and in the early discovery of low-level combustion. An important industry application is the detection of heat leakages or overheating. Some high-end vehicles are equipped with infrared cameras to provide additional safety at night or poor visibility conditions.[252] Biologists and conservationists use thermal imaging to locate nocturnal animals that need protection, or on the contrary, the invasive species that need to be destroyed. For example, the Queensland authorities used helicopter-mounted thermal cameras to find (and subsequently destroy) nests of red fire ants originating from South America.[253]

Infrared cameras are also increasingly used for law enforcement and surveillance purposes throughout Europe and worldwide. Helicopter-mounted cameras support ground forces in searches for suspects, especially at night. Perimeter security systems increasingly deploy thermal imagers to replace, or complement CCTV, both against border[254] and property trespassing[255]. Police forces use them in special operations, as for example recently in Berlin in the search of arsonists.[256] They have also been used in the UK and Germany to find illegal marijuana plantations. Detecting unusually warm houses or storehouses from helicopters is likely to point to the heat lamps used to grow the plants faster. Finally, precision infrared cameras installed at airports, for example, can show elevated body temperature in passers-by; which might be an indication for certain infections, such as H1N1.

Multimodal behavioural sensing

Aside from infrared cameras used for remotely measuring the body temperature, and the backscatter and millimetre wave scanners, there are further, more subtle efforts to remotely sense the physiology of individuals and draw psychological conclusions from it. Automated "behavioural profiling" by BioEdge, for example, aims at replacing TSA agents who watch for suspicious behaviour among passengers (e.g., nervousness) and single out suspects for

[252] Daimler AG, "Night View Assist: How night becomes day". http://www.daimler.com/dccom/0-5-1210218-1-1210320-1-0-0-1210228-0-0-8-0-0-0-0-0-0-0-0.html

[253] National Geographic, "Fire Ants 'Attacked' From Air", 11 Aug 2009.

http://news.nationalgeographic.com/news/2009/08/090811-australia-fire-ant-video-ap.html

[254] Lee, David, "Using Thermal Cameras to Secure the Homeland", *photonics.com*, Feb 2010.

http://www.photonics.com/Article.aspx?AID=40915

[255] FLIR, "Security Cameras: Thermal Imaging for Security". http://www.flir.com/cvs/eurasia/en/content/?id=5868

[256] Taz.de, "Mit Hubschrauber und Wärmebildkamera", 10 June 2011. http://www.taz.de/!72313/

more detailed screening: "Pre-criminals will be identified through the use of remote cardiovascular and respiratory sensors, a remote eye tracker, thermal cameras, high-resolution video, and an audio monitor for pitch change. Additional sensors, such as pheromone detectors, are being considered. People with aberrant readings are likely to receive "special treatment" on the suspicion of their being suspicious."[257] Similar patents by IBM, e.g., "Detecting Behavioral Deviations By Measuring Eye Movements" and "Unique Cohort Discovery From Multimodal Sensory Devices" envision a large number of sensors (e.g., chemical, biometric, but also CCTV, licence-plate recognisers, retina scanners) deployed in an airport that will be connected to all sorts of background information (age, date of birth, medical diagnosis) and real-time behaviour (item of clothing, walking vs. running, type of food eaten) for providing a centralised, real-time classification of travellers.[258]

2.2.6 Location determination technologies

While a wide variety of location determination systems exists, all of them fall into three main classes of localisation techniques: (1) triangulation, (2) proximity sensing, and (3) scene analysis.[259] These basic approaches will be discussed first, before we describe some of the most prevalent location determination techniques – GPS, WiFi/cell phone, and RFID – in further detail.

One of the earliest location determination technologies was measuring the viewing angle of several known points (e.g., lighthouses, mountain peaks) and determining the intersection of the view lines on a map. This technique is known as "Angle of Arrival" (AOA). Distances to known points can also be measured, which then requires one to find the intersection of several circles on a map. Instead of measuring such distances directly, one typically measures signal propagation times *t* and then calculates the corresponding distance *s* through s=v*t (given one knows the propagation speed *v* of the used signal). This is known as "Time of Arrival" (TOA). Typically used signals are sound (e.g., ultrasound), light (e.g., lasers) and electromagnetic waves. Ultrasound has the advantage of relatively low velocity (approximately 344 m/s through 21°C air), rendering location systems possible that measure short distances (a few meters, which correspond to a travel time of milliseconds) with relatively inexpensive (i.e., imprecise) clocks. Ultrasound is typically used for indoor location systems. Light and electromagnetic waves, on the other hand, have a propagation speed of $\sim 3*10^8$ m/s. In a millisecond of travel time, such signals travel thousands of kilometres. In order to measure a distance with a precision of about one meter, the clocks used for the measurement must be exact up to a nanosecond.

Distance can also be measured through signal attenuation. Signal attenuation systems exploit the fact that the strength of radio signals decreases by the factor $1/r^2$, *r* being the distance from the signal's source. Measuring at some point P the signal's strength *S(P)* leads thus to a theoretical computation of the distance *r* to the signal's source according to the formula: , where *S(O)* is the known strength at the signal's origin. Although such systems have been

[257] McElroy, Wendy, "Commentary – 'Pre-criminal' profiling may be coming soon to an airport near you", *TriValleyCentral.com*, 4 Aug 2011. http://trivalleycentral.com/articles/2011/08/04/florence_reminder_blade_tribune/top_stories/doc4e39b5da387f1946508835.txt

[258] Wolfe, Alexander, "Wolfe's Den: IBM Patenting Airport Security Profiling Technology", *InformationWeek*, 19 Jan 2010. http://www.informationweek.com/news/government/security/222301388

[259] Hightower, J., and G. Borriello, "Location Systems for Ubiquitous Computing", *Computer*, Vol. 34, No. 8, 2001, pp. 57-66.

experimentally built – such as the one presented by Krumm, et al.[260] – signal propagation is not uniform. Issues such as refraction, reflection and absorption lead to imprecise distance measurements[261] and render such systems impractical for most purposes. A more practical use of signal attenuation lies in statistical learning: by combining measurements of multiple signal sources over time, clients can reliably learn a so-called "signal fingerprint" of a location, which can later be used to identify one's position. However, signal propagation issues require the frequent updating of such fingerprints. Signal fingerprinting is used in many contemporary smartphones, where large signal fingerprint databases of publicly visible WiFi access points are used to improve or replace GPS positioning information (see next section). In 2010, Google (accidentally, it said) recorded not only signal strength data, but also actual data packets containing logins and passwords while collecting such WiFi fingerprints in Germany, France, and Spain.[262]

Proximity sensing systems work after a rather distinct principle: they do not aim at pinpointing objects or people in terms of coordinates, but at assessing their closeness to a known location. The location is thus a consequence of the neighbourhood relation with a known spot. In order to do so, proximity sensing systems use physical phenomena with limited ranges – when the corresponding phenomenon takes place, the neighbourhood is assessed. Examples include: the usage of magnetic induction in RFID (Radio Frequency Identification) systems to conclude upon the presence of an RFID tag in the vicinity of the antenna; the connection between a GSM base station and a cellular phone to assess the presence of the phone within the base station's cell; an existing connection between a laptop and a WiFi antenna to assess the laptop's presence within the range of the WiFi antenna; or – through low-power magnetic induction – the detection of an ID badge to assess its presence in the close 'neighbourhood' (typically a few centimetres) of the access control antenna.

Scene analysis and recognition systems also infer the position of an entity from a neighbouring relation; the closeness is assessed via image recognition algorithms (applied to still pictures or a video stream). Vehicle licence plate recognition systems use this method, such as the one deployed as part of the London congestion charging scheme.[263] A recognised plate implies the vicinity of the corresponding vehicle to the checkpoint. The purpose of such systems, however, lies mainly with identification and only marginally with positioning.

While this discussion has so far revolved around the types of technologies that can be used in location systems, one further attribute is of outstanding importance from the perspective of a surveillance analysis: whether the location is computed locally (i.e., by the mobile entity itself) or by the infrastructure. The remainder of this section presents the three most prevalent location systems nowadays and discusses them along these two axes: which are the localisation techniques deployed, and where is the localisation computed.

Global Positioning System

---

[260] Krumm, J., G. Cermak and E. Horvitz, "RightSPOT: A Novel Sense of Location for a Smart Personal Object", in A. K. Dey, A. Schmidt and J. F. McCarthy (eds.), *Proceedings of the 5th International Ubiquitous Computing Conference (UbiComp 2003),* Seattle, USA, 2003, pp. 36-43.

[261] Hightower, J., and G. Borriello, *Location Sensing Techniques*, 2001.

http://portolano.cs.washington.edu/papers/UW-CSE-01-07-01.pdf

[262] O'Brien, Kevin J., "Europe Pushes Google to Turn Over Wi-Fi Data", *The New York Times*, 27 June 2010. http://www.nytimes.com/2010/06/28/technology/28google.html

[263] Transport for London, "Congestion Charging". http://www.tfl.gov.uk/roadusers/congestioncharging/

The Global Positioning System (GPS) is a worldwide satellite-based positioning system using time-of-arrival-based triangulation. The system consists of satellites in semi-synchronous Earth orbit (an orbit at 22.200 km of height, where the satellites orbit the planet exactly twice per day).[264] For the three-dimensional positioning on or close to Earth's surface, the distances to at least four satellites are needed. To ensure free line of sight to at least four satellites at any given moment and at any worldwide position,[265] 24 satellites organised in six orbital planes with four satellites per plane are needed.[266] As of 2011, however, 31 satellites are in use to allow for redundancy and thus increased accuracy.

For the time-of-arrival triangulation, and as they do not have a fixed position relative to the planet's surface, the satellites continuously transmit messages (in frames of 30 seconds) containing the time of transmission and their position relative to the Earth. To ensure a high accuracy, the satellites are equipped with atomic clocks synchronised within 40 nanoseconds (ns).[267] From the time-of-arrival measurement, a GPS receiver infers the distances to the individual satellites and computes then its own position.[268]

The satellites transmit simultaneously on two frequencies, known as L1 (1,575.42 MHz) and L2 (1,227.6 MHz). While the L2 band is encrypted and reserved for military purposes only, L1 is the frequency open for civilian use. Until the year 2000, the L1 signal was artificially degraded – a procedure known as "selective availability" (SA). Since May 2000, SA has been turned off, increasing the typical accuracy of GPS positioning to 15 m. While this accuracy is sufficient for numerous applications, for other (most prominently, for vehicle navigation) it is not satisfactory. Several large-scale efforts have been undertaken to improve the accuracy of GPS – most notably among them is the North American Wide Area Augmentation System (WAAS)[269] – with an accuracy of below 3 m – and the European Geostationary Navigation Overlay Service (EGNOS), which improves the accuracy to below 2 meters. They function according to similar principles. To improve GPS's precision in Europe, for example, the European Space Agency (ESA) installed 40 ground stations across Europe as well as three geostationary satellites.[270] Their positions are known with a high accuracy, and GPS receivers can use their signals to improve the position assessment. The EGNOS complementary system became active on the 1st of October 2009.

The GPS location is computed on the receiver's side only. "Traditional" GPS devices are thus unsuitable for any kind of surveillance. Newly emerging services, however, often require the position to be known outside the device itself. As a result, GPS devices are increasingly equipped with a communication module (GSM, HSDPA or some other mobile telephony standard) via which the device can communicate its position (and, possibly, other attributes). Emergency assistance systems for vehicles are such a novel service. Several manufacturers

---

[264] Garmin, "What is GPS?". http://www8.garmin.com/aboutGPS/

[265] "Any worldwide position" not inside a cave, a tunnel, a building, between tall buildings, etc., that is. GPS requires line of sight between the position to be determined and the satellites.

[266] Kaplan, Elliott D., and Christopher J. Hegarty, *Understanding GPS: Principles and Applications*, Artech House, Boston, 2005.

[267] Ibid.

[268] For a discussion of why the imprecision resulting from the relatively inexpensive clocks built into receivers (as compared to the highly precise clocks of the satellites) do not rip apart the system's overall performance, see section 2.1.1 of Kaplan and Hegarty, op. cit., 2005.

[269] Garmin, "What is WAAS?". http://www8.garmin.com/aboutGPS/waas.html

[270] European Space Agency, "EGNOS 'Open Service' available: a new era for European navigation begins today", 1 Oct 2009. http://www.esa.int/esaNA/SEM2HGF280G_egnos_0.html

offer them, for example, Volvo[271], BMW[272] and GM[273]. The functionality of such systems varies, but it usually includes assistance in case of technical failures, remote blocking in case of car theft, and automatic emergency calls in case of accident (if the airbags were triggered, for example). The European Commission also envisions such an emergency function for all vehicles in Europe.[274] Such systems, once installed, can obviously be used for tracking – the vehicles, in this example, and more generally for tracking the GPS device. GPS localisation is also often combined with GSM- and WiFi-based positioning for improved redundancy, in which case tracking again becomes trivial.

Triangulation for mobile phones and WiFi devices

Locating a mobile phone can rely either on simple proximity sensing (a phone is within a specific grid cell when it communicates with the corresponding cell tower) or via triangulation between several cell towers.[275] With the proximity technique, it is inherently possible for mobile telephony providers to determine the grid cell in which individual mobile phones are situated. Increasing the accuracy with infrastructure-based triangulation is technologically also relatively simple as has been done for a relatively long time. Laitinen, Lähteenmäki and Nordström showed that in urban environments, a 90-percentile accuracy of 90 metres is possible.[276] To improve responses to emergency calls, but also to better locate suspected criminals, regulators have asked mobile telephony operators in the US to be able to locate mobile telephones within 150 metres[277], and the European E112 initiative for emergency calls has similar goals.

In more recent approaches, however, mobile GSM devices are also able to approximate their location locally – either using the (known) ID of the cell they are in, or multiple IDs of the cell towers they can receive, together with the respective signal strengths (implementing thus proximity sensing and triangulation, respectively). As the positions of the cell towers are typically not publicly available[278], local positioning algorithms are more challenging than centralised ones. They thus use signal fingerprinting. As described above, the fingerprinting technique relies upon a training phase in which the radio strengths at different known positions are measured and stored in the system. The training phase can be completed by one entity only[279], or collaboratively.[280] Later position computations use this information to interpolate their most probable position.

---

[271] Volvo, "Volvo On Call – Where happy endings get their start". www.volvocars.com/intl/campaigns/misc/oncall/Pages/Overview.aspx

[272] Euro NCAP, "Reward 2010 – BMW Assist Advanced eCall", 2011. http://www.euroncap.com/rewards/bmw_assist_advanced_ecall.aspx

[273] General Motors, "OnStar". http://www.onstar.com/web/portal/home

[274] European Commission, "eCall: Time saved = lives saved", 14 July 2011. http://ec.europa.eu/information_society/activities/esafety/ecall/index_en.htm

[275] Figueiras, J., and S. Frattasi, *Mobile Positioning and Tracking: From Conventional to Cooperative Techniques*, Wiley, Indianapolis, 2010.

[276] Laitinen, H., J. Lähteenmäki and T. Nordström, "Database Correlation Method for GSM Location", *Proceedings of the 53th IEEE Vehicular Technology Conference,* Rhodes, Greece, 2001, pp. 2504-2508.

[277] LaMarca, A., Y. Chawathe, S. Consolvo, J. Hightower, I. Smith, J. Scott, and T. Sohn, "Place Lab : Device Positioning Using Radio Beacons in the Wild", in H. W. Gellersen, R. Want, & A. Schmidt (eds.), *Proceedings of the 3rd International Conference on Pervasive Computing*, Springer, Munich, 2005, pp. 116-133.

[278] Chen, M.Y., T. Sohn, D. Chmelev, D. Haehnel, J. Hightower, J. Hughes and A. LaMarca, "Practical Metropolitan-Scale Positioning for GSM Phones", in P. Dourish and A. Friday (eds.), *Proceedings of the 5th International Ubiquitous Computing Conference (UbiComp 2003)*, Springer, Orange County, CA, 2006, pp. 225 – 242.

[279] Ibid.

Computing the position on the GSM device itself using the proximity sensing (i.e., one cell) approach can achieve accuracies of several hundred metres for densely populated areas to a few kilometres for sparsely populated regions.[281] Using multiple cells and fingerprinting, the localisation on the mobile phone can achieve a median accuracy of about a hundred metres in urban areas.[282]

Similar techniques can be applied to WiFi signals. WiFi has a lower range than GSM, the maximum ranges being 500 m and 35 km, respectively.[283] WiFi connectivity in rural areas, moreover, is scarcer than GSM, and the WiFi antennas are typically not under the control of a single authority. For these reasons, localisation using WiFi signals is less ubiquitously possible but more precise than GSM-based positioning. Furthermore, due to the heterogeneity of the WiFi base stations, triangulation only makes sense on the mobile WiFi-device itself, not in the infrastructure. The RADAR system showed that 1.5 m indoor accuracy is possible within an office building by constructing a – labour-intensive and not scalable – detailed fingerprint map based on a grid of 30*30 cm. The most comprehensive product based on fingerprinting of WiFi access points, Skyhook, possesses according to the producer's claim a database of over 250 million WiFi access points and is able to deliver in urban centres a position accuracy of 20-30 m.[284]

RFID positioning

As its name already suggests, the main purpose of the Radio Frequency Identification (RFID) technique is the identification of objects. The electronic labels, each with a unique ID, can be used to tag, products, entrance and transportation tickets, animals or other objects. They can also be used to uniquely identify a name badge, a passport or a vehicle ignition key, with the aim of authenticating the rightful owners and provide them access to a building, a country, or a car's controls.
Implicitly, however, RFID systems also provide location information through the proximity sensing paradigm. When a tag comes in the neighbourhood of a so-called 'reader', it not only identifies the object it tags, it also implicitly provides the information that the corresponding object (or person) is in the reader's neighbourhood.[285] Often, this information is very precise. RFIDs come in numerous flavours and are mainly divided into active and passive systems. In active systems, the tags have an own battery and can send their identification up to a few hundred metres. In the much smaller, cheaper, and more commonly used passive systems, though, the tags do not possess their own power source and can only "answer" the reader's requests by modifying an electrical or magnetic field. The reading range of passive RFID tags is thus of a few metres maximum, and often much smaller, of just a few centimetres.[286] The

[280] Nurmi, P., S. Bhattacharya and J. Kukkonen, " A Grid-Based Algorithm for On-Device GSM Positioning", in J. E. Bardram, M. Langheinrich, K. N. Truong and P. Nixon (eds.), *Proceedngs of the 12th International Ubiquitous Computing Conference (UbiComp '10),* 2010, pp. 227-236.

[281] Trevisani, E., and A. Vitaletti, "Cell-ID Location Technique, Limits and Benefits: An Experimental Study", *Proceedings of the 6th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 2004),* Lake District, UK, 2004, pp. 51-60.

[282] Chen et al., op. cit., 2006.

[283] Ibid.

[284] Skyhook, "How it Works". http://www.skyhookwireless.com/howitworks/

[285] Figueiras and. Frattasi, op. cit., 2010.

[286] Finkenzeller, K., *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication* (3rd ed.), Wiley, Indianapolis, 2010.

location information they provide are thus relatively precise, albeit also ephemeral, as the tag usually leaves the reader's range quickly.

Aside of the implicit location information any RFID system (such as electronic toll collection or RFID-enhanced passport readers) provides, RFIDs can be used to tag *locations* instead of physical objects and thus be explicitly used for positioning. For example, RFID tags can be built into floors and mobile robots with a reader can navigate by reading the tags and inferring thus the position.[287] Unlike the implicit location of persons (or of objects that can be assigned to persons) referred to above, however, this explicit usage of RFID tags for the guidance of autonomous robots does not seem to offer relevant surveillance potential.

2.2.7 Summary

This section provides a base line for understanding how different surveillance technologies work, what their applications may be and what types of people may be targeted by them. Yet, the presentation of these technologies as individual does not provide an accurate picture of how surveillance technologies are deployed in relation to security and crime control. Rather than functioning as discrete "solutions", different surveillance technologies may overlap to achieve particular functions. For example, both biometrics and visual surveillance images can be used to identify an individual. The following section demonstrates that different families of surveillance technologies can perform particular, similar functions, albeit in different ways and with different levels of comfort for those who experience them.

2.3 FUNCTIONS

While describing surveillance systems using technology families certainly provides one way of categorising such systems, there are a number of other ways to taxonomise surveillance systems. One of these is to group surveillance systems according to the function they perform or are intended to perform. This method of categorisation demonstrates that a number of different types of technologies can perform these specific functions. In this section we examine six different functions of surveillance technologies: the use of surveillance to identify, verify/authenticate, detect/monitor, locate/track, collect information and link information. For each function we examine the level of intrusiveness for the individual being surveilled, the comfort for the person operating the system and speed in which the system returns results in relation to each of the technologies discussed.

2.3.1 Identify

Surveillance technologies are often used for the purpose of identification, meaning that the features collected by the surveillance technology will be compared with all the records in an associated database to see if there is a match. Identification almost always relies upon the presence of a database to perform one-to-many matching, especially if this one-to-many matching is digitised and speed is a priority. Biometric technologies such as DNA matching, fingerprints, iris scanning, facial recognition and other soft biometrics are used primarily as identification (and/or verification) technologies. In addition, other technologies such as RFID and CCTV can also be used to identify individuals.

---

[287] Hähnel, D., W. Burgard, D. Fox, K. Fishkin and M. Philipose, "Mapping and Localization with RFID Technology", *Proceedings of the IEEE International Conference on Robotics and Automation (ICRA '04)*, New Orleans, USA, 2004, pp. 1015-1020.

DNA identification is intrusive for the individual being surveilled as it requires them to give a biological sample in the form of blood or saliva. As discussed in the previous section, DNA samples can be obtained by reasonable force in some contexts, and this increases the discomfort and intrusiveness associated with this type of identification. DNA matching is also uncomfortable for the operators, such as police officers, who must take the DNA sample from the individual, particularly if this sampling is non-consensual. However, for those working in the lab, the surveillance is distantiated and thus reasonably comfortable. DNA identification is relatively slow as samples must be sent to centralised laboratories and relies upon a number of laboratory techniques, as well as the searching of large databases. Court cases surrounding the storage of DNA records on national criminal justice DNA databases illustrate the relative discomfort individuals experience in relation to this technology of surveillance.

Fingerprint surveillance is significantly less intrusive than DNA surveillance as it does not require a biological sample. However, fingerprints are associated with the criminal justice system and the taking and storage of fingerprints in non-criminal justice contexts is often uncomfortable for those whose biometric sample is being taken. For example, travellers to the US who were confronted with the US immigration fingerprinting scheme have described it as making them feel like a "criminal".[288] Fingerprint surveillance is relatively comfortable for the operators and relatively quick in returning potential matches.

The relative intrusiveness of iris scanning has been debated as many individuals appear willing to submit this biometric particularly in order to bypass immigration queues at airports, while others have described discomfort with the process as well as the greater social meanings associated with the eyes.[289] Yet, iris scanning is very comfortable for operators, as often times, iris scanning can be done automatically without the need for human intervention. As evidenced by its use for border control, iris scanning is also fairly quick and identification of an individual from database data takes no more than a few seconds.

Facial recognition systems are fairly unintrusive for the individual being surveilled primarily because they rely upon photography or CCTV, both technologies with which people are familiar. The error rates associated with facial recognition technology may, however, make false positives or false negatives uncomfortable for individuals. Yet, this technology is comfortable for operators as they do not necessarily have to come into contact with the individuals whom they are attempting to identify. Facial recognition technology can return results quite quickly.

Soft biometrics such as voice recognition, gait recognition and behavioural pattern recognition are less intrusive than other biometrics. Specifically, both gait recognition and behavioural pattern recognition use visual surveillance such as CCTV systems that are deployed at a distance, while voice recognition requires the co-operation of the individual being surveilled. However, as discussed above, Wei and Li note that individuals are sometimes sensitive about having their speech recorded in voice recognition systems. Furthermore, the reliance upon distantiated surveillance for gait and behavioural pattern recognition means that the operation of these technologies is fairly comfortable for operators, who do not come into contact with the person or persons being surveilled. The time these biometrics take to identify an individual vary depending upon the soft biometric used. Gait

[288] Finn, Rachel L., and Michael McCahill, "'Good' and 'Bad' Data Subjects: Media Representations of the 'Surveilled' in Three UK Newspapers", in Stéphane Leman-Langlois (ed.), *Technocrime2*, Routledge, London, 2012 [forthcoming].

[289] Ings, Simon, "The soul stealers: Our beautiful, unique irises are to be relegated to the dystopian realm of state security", *The Guardian*, 19 Jan 2008, p. 38.

recognition is still in development and so this form of identification takes some time, whereas voice recognition systems may take less relative time to search associated databases.

The intrusiveness of CCTV surveillance depends largely upon the context in which it is used. Most people feel that CCTV surveillance, as used to identify individuals, is dependent upon the activities that the surveillance technology records and how the information is used. In a UK case, a man whose suicide attempt was captured on CCTV and then released to the media successfully argued to the European Court of Human Rights that the release of the images and the ability to identify him within those images seriously breached his right to privacy.[290] However, CCTV identification is fairly comfortable for operators as they do not come into contact with the individual being identified. The time it takes to identify an individual from CCTV footage can vary depending on the identification method used.

RFID identification is quick and reliable, and it eliminates the need for human operators altogether. It does, however, identify an electronic tag, and not directly its holder. While for some applications the risks posed by the RFID tag being given, lost or robbed are acceptable, for other applications such systems can either not be used at all, or only alongside further identification methods such as biometrics or CCTV.

2.3.2 Verify, authenticate and authorise

While identification involves one-to-many matching, verification, authentication and authorisation involve the database system retrieving the features of a single person and performing a one-to-one comparison. A number of different types of surveillance technologies can be used to perform such verification, but again, like identification, it is primarily biometrics that performs these functions.

Biometrics such as fingerprints, iris recognition, voice verification and facial recognition all perform verification in a fairly quick and relatively comfortable manner. This is partly related to the differences between identification and verification, whereby verification implies that the individual has already consented to or co-operated with the use of this surveillance technology and has actively enrolled in the system, for example, in relation to access control. Furthermore, verification databases are often smaller than identification databases and fewer records need to be sifted through. These surveillance technologies may also work in conjunction with other technologies. RFID enabled e-passports provide an example of such interconnection, where the RFID chip in the passport stores the biometric information associated with the legitimate holder and the immigration officer need only match the individual with the document without a database search. Despite this, some stakeholders have expressed discomfort with biometric information being taken and stored by the state, workplaces or other entities, particularly in relation to function creep and information security.

In contrast, DNA surveillance and soft biometrics such as gait recognition remain relatively slow, even for verification, because they rely upon a laboratory or other investigative techniques to generate data and match the individual with that data.

[290] *Peck v. United Kingdom*, 36 E.H.R.R. 41, 2003.

2.3.3 Detect/monitor

Another function of surveillance is to detect unauthorised behaviours or to monitor spaces, persons or groups for signs of unauthorised behaviour. While this surveillance, particularly in public or semi-public spaces, is thought to be more comfortable than identification technologies such as DNA testing, this also depends upon the circumstances or context in which the surveillance is taking place.

The installation and justification for CCTV is often centred on the prevention and detection of crime, therefore, detection and/or monitoring are central functions associated with this technology. CCTV surveillance is usually operated at a distance from those being monitored, and as such, offers relative comfort for those being monitored and for CCTV operators. A large majority of people in many different countries support the use of CCTV surveillance for this function in public space, and state that it makes them feel safer.[291] However, in non-public spaces, CCTV surveillance may be somewhat covert in the sense that the person being surveilled may not realise that they are being watched. CCTV is a relatively quick form of monitoring and detection as fully functional pan, tilt, zoom cameras can be easily manipulated to ensure that operators can follow/monitor someone or something. However, the camera must be pointing the right way and be capable of viewing an event or person. Furthermore, despite the general public's relative comfort with CCTV, the monitoring of some spaces such as toilets, certain shops or entertainment spaces, private residences and other locations are thought to be too sensitive to actively monitor.

An individual's comfort with their experience of photography, like other visual surveillance devices, depends on the activity that is being photographed, and whether this surveillance was overt or covert. Covert photography might cause an individual discomfort if they did not know they were visible to others, or if they did not wish the information generated to be shared with others. For example, many celebrities and politicians have expressed concerns about the use of photography in synoptic surveillance practices to reveal activities that they wished to remain private or to "place" them in certain locations. However, photography is quick and comfortable for the person utilising the technology and in non-covert circumstances, people may experience photography as quite comfortable and non-intrusive as it is a technology with which many people are familiar.

If fitted with CCTV, photography equipment, infrared cameras, thermal imaging cameras or other visual surveillance devices, unmanned aircraft systems can be used to monitor individuals or locations or detect unauthorised activity. UASs are often comfortable for the operator to utilise and are responsive and easily manipulated. However, the comfort/intrusiveness of experiencing UAS surveillance is unknown. UAS surveillance can be covert as high altitude aircraft are almost invisible to the naked eye and can be almost silent.[292] Therefore, individuals may be uncomfortable upon discovery that they were under surveillance.

For the detection of illegal trespassing of borders or private property, CCTV cameras are increasingly replaced or complemented with infrared cameras. While the costs for infrared cameras are higher, these provide accurate images both during daylight and at night,

[291] McCahill, Michael, *The Surveillance Web: The Rise of Visual Surveillance in an English City*, Willan, Devon, 2002.

[292] Lewis, Paul, "CCTV in the sky: police plan to use military-style spy drones", *The Guardian*, 23 Jan 2010. http://www.guardian.co.uk/uk/2010/jan/23/cctv-sky-police-plan-drones and OPARUS, "Concept and Approach", 2010. http://www.oparus.eu/index.php/concept-a-approach

significantly increasing the security of the perimeter and/or reducing the need for patrolling personnel at night. Like visual cameras, infrared cameras provide their information instantaneously, and are comfortable for the operator.

There are a range of different types of imaging scanners, and different types of scanners have different relative comfort of operation or experience, as well as different levels of intrusiveness. Imaging scanners which focus on the body, such as airport body scanners, can be intrusive and they have been referred to as a "virtual strip search" by some stakeholders.[293] Yet this intrusiveness can be mitigated by imaging software which uses a generic human figure or a CCTV image of the person, as is used in Amsterdam's Schiphol airport.[294] Furthermore, while some regard body imaging scanners as intrusive, others argue that they are less intrusive than targeted pat downs by security officials.[295] Other types of imaging scanners, such as thermal imaging which can see into homes and through walls, can also be experienced as intrusive, as it is usually covert and individuals do not know they are being monitored. Imaging scanners are often comfortable for the person operating the system, and they are quick in returning data.

Metal detectors are relatively unintrusive and a technology with which both operators and targets are familiar. They are quick and comfortable for both users and operators as they focus on the body but do not involve touching the person or their possessions.

Most types of sensors are fairly intrusive in the sense that it is the body or possessions that are being monitored or tested for explosives or other prohibited items or substances. Individuals may experience discomfort while they or their possessions are being monitored or tested. However, if the monitoring is covert, as is the case for some explosive sensing devices, they may not be aware of it. Audio sensors have proved to be a particularly uncomfortable technology, as many areas have refused the installation of CCTV systems with audio sensors due to fears around privacy and people's conversations being monitored.[296] However, sensors that simply identify sounds, such as gunshots, may not be viewed as intrusive. Most sensors are fairly quick to return results, and are comfortable to operate.

While surveillance associated with house arrest, such as the use of an electronic monitoring device, is understood to be less intrusive and more comfortable than prison, it does represent an intrusion on an individual's lifestyle. The controversy surrounding the use of control orders for terrorism suspects in the UK illustrates the level of discomfort and intrusion that these individuals experience as a result of this technology.[297] The technology is, however, relatively comfortable for the operator of the system as the monitoring is remote. The speed of

---

[293] *EDRi-gram*, "The European Parliament says no to airport body scanners", No. 6.21, 5 Nov 2008.

[294] Schiphol Airport Security, *Security Scan Brochure*.

http://www.schiphol.nl/Travellers/AtSchiphol/CheckinControl/SecurityChecksUponDeparture/SecurityScan.htm

[295] See BBC News, "'Naked' scanner in airport trial", 13 Oct 2009. http://news.bbc.co.uk/1/hi/uk/8303983.stm and Etzioni, Amitai, "Private Security: In defense of the 'virtual strip-search'", *The New Republic*, 9 Oct 2010. http://www.tnr.com/article/politics/78250/private-security-virtual-strip-search

[296] Hamill, Jasper, "Privacy fears over the device that can eavesdrop on crime", *Herald Scotland*, 21 June 2010.

[297] Control orders are court orders limiting the freedom of those suspected of terrorism related offences, where the government does not have enough evidence to prosecute the suspect. Control orders often limit the subject's use of the telephone, the number of hours they may leave the house (if at all), whom they may communicate with, who may visit the home and where they may go when they leave their home. Liberty, "The human cost of control orders", 10 Aug 2010. http://www.liberty-human-rights.org.uk/news/2010/the-human-cost-of-control-orders.php

identification of breach of house arrest is very quick, as the notification is via a computer and is transmitted via telephone line.

The intrusiveness of data mining technologies or applications depends upon who is collecting the data and what types of data they are collecting. Many consumers feel discomfort when they discover that companies and other entities know more information about them than they expected.[298] However, other data mining applications, such as the use of data mining for national security, are often covert and individuals do not know it is occurring. Data mining often takes a significant amount of time. It is comfortable for the operator.
Like photography, the use of databases as a monitoring technology is familiar to most individuals. Database construction and storage is also comfortable for operators. However, like data mining, some individuals who are subject to this form of surveillance may feel discomfort when discovering how much information is held about them. Furthermore, individuals may experience discomfort if the data is not adequately protected and information about them becomes known to unauthorised persons. Database applications offer a quick and simple way to access information about individuals.

The use of wiretapping to monitor individuals or detect unauthorised behaviour is relatively comfortable for operators. However, it can be uncomfortable and intrusive for targets as their speech is being recorded and personal information may be transmitted that they did not wish to share. Specifically, wiretapping has been described as a particularly "insidious" search.[299] Although obtaining the wiretapping signal is straightforward, many wiretapping uses require a warrant or the permission of a senior officer and this can take time to obtain. Therefore, it is not an especially quick surveillance system to set up, but once installed, it does return results quickly.

The monitoring of email communications can also be relatively quick and comfortable for operators. Yet, like wiretapping it can be uncomfortable and intrusive for those whose communications are being monitored.[300] As discussed above, many spyware applications can be installed on a computer unknown to the individual concerned.

2.3.4 Locate/track

A fourth function of surveillance technologies is the use of surveillance technologies to locate or track the movements of a person or object. A number of different surveillance technologies can be used to locate or track including satellite surveillance, mobile phone tracking, RFID and unmanned aircraft systems.

Satellite surveillance is one technology that is often used to locate and/or track persons or objects. Examples include the location and/or tracking of vehicles, offenders, children, older people, etc. This surveillance is comfortable for operators. However, depending upon whether the surveillance is overt or covert or whether it is constant or only triggers an alarm when certain parameters are breached will have an effect on whether it is comfortable or intrusive for those being located or tracked. The intrusiveness will also depend upon whether the individual has agreed to the tracking or whether it is mandatory (for example, offenders

[298] O'Harrow, Robert, *No Place to Hide*, Free Press, New York, 2006.

[299] Diffie, Whitfield, and Susan Landau, "Communications Surveillance: Privacy and Security at Risk", *Communications of the ACM*, Vol. 52, No. 11, Nov 2009, p. 44.

[300] McCahill, Michael, and Rachel L. Finn, "The Surveillance of Political Activists: Subjective Impacts and Behavioural Responses", *Surveillance Studies Network Conference*, City University London, 13-15 April 2010.

and/or the tracking of vehicles used by employees for work). Such monitoring is relatively quick, particularly when the item or person being surveilled is in an area which is visible via satellite. However, geographic features and urban features such as skyscrapers can make this type of surveillance difficult.

Mobile phone tracking is comfortable for operators, and again depending upon the reason an individual is being tracked can be more or less comfortable or intrusive for individuals. Much mobile phone tracking is in response to a triggered alarm, such as an emergency services phone call, or to locate persons of interest.

RFID technologies or applications can also be used to locate or track individuals or items. Two specific examples include biometric RFID enabled passports and RFID enabled travel cards. Both are fairly comfortable for operators. However, the comfort and intrusiveness of these applications for individuals depends upon the context and how the data are used. These applications can be used to track an individual's international travel, or they can be used to track an individual's movement through a transport system. This can have unintended or intrusive consequences, as for example, travel card data is often used to retrospectively track and individual's movements in police investigations[301] and in one case an travel card data thought to be associated with an individual's movements was downloaded and then used against him in divorce proceedings[302].

Individual or vehicle movements can also be tracked in real time via UAS surveillance. This is a comfortable, fairly quick and responsive method of surveillance for operators to use. UAS surveillance can also be overt or covert, and this can be intrusive for individuals who have no way of knowing if they are being monitored or who find out later that their movements were being tracked.

2.3.5 Collect information

Information collection and aggregation is thought to help to predict consumer, criminal or terrorist behaviour. Most dataveillance technologies and applications collect and process information, including data mining, data matching and data aggregation technologies. Data collection also occurs through communication surveillance such as call logging, email monitoring and internet intercepts.

In relation to data mining and data matching technologies and applications, these can be experienced as intrusive and uncomfortable for individuals being monitored. One indication of this intrusiveness is the withdrawal of the Total Information Awareness Act by the US Congress once citizens and lawmakers understood and objected to how information would be collected and how it could be used.[303] However, in relation to detecting credit card fraud, data mining has proved a success story that is largely supported by consumers.[304] Therefore, like other surveillance technologies, the context of the application influences how comfortable

[301] Octopus Holdings Limited, "Customer Data Protection", 2009 and "Oyster data use rises in crime clampdown", *The Guardian*, 13 Mar 2006.

[302] Bloomfield, Steve, "How an Oyster Card can Ruin your Marriage", *The Independent on Sunday*, 19 Feb 2006. http://www.independent.co.uk/news/uk/home-news/how-an-oyster-card-could-ruin-your-marriage-467077.html

[303] Garfinkel, Simson, and Michael D. Smith, "Data Surveillance", *IEEE Security & Privacy*, Nov/Dec 2006.

[304] Schneier, Bruce, "Why Data Mining Won't Stop Terror", *Wired News*, 9 March 2005. http://www.schneier.com/essay-108.html

individuals are in their experience. Data mining and data matching are comfortable for operators to utilise, and are often automated processes.

Information collection via communications surveillance, such as call logging, can provide information about which persons are linked with one another through the presence or absence of communication between them.[305] This is comfortable for the operator, and relatively comfortable and non-intrusive for the person being monitored as it does not record the content of the communication. This information is also available fairly quickly, although some law enforcement uses require a warrant or special permission from a senior officer, which could take time to obtain.

Information collection can also occur through internet intercepts, such as the collection of Wi-Fi information by Google during its information collection for Google Street View. Internet intercepts can occur when information is gleaned from unencrypted wireless communications. This can be quite intrusive as email communications, personal data and financial data can all be intercepted, which can have significant consequences for individuals. In response, German and Spanish authorities have sued Google over their information collection practices during their collection of data for Street View.[306] This information is relatively straightforward for operators to collect and the data can be obtained in real-time.

2.3.6 Link information (profiling)

Surveillance technologies can also be used to link information together, particularly in relation to database or other information. As such, a range of dataveillance functions and applications can be used to link data together. Hildebrant states that "we cannot reflect upon the way that profiling impacts our actions because we have no access to the way they are produced and used. This last difference suggests that profiling hampers our freedom to act autonomously".[307] However, others have also argued that profiling offers improved products and services, as well as focuses authorities' attention of threats more accurately than other investigative methods. Specifically, data mining is thought to be able to predict certain types of terrorist, criminal or consumer activities.[308]

One of the primary functions of data mining or data matching is to link information together and create criminal, terrorist or customer profiles. Amazon's "customers who bought this item also bought", is an example of such customer profiling, as is the exchange of passenger name records on international flights. However, this matching can be uncomfortable for individuals who have experienced a false positive match with particular profiles.[309] Because it operates remotely, data mining or matching is comfortable for operators.

As discussed above, the linking of call logging information, such as telephone or mobile conversations and text or other types of messages can help law enforcement or other actors to better understand who is linked with whom, as well as try and understand the structure of an

[305] Diffie and Landau, op. cit., 2009.

[306] Minder, Raphael, "Google Sued in Spain Over Data Collecting", *The New York Times*, 17 Aug 2010. http://www.nytimes.com/2010/08/18/technology/18google.html?_r=1&ref=technology

[307] Hildebrandt, Mireille, "Profiling and the rule of law", *Identity in Information Society,* Vol. 1, 2008, p. 4 http://ssrn.com/abstract=1332076

[308] Seifert, Jeffrey W., *Data Mining: An Overview*, Congressional Research Service, 16 Dec 2004.

[309] Schneier, op. cit., 2005.

organisation. This is thought to be relatively more comfortable than wiretapping as people's conversations are not recorded, nor are the contents of messages revealed.

Like data mining, data aggregation can be uncomfortable for those who experience it; particularly in areas where getting it "wrong" can have significant effects for an individual. Such negative effects can include a poor credit scoring which could affect someone financially for a number of years, or being included on a no-fly list, which could hamper someone's movement and travel. According to Privacy Activism, some of this data may also be used for employee background checks, and the significant errors in personal data reported in this document suggest that this could have negative impacts on people's ability to find a job, etc.[310]

2.3.7 Summary

This section demonstrates the range of different technologies that can be used to perform particular functions. Yet, it also illustrates that some technologies are more comfortable for operators and individuals being surveilled than others. Furthermore, some technologies are perceived as intrusive in some contexts and relatively unintrusive in others. For example, the use of data mining to detect credit card fraud has been supported by individuals, however, there was an outcry over the proposed use of data mining techniques to monitor citizens' behaviour and build terrorist profiles. Often, the technology and context deployed depends upon the stakeholders involved in the deployment of these technologies and their relative positions, as well as the drivers associated with these deployments. The next section examines these issues.

2.4 STAKEHOLDERS AND DRIVERS

Given the range of surveillance technologies available in contemporary society, this section examines the stakeholders who are involved in developing, implementing and operating surveillance systems, as well as the technological, economic, political and social drivers associated with this implementation. Within these discussions we touch upon many of the key debates surrounding the implementation of surveillance systems, and how these have differed in different contexts and applications.

2.4.1 Surveillants, surveilled and other stakeholders

We can identify no less than seven main stakeholders in a surveillance society: authorities, industry, academia, policy makers, NGOs, the media, and citizens. We will briefly discuss their roles and interests in turn.

Governments and public authorities

Governments and other public authority stakeholders are intimately involved in the introduction of surveillance systems. Governments wish to protect citizens and the state from illegal immigration, terrorism and crime, and as such they must often pass laws introducing or enabling new surveillance systems. Governments or related authorities may also procure surveillance systems, as is the case with systems for immigration, policing, border control and

[310] Pierce, Deborah, and Linda Ackerman, *Data Aggregators: A Study of Data Quality and Responsiveness*, Privacy Activism, 19 May 2005.

traffic management. DNA databases and national biometric databases, particularly those related to criminal justice are often run by local, state or national authorities. In the USA, CODIS (the combined DNA index system) and AFIS (the automated fingerprint identification system) are both run by the FBI but link with local, state databases. In the UK, the national DNA database is run by the Forensic Science Service, a publicly run organisation. In relation to immigration, the Eurodac database, which holds fingerprints of asylum seekers, is run by the European Union, as is the Visa Information System, which holds personal details, facial images and fingerprints of visa applicants to the EU. Government authorities may indirectly operate surveillance systems as well, for example, the Transportation Security Administration in the USA operates airport body scanners, while the Highways Agency operates automatic number plate recognition systems in the UK.

Public authorities also participate in the introduction of surveillance technologies via the judicial system. The judicial system provides a way for those who question the legality of surveillance systems, including citizens, civil society organisations or other stakeholders, to challenge the government. For example, the UK court recently ruled that the UK police had acted illegally in storing the photograph of a protester who was not suspected of any wrongdoing.[311] Similarly, Liberty, a UK civil society organisation successfully applied to the European Court of Human Rights to force the UK government to delete the DNA samples and fingerprints of two individuals who were arrested but never convicted of a crime.[312] Finally, individuals who are employed by public authorities may also find that they are subjects of synoptic surveillance by the media or individuals either in relation to criminal justice or for entertainment.

Industry representatives

Industry representatives make up a large proportion of the stakeholders involved in the introduction of surveillance technology. Often these industry representatives may come from a range of different links in the surveillance chain. They may be developers of technology such as defence contractors, they may be manufacturers, suppliers or sales people for the technologies, they may implement and operate the technologies, or they may be industry associations or other organisations who lobby for surveillance technology-friendly policies at the local, national or regional level. The number of surveillance industry stakeholders are too numerous and diverse to detail here; however, major companies such as Boeing and BAE systems are involved in the production of surveillance systems, as are small, local enterprises. Industry associations include the International Biometric Industry Association which exists to promote the use of biometrics by the government, private sectors and consumers[313] or Unmanned Vehicle Systems International, the Unmanned Aerial Vehicle Systems Association and the German Aerospace Industries Association, which represent the UAS industry in its interfaces with government[314] and provide "political support" for the integration of UASs into civil applications.[315] Another organisation, the Canadian Advanced Technology Alliance (CATA) adopts a public education strategy to compel industry and government to recognise the value of technology in securing environments, places and personal information.[316] However, organisations such as Statewatch accuse industry of playing in a "politics of fear",

[311] Taylor and Lewis, op. cit., 2009.

[312] *S. & Marper* v. *United Kingdom*, ECtHR Nos. 30562/04 and 30566/04, 2008.

[313] Lyon, op. cit., 2008.

[314] Unmanned Aerial Vehicle Systems Association, "About us", 2011. http://www.uavs.org/

[315] Eick, op. cit., 2009.

[316] Zureik and Hindle, op. cit., 2008.

where the close interactions between governments, industry and industry organisations, such as CATA, are focused on selling new technologies to governments, and subsequently the public, based on inflated threats.[317]

Academics

Academics are involved in the introduction of and debates around surveillance technology, as evidenced by the sheer numbers of books, articles in peer reviewed journals and research reports dedicated to the introduction of "new technologies" of surveillance. Academics are involved in a range of different activities in relation to surveillance technologies, including developing new technologies or methods, exploring applications for those technologies, developing standards and interoperability, exploring the social implications of new technologies and encouraging the take-up of new technologies. For example, the Netherlands Biometric Forum is run by academics, as is the Surveillance Studies Network, which describes itself as an international clearing house for the study of surveillance in all its forms.[318]

Policy-makers

At the European level, one of the key policy-making organisations is the Article 29 Data Protection Working Party (Article 29 WP). The remit of the Article 29 WP is to provide expert advice to policy-makers in relation to data protection in Europe. The Article 29 WP has commented on the introduction of RFID technology, body scanners, electronic health records, passenger name records, video surveillance, smart phones, online social networking and electronic communications, as well as many other issues. Their role is to provide information on how personal data can best be protected given the range of security issues with which Europe is confronted. Also in Europe, the European Data Protection Supervisor is an independent supervisory authority who monitors the processing of personal data in Europe and offers expert advice on policy and legislation that could affect privacy. Each European Member State also has a national data protection authority who comments on the privacy implications of proposed or existing legislation and monitors the processing of personal data in that state. Canada and Australia both have a Privacy Commissioner. In various countries, departments of defence or law enforcement also influence law and policy in relation to surveillance technologies, as do legislative committees.

Civil society organisations

According to Lyon, civil society organisations such as civil libertarians, human rights groups, privacy advocates and academic networks are the primary way in which details about how surveillance technologies may influence individual privacy are disseminated.[319] A range of civil rights organisations have generated information and undertaken legal action against governments, public authorities or other entities who implement surveillance technologies in ways which infringe upon privacy and other human rights. For example, Liberty brought a case about the UK DNA database to the European Court of Human Rights and the Electronic Privacy Information Centre (EPIC) challenged the use of body scanners in US courts. Other

[317] Statewatch, *Detection Technologies and Democracy*, Sept 2006. http://www.statewatch.org/analyses/no-56-democracy-and-technology.pdf

[318] Surveillance Studies Network, "The Surveillance Studies Network", 2011. http://www.surveillance-studies.net/

[319] Lyon, op. cit., 2009.

examples of privacy and civil rights organisations active in providing commentary around the use of surveillance technology include Privacy International, the American Civil Liberties Union, Bits of Freedom in the Netherlands, the "Chaos Computer Club" in Germany, Statewatch, European Digital Rights (EDRi-gram) and the Electronic Frontier Foundation (EFF). Other civil society organisations, such as unions for workers who are charged with operating or testing surveillance technologies, have also taken stances some technologies. For example, the national police union in Germany (GdP) has declared itself against the use of body scanners[320] and the airport workers union in the UK successfully battled to prevent airport workers from becoming the first group to be issued with mandatory biometric identity cards.[321]

The media

The media are a key set of stakeholders who are involved in a range of activities across the surveillance spectrum. The media often distribute information and set the public agenda, particularly around the implementation of surveillance systems. They reproduce calls by government, industry and policy makers to implement surveillance systems, often in response to particular incidents. However, the media also give voice to the potential negative privacy impacts of surveillance systems, and particular journalists may undertake a range of different stories outlining the arguments around the introduction of specific surveillance systems, or surveillance systems in particular contexts. Journalists may also critique surveillance technologies or systems themselves via blogs or other new media content, and particular publications, for example, *EDRi-gram*, may function as watchdogs in the implementation of surveillance systems. Finally, journalists are often involved in implementing or operating surveillance technologies themselves, including visual surveillance and communications surveillance technologies in order to investigate or supplement a news story.

Citizens and other groups of people (including targets of surveillance)

Citizens, individuals and other groups of people are generally involved in surveillance through being targets of surveillance technologies. While surveillance systems are generally intended to target offenders, terrorists, illegal immigrants or other socially "undesirable" individuals, all different types of individuals may be surveilled in attempting to identify these intended targets of surveillance. Particular types of surveillance, such as numerous dataveillance systems, cyber surveillance deployed by Internet service providers, or ubiquitous CCTV surveillance, are designed from the outset to target large parts of the society. Lyon notes that "insufficient attention" has been paid to "how ordinary citizens may be included or excluded" from full participation in debates around surveillance.[322] He argues that this may be because of a lack of knowledge necessary for full, informed consent, the mandatory nature of many surveillance schemes (or the inability to exclude oneself from them) or because of a lack of information around interoperability or the potential for function creep. Furthermore, surveillance systems are often directed at populations who are already marginalised or disadvantaged. Many surveillance systems are used for law enforcement, to monitor social assistance and to secure borders, thus implicating the poor, people of colour and those known to the criminal justice system, which can have social sorting effects on those

[320] UPI, op. cit., 2009.

[321] Millward, David, "Airlines anger over ID cards", *The Telegraph*, 2 July 2008.
http://www.telegraph.co.uk/travel/2236720/Airlines-anger-over-ID-cards.html

[322] Lyon, op. cit., 2009, p. 503.

targeted by surveillance.[323] The Electronic Frontier Foundation concurs, arguing that immigrant and refugee groups are unlikely to object to surveillance systems with which they are confronted "since they lack any power to speak of".[324] Therefore surveillance runs the risk of ensuring that marginalisation is re-produced in society.

2.4.2 Technological drivers

Although there are a range of different stakeholders involved in the introduction of surveillance systems, these stakeholders are influenced by particular "drivers", some of which are technological. For example, new discoveries, new standards and simply increases in available information can drive the introduction of particular technologies. As one example, a number of media and civil society organisation commentators have described the introduction of CCTV and the proposed introduction of biometric identity cards in the UK as "a solution looking for a problem", meaning that the UK government supported the introduction of these technologies simply because they were available and relatively affordable.[325] In a similar vein, some have argued that the mass collection of information by governments in relation to air travel or consumer behaviour is driven by the simple fact that this information is available. Increasing interoperability is also a technological driver, in that the ability to link systems together increases the attractiveness of technologies for stakeholders who are charged with procuring systems. For example, in 2002 the US and Canadian government encouraged the introduction of common standards to enable the interoperable reading of biometric passports in both the US and Canada for their "smart border" programme.[326]

Similarly, as technologies are always embedded in social systems and discourses, an understanding of technology as infallible also drives the introduction of surveillance technologies. Lyon argues that an understanding of technology as infallible drives the introduction of surveillance technologies because it shifts responsibility from humans, who can make mistakes, blink or lose concentration, to machines that do not.[327] Zureik and Hindle note that this use of technology as "the main tool for risk assessment" creates an "illusory sense of security".[328] According to Lyon in relation to biometrics, "such factors play into the hands of the marketers of biometrics, but they in turn find supporters, such as politicians and academics, and even critics, who further strengthen their hand".[329]

2.4.3 Economic drivers

In addition to technological drivers, another key driver of the introduction of surveillance technologies is economics. One such economic driver consists of stakeholders looking to maximise or maintain their profits. Zureik and Hindle note that "the economic payoff for the biometrics industry in the United States has been substantial" after September 2001.[330] This is particularly the case as the defence industry has sought new markets for technology it

[323] Lyon, David, *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge, London, 2003.

[324] Zureik and Hindle, op. cit., 2004, p. 129.

[325] See for example, Liberty, *Liberty's Evidence to the Home Affairs Committee on the Government's Identity Card Proposals*, Dec 2003.

[326] Zureik and Hindle, op. cit., 2004.

[327] Lyon, op. cit., 2008.

[328] Zuriek and Hindle, op. cit., 2004, p. 114.

[329] Lyon, op. cit., 2008, p. 503.

[330] Zureik and Hindle, op. cit., 2004, p. 123.

developed originally for military use. Unmanned aircraft systems, imaging scanners, biometrics and satellite surveillance provide some examples of such market augmentation. Both Wei and Li and Zuriek and Hindle predicted that the biometrics industry, in particular, would grow exponentially in the decade after 2001.[331] Maintaining revenue streams is a similar driver for the maintenance of surveillance systems. As Rothstein and Talbott note, virtually all of the data surrounding the effectiveness of DNA databases in relation to criminal justice are compiled and released by "crime laboratories and other entities with an interest in promoting the maintenance or expansion of DNA databases".[332]

Researchers also note that decreases in the cost of surveillance technology are another driver of surveillance technology uptake. In particular, Wei and Li state that because of a decrease in cost and an increase in convenience of use, fingerprinting is becoming increasingly popular for personal property protection, and in Asia and Europe, fingerprint readers are used to ensure that only legitimate owners are able to utilise their personal mobile phone.[333]

This also links to another driver of the introduction of surveillance technology – the protection of goods, services or property from theft, tampering or fraud. In addition to fingerprint readers, other technologies such as RFID and satellite tracking of vehicles represent further examples. Organisations installing surveillance technology also seek to use them for risk management or to avoid liability. McCahill finds that one of the uses of CCTV in shopping malls is to protect the management company from law suits as a result of trips, falls or other injuries as a result of spills or other obstacles.[334]

Government investment and other financial incentives are other drivers for the introduction of surveillance technology. Specifically, Zureik and Hindle note that the Homeland Security Administration in the US had a budget of $38 billion for investment in domestic security in 2004[335], while Webster notes that the UK government made approximately £200 million available for CCTV schemes between 1994 and 2003[336].

Retaining or increasing a customer base represents another economic driver. Again, McCahill notes that one of the primary reasons for the introduction of CCTV in the UK is to enable customers to "feel safe" shopping in the city centre, and prevent them from moving to the outskirts of the city to shop. As a result, public authorities and private companies such as retailers joined together to draw up proposals for the introduction of CCTV schemes in many town centres.[337]

2.4.4 Political drivers

The introduction of surveillance technologies also relies upon a number of political drivers. These political drivers include protecting citizens, reducing threats from crime and terrorism, reducing illegal immigration and co-operating with other governments or authorities. In terms

[331] Ibid. and Wei and Li, op. cit., 2006.

[332] Rothstein, Mark A., and Meghan K. Talbott, "The Expanding Use of DNA in Law Enforcement: What Role for Privacy?", *Journal of Law, Medicine & Ethics*, Summer 2006, p. 155. http://ssrn.com/abstract=1512746

[333] Wei and Li, op. cit., 2006.

[334] McCahill, op. cit., 2002.

[335] Zureik and Hindle, op. cit., 2004, p. 121.

[336] Webster, C.W.R., "CCTV policy in the UK: reconsidering the evidence base", *Surveillance & Society*, Vol. 6, No. 1, 2009, pp, 10-22. http://www.surveillance-and-society.org

[337] McCahill, op. cit., 2002.

of protecting citizens, this includes protecting citizens from crime and terrorism, as is the case with CCTV in town centres, on mass transportation and the use of CCTV combined with ANPR to reduce speeding and other motoring offences. Zureik and Hindle note that one of the main rhetorics espoused by government stakeholders is the use of surveillance technology for citizen protection.[338]

Reducing crime can also take the form of reducing the potential for illegal immigration, asylum shopping or other related border offences. Again, government stakeholders and the media often discuss surveillance technologies such as biometrics, imaging scanners and dataveillance as having the potential to reduce such offenses. For example, the Standing Committee on Citizenship and Immigration recommended that the US and Canadian authorities should increase co-ordination and the use of new technologies to gather intelligence and to implement "biometric tools, electronic finger print systems, linked databases and proximity card technology".[339] In terms of reducing threats from terrorism and crimes such as identity theft, Zureik and Hindle state that there is wide public acceptance in Canada, the United States and Britain for surveillance technologies such as biometrics that reduce these threats.[340]

Finally, as alluded to above, cooperating with other governments or authorities is also a political driver for the introduction of surveillance technology. Perhaps most famously, the introduction of RFID-enabled biometric passports in Europe was driven largely by a US declaration that this technology was necessary in order to enable visa-free entry to the USA for European citizens. As Lyon notes, "[there is] concern in Europe (and echoed, of course, in Canada, Mexico and elsewhere) that US demands dominate police and judicial approaches to cooperation."[341]

2.4.5 Social drivers

In addition to technological, economic and political drivers, there are also social drivers around the introduction of surveillance technologies. One such driver is the need to meet citizens' demands regarding subjective feelings of safety and security. David Lyon discusses this driver in terms of perceived "risk" in society, where terrorism is a "dread risk" with a low probability of occurrence but high consequence. As a result, "zero risk" options such as hi-tech interventions are favoured to attempt to eliminate the threat.[342] The introduction of CCTV in many contexts is also a reaction to citizen's demands; particularly if other, nearby areas already have CCTV systems, which is perceived to increase the threat from crime in a particular local area.[343] Surveillance technologies may also be demanded by insurance companies as a condition of insurance coverage. This may include access control systems for dangerous goods, security systems to protect private property or dataveillance systems to detect unusual activity. Finally, and perhaps paradoxically, some surveillance systems are introduced to meet privacy demands. One example is the introduction of body scanners at airports, particularly those with privacy enhancing software or other safeguards, which passengers seem to prefer to physical pat-down searches by security officials.[344]

[338] Zureik and Hindle, op. cit., 2004.

[339] Zureik and Hindle, op. cit., 2004, p. 125.

[340] Zureik and Hindle, op. cit., 2004.

[341] Lyon, op. cit., 2008, p. 503.

[342] Lyon, op. cit., 2008, p. 503.

[343] McCahill, op. cit., 2002.

[344] Jones, Jeffrey M., "In U.S., Air Travelers Take Body Scans in Stride", *Gallup*, 11 Jan 2010.

2.4.6 Summary

These different drivers and the stakeholders involved often determine which technologies are deployed in specific contexts and to perform particular functions. However, stakeholders often need to meet a range of demands and use surveillance for a number of different purposes. For example, public authorities need CCTV systems to respond to citizen demands for safety in public space as well as law enforcement demands for border security. Furthermore, the criminal justice system needs to be able to both detect crimes and identify individuals who are involved. The following section examines how surveillance technologies are organised into systems for particular purposes.

2.5 PURPOSES

In addition to assisting with different functions, the surveillance technologies described in this report are also used for a number of purposes, including border control, criminal justice, airport security, transport access, retail security, local authority/social service investigations and entertainment. In order to accomplish these purposes, this section demonstrates that surveillance technologies increasingly work as systems, where different technologies are interlinked and work to supplement or complement one another. This section will examine which surveillance technologies are being used to satisfy these different needs as well as whether and how these technologies are organised into "smart" systems that work in conjunction (assemblages).

2.5.1 Border control

A number of different, and sometimes interconnected, surveillance technologies are used to assist with border control in Europe as well as other countries. Visual surveillance is used to monitor land borders in a number of countries. In 2005, Predator UAVs along Arizona's border with Mexico were integrated into a surveillance system that included seismic sensors, infrared cameras and laser illuminators. If the seismic sensor is triggered by unauthorised immigrants or drug smugglers, "the Predator can investigate and...tag them with its laser illuminator. With the GPS coordinates and the infrared illuminator, agents have no difficulty intercepting" the individuals.[345] Sensors are also used to check trucks entering the UK from Calais, France and every lorry that passes through Calais is screened by CO2 probes, heartbeat monitors and passive x-ray scanning to try and detect illegal entrants.[346] Border control also utilises a range of database-dependent biometrics. The US-VISIT system collects and stores fingerprint and digital photograph data for those entering the country and is used to verify individuals before allowing them entry. In Europe, the Eurodac database holds fingerprints and personal details of asylum seekers, to prevent individuals from claiming asylum in more than one European country. The VIS II database holds fingerprints, facial images and personal details of individuals applying for visas to Europe. These details can be checked against terrorist watch lists and those who have committed immigration offences in other countries. New RFID-enabled biometric passports also integrate biometric details such as facial images and fingerprints, and iris scanning systems are used in some airports to allow

http://www.gallup.com/poll/125018/Air-Travelers-Body-Scans-Stride.aspx

[345] Dunlap, Travis, "Comment: We've Got Our Eyes on You: When Surveillance by Unmanned Aircraft Systems Constitutes a Fourth Amendment Search", *South Texas Law Review*, Vol. 51, No. 1, Fall 2009, pp. 173- 204.

[346] Ford, Richard, "Pushing Back the Boundaries", *The Times*, 22 Apr 2008, p. 5.

some travellers to avoid immigration checks. Finally, satellite surveillance may also be used to detect tunnels or other changes along borders that might suggest illegal entry or other criminal activity.

2.5.2 Anti-terrorism and criminal justice

Most surveillance technologies that are being used outside the military are being deployed in relation to anti-terrorism and/or criminal justice. CCTV was one of the earliest deployments of surveillance technology, as mass deployment began in the 1990s.[347] In the last 20 years, the use of CCTV has been expanded and augmented by other, associated applications such as combining CCTV with other technologies, as is the case for video enabled UASs, or combining CCTV with various recognition technologies. These recognition technologies may be focused on identifying people, such as is the case with facial recognition technologies, or identifying objects as used for automatic number plate recognition. In both these CCTV enabled applications, CCTV and recognition algorithms are combined with databases to enable recognition. Visual surveillance devices such as fixed or mobile CCTV cameras or UASs equipped with CCTV cameras may also be equipped with audio sensors or microphones to enable the recording of speech or the recognition of sounds such as gunshots. Other imaging devices like thermal imaging scanners or infrared imaging can be combined with CCTV cameras or UASs to assist in visual surveillance, or they can stand alone. Thermal imaging scanners can be used to detect unusual heat sources in a home or other private building, which might suggest marijuana cultivation and imaging scanners such as millimetre wave scanners can be used to detect weapons or other prohibited materials. Satellite, mobile phone and/or GPS surveillance can all be used to monitor or locate an individual or a space or place. These technologies may also be used to track an individual's movements either retrospectively or in real time. Communication surveillance such as wiretapping, and more recently call logging or e-mail monitoring can help to understand organised crime organisations and detect illegal activities. Biometrics, such as fingerprints and DNA data are stored by law enforcement authorities in large, searchable databases (such as AFIS – automated fingerprint identification system, and CODIS – combined DNA index system) to enable the identification of known individuals. Increasingly devices which read biometric data are being miniaturised to allow police to carry fingerprint readers or facial recognition devices with them.[348] Dataveillance technologies such as data mining and profiling are also being used by law enforcement to understand patterns of behaviour and attempt to predict which individuals might have criminal or terrorist inclinations.

2.5.3 Airport security

In relation to a number of events, but particularly since the events of September 2001, airports have been a focus of surveillance technology for security. Airports use imaging scanners for luggage, carryon items and to look for prohibited items concealed underneath passengers' clothing. Airports supplement these imaging scanners with other visual surveillance technologies such as CCTV systems to monitor passengers' activities and demeanour. Airports also deploy sensors such as metal detectors to attempt to identify whether a passenger is carrying weapons and explosive sensors to check whether passengers or their belongings have come into contact with explosive chemicals. Airports also install access control systems, which may rely upon RFID cards or biometrics to ensure that access to restricted areas is limited to authorised personnel. Finally, biometrics, specifically facial

[347] Webster, op. cit., 2009.

[348] Steel and Angwin, op. cit., 2011.

recognition technologies, fingerprint scanners, iris scanners and biometric passports are used to verify that the person presenting him or herself to airport security is the person who owns the identification documentation.

2.5.4 Transport access and security

Mass transport systems also use a range of technologies to enable access and to provide security. The use of these systems to provide security share many applications with law enforcement technologies (such as CCTV), and these are discussed above. This sub-section focuses on technologies or assemblages which are primarily used on mass transport systems. The primary surveillance technology that provides access to transportation is the use of RFID enabled travel cards. These travel cards integrate an RFID chip that produces a unique ID number, which is connected to personal information stored on databases in the back end system. This technology also increases transportation security, since only individuals who have paid a fare are able to access waiting areas, buses, trains, etc. Another technology that increases transportation security is behavioural recognition technology connected to CCTV systems. This technology uses pattern recognition to determine whether unusual activity is taking place, such as loitering on train platforms, unattended baggage or other potentially dangerous or harmful activities.[349]

2.5.5 Retail security and fraud prevention

In relation to retail security and fraud prevention, a number of surveillance technologies are used to prevent crime and fraud, including RFID technology and other tag sensors, CCTV and dataveillance applications such as databases, data mining and data profiling. RFID tags and other tags with associated sensors are used to track the purchase of individual items and record when they leave the store. RFID tags were used in Metro stores in Germany before an outcry by digital rights campaigners.[350] Shopping malls, small private stores and other retailers use CCTV technology to prevent or detect shoplifting and other crimes. In some cases, RFID and CCTV have been used in conjunction, where the movement of an RFID chip embedded in particular products, such as hi-end razor blades, triggered a CCTV camera to take an image of the person who moved the item.[351] However, this trial was also abandoned after consumer outcry. In contrast, databases, data mining technologies and profiling applications are more widely supported by consumer groups as they have been successful in combating credit card fraud and other criminal activities.

2.5.6 Local authority/social service investigations, etc.

A range of surveillance technologies are also used to conduct social service checking or investigations as well as local authority investigations. In relation to social service checking, biometric technologies such as fingerprints have been used to ensure that an individual is only claiming benefits under one name, or in only one jurisdiction.[352] Gilliom has also found that databases of benefit recipient personal information are being matched against employer and tax records to ensure that individuals who are claiming benefits are not hiding income they

[349] Prati, Andrea and Rita Cucchiara, "Video Analysis for Ambient Intelligence in Urban Environments", in Katherine J. Strandburg and Daniela Stan Raicu (eds.), *Privacy and Security Technologies: An Interdisciplinary Conversation*, Springer, New York, 2006.

[350] Libbenga, Jan, "German Revolt against RFID", *The Register*, 1 Mar 2004.

[351] Jha, Alok, "Tesco tests spy chip technology: Tags in packs of razor blades used to track buyers", *The Guardian*, 19 July 2003, p. 10.

[352] Lyon, op. cit., 2009.

may be earning which could affect their benefits.[353] A similar system is also being used to ensure that those claiming single occupancy benefits on local taxes do not have more than one adult registered on the electoral roll.[354] In the UK, local authorities can also use CCTV and other surveillance devices to conduct investigations into whether individuals are fraudulently claiming to live in particular school catchment areas, to ensure premises with liquor licenses are not selling to minors and other, similar infringements.

2.5.7 Entertainment (Television shows, "selling newspapers")

Many different types of surveillance technologies are also used to support entertainment. One of the classic examples is the television show "Big Brother" which uses CCTV cameras to monitor the daily activities of individuals who agree to live in a house for a set period of time. CCTV images are also used by mass media in news entertainment. One example includes the use of CCTV images of crimes for a show called "Crime Stoppers" which is an "institutionally embedded" news entertainment programme that is aired on television in North America as well as "twenty other countries, including the United Kingdom, Australia, India, the Netherlands and South Africa".[355] These shows utilise CCTV images in an attempt to ask the public to participate in crime fighting by identifying any individuals they recognise. However, Lippert and Wilkinson argue that many of the strategies used in the reporting of crimes via shows such as Crime Stoppers explicitly seek to make the show entertaining. Such use of CCTV images is not confined to the television; they are also used to sell newspapers. Finn and McCahill describe a popular newspaper format in the UK called "Caught on Camera" where CCTV images are reproduced in newspapers to encourage readers to identify suspects.[356] Photographic images of celebrities have long been used by media organisations to entertain readers and sell products. The recent scandal around the *News of the World* demonstrates that communication surveillance (voice message hacking of celebrities and other figures) as well as visual surveillance is used by journalists or other media figures in order to entertain and/or increase market share. Another entertainment based surveillance practice is celebrity location tracking applications, which use location based surveillance, specifically mobile phone triangulation, alongside photography to enable individuals to "track" celebrities.[357] Subscribers who see a celebrity in public note the location of the celebrity and/or combine this with a photo of the celebrity in that location. The subscriber then uploads the information to the application and phone network and shares it with other subscribers.

2.5.8 Summary

This section demonstrates the ways in which formerly distinct surveillance systems are converging and being combined in order to accomplish specific purposes.[358] Both data

---

[353] Gilliom, John, *Overseers of the Poor: Surveillance and the Limits of Privacy*, University of Chicago Press, Chicago, 2001.

[354] Welch, James, "Data matching: a threat to privacy?", *The Guardian*, 23 Nov 2009. http://www.guardian.co.uk/commentisfree/libertycentral/2009/nov/23/data-matching-privacy

[355] Lippert, Randy, and Blair Wilkinson, "Capturing crime, criminals and the public's imagination: Assembling Crime Stoppers and CCTV surveillance", *Crime Media Culture*, Vol. 6, No. 2, 2010, p. 132.

[356] Finn and McCahill, op. cit..

[357] Bryant, Martin, "Proof That Location's Gone Mainstream: The Celebrity Stalking App", *TNW (The next Web apps),* 28 June 2010.

http://thenextweb.com/apps/2010/06/28/proof-that-locations-gone-mainstream-the-celebrity-stalking-app/

[358] Haggerty, K., and R. Ericson, "The surveillant assemblage", *British Journal of Sociology*, Vol. 51, No. 4, 2000, pp. 605-622.

collection and data processing are becoming more complex, more varied, and are being automated.[359] Surveillance technologies, which used to be the prerogative of government agencies, are now in the reach of companies and citizens.[360] Taken together, these trends lead to what we call "smart surveillance", which Wright et al. define as "surveillance systems that are capable of extracting application-specific information from captured information (be it digital images, call logs or electronic travel records) in order to generate high-level event descriptions that can ultimately be used to make automated or semi-automated decisions. Smart surveillance systems inherently offer a high level of scalability, as they in turn can act as input to other surveillance systems."[361] The following section discusses how different surveillance technologies are developing and evolving, and how complexity and automation are becoming more prevalent in surveillance technologies, systems and assemblages expected to emerge over the next 10 years.

2.6 MAJOR SMART SURVEILLANCE RESEARCH INITIATIVES

The main aim of this section is to present the smart surveillance systems expected to emerge over the next decade. A good starting point for this future-oriented task is represented by the recent research initiatives funded by the European Commission within the Seventh Framework Programme (FP7, 2008-2013), and United States agencies such as the Defense Advanced Research Projects Agency (DARPA) and the National Science Foundation (NSF). Some of these research initiatives include foresight studies designed to identify technological trends in sectors such as surveillance and security. This section will also highlight the "critical parts" of smart surveillance (e.g., for crime control, border control, airport security) in order to contrast them with less critical parts (such as commercial applications or applications used by local authorities and individuals).

In a first step, we collected relevant projects in a comprehensive list (the annexed *Smart Surveillance Research Projects List)* that identifies 38 projects funded by the European Commission (FP7, mainly under the Security[362] and ICT Themes[363]) and 20 US projects, funded by DARPA[364] and the NSF. The absolute number of projects does not directly reflect the budget devoted to a specific research area, though – DARPA projects usually have a wider scope (and a considerably larger budget) than individual EU projects.

For each project, we list the following information:

- *full title*, *acronym* and *webpage*: in order to identify the project

[359] An example for the automation of data collection is given by Diffie, W., and S. Landau, "Communications Surveillance: Privacy and Security at Risk", *Communications of the ACM*, Vol. 52, No. 11, Nov 2009, pp. 42-47, for the surveillance of communications. The widespreading and automation of data analysis can be observed, for example, by means of the profiling technique, which is enabled by data mining: Hildebrandt, M., "Defining Profiling: A New Type of Knowledge?", In M. Hildebrandt and S. Gutwirth (Eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, New York / Heidelberg, Springer, 2008, pp. 17-46.

[360] Wright, D., M. Friedewald, S. Gutwirth, M. Langheinrich, E. Mordini, R. Bellanova and P. De Hert, "Sorting out smart surveillance", *Computer Law & Security Review*, Vol. 26, No. 4, 2010, pp. 343-354.

[361] Ibid., p. 344.

[362] The complete list of projects funded under the theme security is available at http://cordis.europa.eu/fp7/security/projects_en.html

[363] See the FP7 projects dynamic database developed by the HIDE project and available on the HIDE website at http://www.hideproject.org/references/fp7_projects.html

[364] Information taken from DARPA *Financial Year 2012 Budget Estimates*, available on the DARPA website.

- *period*: since the main aim of this task is to focus on *emerging* smart surveillance, we collected information on projects that have been funded very recently, or that have just been approved for funding. The list of EU projects covers the period from 2008 to 2014 (as an exception, we also included a foresight project on Information Society technologies in the European research area funded under FP5). For the US projects, the period covered starts with the 2010 budget. For many US projects, we have not provided an end date, since they are defined as "continuing projects".
- *type*: the projects mainly have a technology focus, but we have also taken into account ethical assessment and foresight projects.
- *programme/agency*: indicates the source of funding, i.e., US agency or European programme and sub-programme.
- *funding*: the total amount of funding.
- *abstract*: this section reports the main goals of the project and the strategies to achieve these objectives.
- *comments/results*: relevance for smart surveillance research and already available results when applicable.

In a second step, we then distilled this information in order to identify trends, core research areas and critical parts. We therefore extracted from each project – dependent both on its semantic breadth and its size – up to three main aims (e.g. "person identification" or "activity recognition"). We also identified the core technologies (for non-technological projects: the methods) used to achieve these aims. A subsequent mind mapping exercise revealed shared aims and common technologies across all research projects. Finally, we created groups of semantically related project aims (such as "person identification", "activity recognition", "person tracking" and "intrusion detection"). The more ubiquitous the presence of such a group within individual projects, the more likely it is to point towards a future trend.

2.6.1 Foresight studies

In addition to research on technology development, we also took recent foresight studies into account in order to identify technological trends. Most of them do not, however, have a particular focus on the development of surveillance technology. One UK foresight study, for instance, only states that a wide range of technological developments will increase the capability for continuous and widespread surveillance. It then lists well known technologies ranging from CCTV and spy satellites to AI methods to identify persons or suspicious behaviour from video (or other sensor) material.[365]

Recent foresight studies dealing with security issues originated in the FP7 projects "Europe's evolving security: drivers, trends and scenarios" (FORESEC, 2008-10) and "Foresight of Evolving Security Threats posed by Emerging Technologies" (FESTOS, 2009-11). The FORESEC Delphi survey report summarises the experts' expectation that "official forces will use IT for enacting more security, e.g. by implementing more surveillance technologies". More than 80 per cent of the experts think that a substantial deployment of surveillance technologies is very probable or almost sure. A majority of these experts also think that surveillance technologies are crucial or very important for security.[366] FESTOS is less specific regarding surveillance technologies. Among the surveillance-related technologies that might become security threats, however, the study lists: ambient intelligence/Internet of

[365] Rhydderch, Alun, Peter Glenday and Farzana Dudhwala, "Technology and Innovation Futures: UK Growth Opportunities for the 2020s", URN 10/1252, Foresight Horizon Scanning Centre, Government Office for Science, London, 2010, Annex, p. 177. http://www.bis.gov.uk/foresight.

[366] Aguirre-Bastos, Carlos, Susanne Giesecke, Dana Wasserbacher and K. Matthias Weber, "1st Delphi Report", FORESEC Deliverable 4.3, FORESEC Project 2009. http://www.foresec.eu/wp3_docs/Delphi.pdf

things, mobile phone technology mash-ups, RFID and smart dust, swarm robotics as well as cyborg insects.[367]

2.6.2 European Security Research and Innovation Forum

EU and US research on smart surveillance is mainly focused on law enforcement, military and intelligence purposes in high-level security applications. However, the technologies developed by this research have the potential of being used for other, more general purposes. The ESRIF[368] final report traced the objectives of future EU security research. ESRIF's task was to develop an EU strategic plan for security research over the next 20 years – the European Security Research and Innovation Agenda (ESRIA). The report defines surveillance as a top priority for the future EU security research, and identifies the key research needs in this field. The report specifically takes into account the broader implications of surveillance technologies for society:

> Ideally in a secure society, citizens live in an environment of dignity and respect for their privacy rights and their possessions. [...] However, the same society has to cope with threats from criminal, terrorist and natural sources. In order to sustain its future, society must be prepared for such attacks and develop knowledge and tools to be resilient. [...] Surveillance is increasingly a central element of security management and takes place through a number of means, from closed circuit television to various biometric tools. As these tools are developed, the impact on European values of the relation between surveillance and civil and human rights, the place of new technologies in society role, their role in security crises and their consequences for the individual remain poorly understood. Future research and innovation should carefully assess these societal questions and their links with Europe's security.[369]

The ESRIF report identifies the most urgent need for surveillance technology research in the mission areas "security for citizens" (i.e., protection against terrorism and organised crime), "border security" and "situation awareness". For protection against terrorism and organised crime in public areas and specific locations, ESRIF asks for the development of "high capacity discrete surveillance systems" (satellite, air, terrestrial and tactical) and integrated control centres which can apply automated recognition, tracking and tracing techniques. For border control (and in the field of transportation in general), the report sees a need for systems that are capable of monitoring wide areas and big crowds. This requires an adaptive network of sensors (airborne and terrestrial) as well as advanced techniques for pattern analysis. The challenge is to have wide coverage with a reasonable resolution and a low false alarm rate. Situation awareness is a cross-cutting topic dealing with data fusion, information management and decision support.

According to the report, the development of surveillance systems capable of an automated analysis of data that could be combined with pre-existing intelligence databases as well as technologies for the automated assessment of suspicious behaviours are included among the top priorities and key challenges for future security research in Europe. The *Smart*

---

[367] Hauptman, Aharon, Ori Katz, Yoel Raban and Yair Sharan, "Report on potentially threatening technologies", FESTOS Deliverable 2.3, FESTOS Project, 2011. http://www.festos.org/images/stories/FESTOS/festos%20d2.3-ver2.0_290511.pdf.

[368] European Security Research and Innovation Forum, "Final Report", December 2009. www.esrif.eu

[369] Cited from ESRIF, op. cit., p. 21.

Surveillance Research Projects List and the related *mind maps* below largely reflect the priorities and research needs identified by the ESRIF report.

2.6.3 Top priorities and funded projects

In FP7, the European Commission funds surveillance research mainly within the scope of two themes (SECURITY and ICTs), but surveillance-related projects can be found in other segments of the Cooperation programme, such as Transport and Space. The main research goals of the enlisted projects include the development of systems for the automated identification or tracking of individuals or of objects that can be related to individuals, activity recognition, software that identifies "suspicious" behaviours or intentions, and automated identification of illegal trespassing.

EU projects related to the automated identification of individuals or tracking of objects include *INDECT, SAMURAI, SUBITO, TASS, EFFISEC, I2C, BIODISTANCE, SEARISE*, and projects related to intrusion detection or activity recognition include *ADABTS, INDECT, SAMURAI, OPARIUS, TALOS, WIMAAS, MISPIA, PROMETHEUS, SEARISE, SFLY, VANAHEIM*. Part of the EU funding also goes to the development of new algorithms and data integration systems that are expected to facilitate the automated processing of data, and to the research on new sensors that could expand the type of data being collected. Such projects related to the development of new algorithms and techniques for data fusion and data mining include *SCIIMS, AMASS, APIDIS, 4DVIDEO FEEDNETBACK, FINE*. DARPA, on the other hand, groups its current research focus into nine so-called "strategic thrusts"[370]:

- Robust, Secure, Self-forming Networks;
- Detection, Precision ID, Tracking, and Destruction of Elusive Targets;
- Urban Area Operations;
- Advanced Manned and Unmanned Systems;
- Detection, Characterization and Assessment of Underground Structures;
- Space;
- Increasing the Tooth to Tail Ratio;
- Bio-Revolution;
- Core Technologies.

Examples of current research projects funded by DARPA on smart surveillance have been divided according to the budgetary line they refer to: 1. Basic research – supporting the scientific study and experimentation that is the basis for more advanced knowledge and understanding in information, electronic, mathematical, computer, biological and materials sciences; 2. Applied science – directed toward the application of advanced, innovative systems and technologies; 3. Advanced technology developments – aiming at evaluating and testing advanced information systems research and development concepts.

Surveillance-related projects or projects that are potentially relevant for future military and security applications are included within these three budgetary lines. The main goals of DARPA research projects in the field of smart surveillance include the development of new theories on machine learning and reasoning that could enhance the capabilities of future surveillance systems (*Mathematics of the Brain*, *Mathematics of Sensing, Exploitation and Evaluation*, *Machine reading and reasoning technologies*, *Mind's Eye*), cognitive and ubiquitous powerful computing (*Cognitive Cloud, Ubiquitous High Performance Computing*), video surveillance and threat detection systems (*Video and Image retrieval and analysis tool*,

[370] See *Defense Advanced Research Projects Agency (DARPA) Strategic Plan*, May 2009.

Visibuilding, Wide Area Video Surveillance, *Wide Area Network Detection*, *Nano air vehicle*, *Military Imaging and Surveillance Technology*), automatic information processing systems (*Web scale information integration*, *Insight*), new sensors (*Bionic sensors for threat detection*, *Advanced Soldier Sensor Information System*), social networking monitoring (*Maths for social networks*, *Nexus 7*), and communication surveillance (*Global Autonomous Language Exploitation*, *Robust Automatic Translation of Speech*).

The list of DARPA projects shows a considerable difference with respect to the EU research focus. The US Agency pays particular attention towards the creation of advanced tools for what could be called "surveillance 2.0": apart from the development of traditional video surveillance technologies and threat detection systems, large research efforts of DARPA are devoted to the development of systems for the (entirely or partially automatic) monitoring of social networks.

2.6.4 The ethical, social and legal aspects of EU and US surveillance research

The majority of the enlisted EU projects, and the totality of the US ones, are technical, i.e., they focus on engineering issues and technological development and demonstrations. However, part of the European research effort is also devoted to the analysis of the broader ethical and legal implications of security technologies. The European Commission has funded research and supported activities on social implications of security technologies since its Fifth Framework Programme[371]. Starting with the current FP7, the Commission has included an "ethics, security and society" theme in the Security Programme under Activity 6 (Security and Society). The ESRIF report thus states that, "ethical issues and full respect for privacy, liberty and civil rights are aspects that cannot be neglected in all present and future technological developments. A balance must be achieved between the privacy rights of citizens and the need to protect Europe and its citizens against threats."[372]

Projects funded in the scope of the Security, as well as the Science and Society FP7 themes, which could be of relevance for future EU research on smart surveillance, are:

- *ADDPRIV*: devoted to the development of a privacy sensitive video surveillance.
- *INEX*, *DETECTER*, *SAPIENT*: ethical and legal assessment of security technologies.
- *FESTOS, FORESEC*: foresight projects on evolving security threats posed by emerging technologies.

In the ICT and Science in Society themes, the ethical aspects of emerging surveillance technologies are addressed by:

- *ETICA,* on ethical issues of emerging ICT applications,
- *HIDE,* on ethics of homeland security, identification technologies and personal detection, and
- *RISE, on rising pan-European and international awareness of biometrics and security ethics*.

Despite its lack of projects focusing directly on ethical assessments, DARPA is committed to take into consideration all non-technical, sensitive aspects of its research:

---

[371] E.g., Changing landscape of European liberty and security (CHALLENGE), a project which took place from 2004 to 2008; European liberty and security (ELISE), 2004-2008; Bioethical Implications of Globalisation (BIG), 2002-2006.

[372] ESRIF, op. cit., 2009, p. 155.

> "There is often a tension between novel concepts and an underdeveloped ethical, legal, and societal framework for addressing the full implications of such research. This is a problem not unique to DARPA. Other agencies have faced it, such as NIH, during the Human Genome Project. If we do our research well, we will necessarily bump up against these concerns."[373]

In order to address privacy implications, DARPA states that the agency will "consistently examine the impact of its research and development on privacy, responsibly analyse the privacy dimension of its on-going research endeavours with respect to their ethical, legal and societal implications (ELSI), transparently respond to the findings of its assessments for unclassified work, and ensure independent review of its classified work, in accordance with a commitment to shared responsibility for addressing the privacy issue."[374] To fulfil its responsibilities both to innovation and ethical assessment, DARPA has taken some initiatives, such as the creation of an internal independent privacy review panel that works in liaison with the Department of Defense Privacy Office, and the establishment of an ELSI working group together with the National Science Foundation.

2.6.5 Analysis

Figure 2.2 and Figure 2.3 below summarise the findings of the previous section, structuring both the aims of the individual projects, as well as the technologies used and/or envisioned to achieve these goals. As the discussion in the last section has shown, most projects financed by the European Commission and DARPA focus directly on different aspects of *human surveillanc*e. Five European and two US projects have *automatic identification* of persons amongst their main goals; nine projects (seven EU and two US) focus on the *automatic recognition of human activity*; a further 10 projects (five each) on the *tracking of persons*, including the simultaneous tracking of several persons; and another nine projects (eight EU and one US) aim at *intrusion detection*, either for a particular property or across the border.
Some projects aim at the *monitoring of objects*. While at first glance they might thus not seem relevant to an analysis of surveillance, they actually can be significant:

- either because the objects under scrutiny (such as luggage within an airport) can easily be matched to their owners, turning thus an object monitoring system into a human tracking and/or activity recognition one,
- or because the technology developed for such a project (such as unmanned flying drones fitted with a variety of sensors and cameras) can easily be used for human surveillance as well.

A second core area focuses on what is often called *big data*: combining the information from various sources (including the direct surveillance sources above), searching for patterns or stereotypes, and generating higher-level information. While the European projects in this domain focus more on combining many individual information sources, the DARPA projects aim rather at generating new or better information from existing sources. There are two DARPA projects aiming at the machine-based distillation of information, and another two projects aiming at the autonomous translation of speech recorded in noisy natural environments (such as a crowd of people).

---

[373] Defense Advanced Research Projects Agency, "DARPA's S&T Privacy Principles". http://www.darpa.mil/About/Initiative/DARPA%E2%80%99s_S_T_Privacy_Principles.aspx

[374] Defense Advanced Research Projects Agency, op. cit.

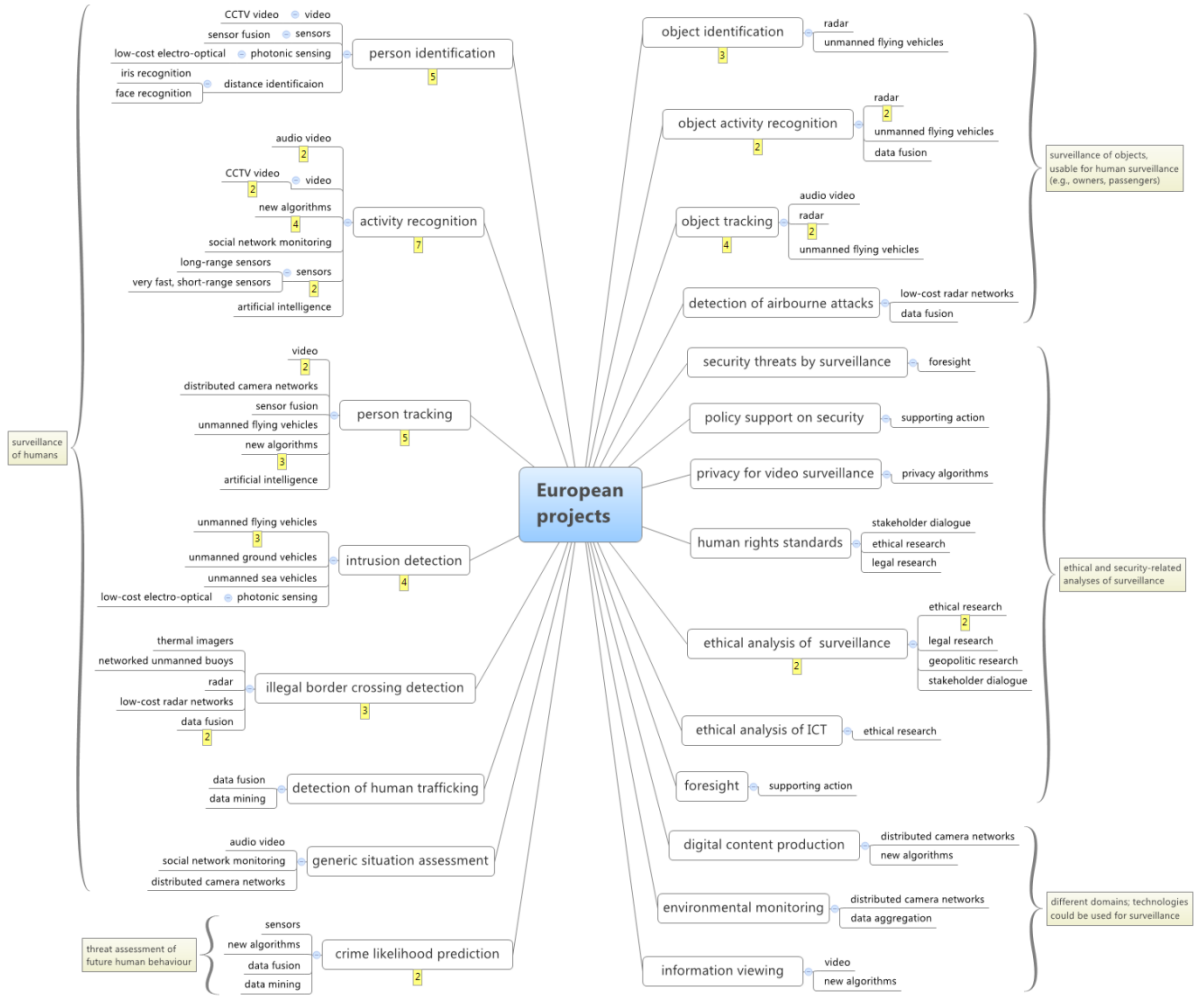


Figure 2.2: European projects exploring different surveillance-related aspects. The first-level indicates the main aims of the projects, while the second layer indicates the technological means to achieve them. The small numbers indicate the frequency of occurrence across all surveyed projects.

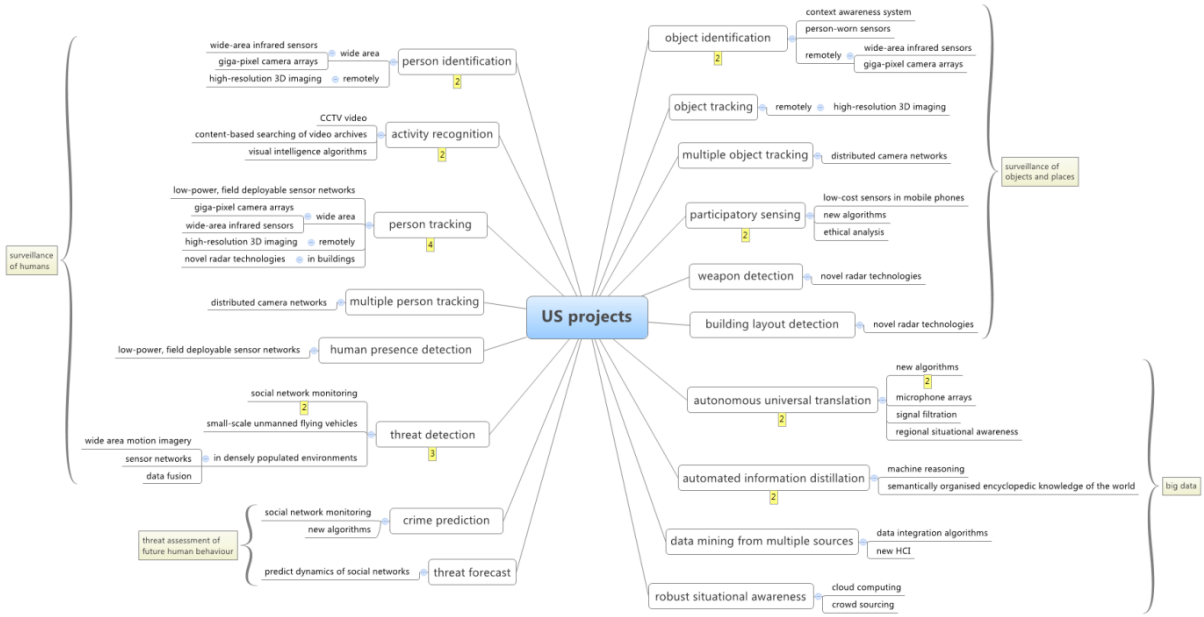


Figure 2.3: Surveillance-related research in the US (DARPA and NSF). In contrast to EU-funded research, there is a notable absence of projects targeting ethical analysis.

The EC and DARPA have each funded two projects focused on *predicting unwanted events* such as terrorist or criminal acts.

In the European FP7 program, and unlike the DARPA projects, the *ethical analysis* of surveillance is plainly represented. From the total of 38 surveillance-relevant research projects identified, no fewer than seven investigate the ethics of state surveillance at different abstraction levels: from concrete technological proposals for a better privacy-compliance of video surveillance up to the effects of today's and tomorrow's surveillance on human rights.

2.7 EMERGENT TECHNOLOGIES AND ASSEMBLAGES

The research initiatives presented above have given rise to particular new technologies, which are increasingly organised into assemblages or "smart surveillance" systems, reinforcing and widening thus the trends presented in section 0. These emergent technologies and new types of assemblages are discussed here.

2.7.1 Technologies

To achieve the aims of the projects listed above, numerous, heterogeneous technologies are under research within the different projects. While some projects have the exclusive development of a new technology at their core, most projects use them jointly with existing technologies to achieve a surveillance goal. *BIO-DISTANCE*, which focuses on the development of technologies for remote biometric identification, is an example of a project with an exclusive focus on a new technology; the *ADABTS* project, which uses video input from off-the-shelf CCTV cameras to study new activity recognition algorithms, is an example of integration with existing technology.

New sensors

One of the most important technologies for surveillance is obviously *video* – a total of 14 projects use video data. Most projects, though, do not develop new video technology. They rather use existing cameras and focus their technological efforts elsewhere, often in the development of smart surveillance algorithms evaluating the video input. There are exceptions though: the *IDETECT4ALL* project, for example, develops new low-cost electro-optical components for the identification of persons and of possible intrusions.

While video is the most widely used type of sensor data in both European and US projects, it certainly is not the only one. Other types of sensors developed in European and US projects include:

- *biometrical sensors* for remote identification and authentication (*BIO-DISTANCE*, *MIST*),
- *novel radar technologies* for the identification of persons and objects (such as weapons) remotely, for example, inside buildings (*I2C*, *Visibuilding*),
- *sensor networks* for the autonomous transmission of information between nodes in the area under scrutiny (*AMASS*, *Networked Bionic Sensors for Threat Detection*, *WAND*),
- *new microphone arrays* for voice recording in natural environments and subsequent automatic translation (*RATS*), and
- an architecture for *participatory sensing* (*NeTS*).

Unmanned vehicles as mobile sensor platforms

Sensors need a physical platform from which to operate. While for numerous applications (for example, for biometric access control) a static platform is adequate, a mobile sensor platform opens new surveillance possibilities.

The recent surge of interest in unmanned aerial vehicles (*drones*) is well represented in European and US projects. Six projects in total make use of UAVs as mobile sensor platforms (*I2C*, *OPARUS*, *TALOS*, *WIMAAS*, *SFLY*, *NAV*). As with video cameras, while most projects use existing drones in their technological mix aimed at surveillance, some try to advance the technology itself. For example, the *NAV* project is developing very small-scale (a few centimetres) autonomous drones.

Two projects (*AMASS*, *WIMAAS*) propose the related *unmanned networked surveillance buoys* and *unmanned sea vehicles*, respectively, and *TALOS* uses *unmanned ground vehicles* next to airborne ones.

New powerful algorithms

The automatisation of surveillance (in other words, the emancipation from the processing limits imposed by human operators and from the risk of error due to their fatigue) lies at the core of all advanced surveillance projects. In all examined projects, software systems take care of identification, monitoring, tracking, or activity recognition – human operators are sometimes consulted in a second step for the fine-tuning of already filtered events.

Due to these processing capabilities, but also to powerful, wide-area and detailed sensorial coverage, some of the projects display an impressive capacity for surveillance. DARPA's *Wide Area Video Surveillance* project, for example, can choose 130 independent targets within a Giga-pixel camera array (providing both video and infrared imagery) and automatically follow their movements. While the system is aimed at battlefield surveillance, such systems could be deployed for other surveillance tasks as well.

Unlike European projects, DARPA projects are developing a class of algorithms that will surveil social networks with the aim to infer current or future threats.

2.7.2 Future smart surveillance assemblages

The saying that "predictions are difficult, especially about the future" applies a fortiori to a domain as vast, heterogeneous and dynamic as surveillance. Nevertheless, combining the surveillance technologies most prevalent in current research projects with already existing technologies, and taking into account current societal, political and economic trends, we can arrive at a number of future smart surveillance systems and assemblages that are feasible, if not likely, to emerge over the next decade. Four such future smart surveillance scenarios are illustrated below.

Border and crowd control with drone-mounted sensors

The detection of illegal trespassing ranks high among the aims of current European projects. No fewer than eight of them have "intrusion detection", "illegal border crossing detection" or "detection of human trafficking" as a core function related to the security of borders or

infrastructures. To achieve such functions, a large number of the projects rely on sensors or networks of sensors mounted on unmanned aerial, sea or land vehicles.

As outlined above, police forces already use drones for the video surveillance of rallies or sport events that might lead to riots, or for the security of sensitive meetings. Video-equipped drones are also used for border control. It is likely that ever smaller and cheaper drones will be able to patrol increasingly long border stretches – not only North American ones, but the long maritime borders of Europe as well. The next logical step for UAVs used for crowd control is the development of smart CCTV algorithms for person tracking, facial and/or activity recognition – and indeed such development is the subject of on-going research.

Becoming more speculative, law enforcement might start using swarms of drones, similar to the "spiders" depicted in Steven Spielberg's film *Minority Report*.[375] The speculation here is more related to the societal acceptance than the technological feasibility. Technologically, such small-sized crawling drones equipped with both optical and infrared cameras are already being produced,[376] and police forces in the US have been testing them for reconnaissance in dangerous environments. In a decade from now, such land-based drones are not likely to achieve the agility or group intelligence of Spielberg's spiders. However, they might very well be equipped with iris scanners and be wirelessly connected to a biometric database, making them able to identify humans, as in the movie (albeit they will surely not force citizens' eyes open). Networked crawling, swimming and aerial drones might become a standard tool for law enforcement and counter-terrorist forces; the sensors with which they can be equipped, and the level of surveillance and intrusion they are allowed might become a matter of debate.

Lateral surveillance with drone-mounted sensors

Lateral surveillance could also be on the verge of a boom due to sensors mounted on unmanned vehicles, particularly UAVs. Hobby pilots of remote controlled (R/C) aircraft and helicopters routinely fly UAVs along the highest peaks of the Alps, along motorways, above private properties, and vertically along skyscrapers, as numerous clips on Internet film platforms show.[377] There is an obvious lateral surveillance potential to this development, for example, when filming unsuspecting targets from above their own property or through the windows of their apartment on the 45th floor.

In addition to cameras, UAVs can be equipped with other sensors used for different sorts of lateral surveillance. A slightly curious such example is represented by a rather large UAV carrying computation equipment strong enough to be used for communication surveillance. The drone can crack GSM encryption and carry out a man-in-the-middle attack for WiFi communication.[378] Other assemblages are possible: combining sensor-recorded data with public data from the yellow pages or the telephone book, it might be possible to match the data recorded by the UAV to known names and addresses. In a negative but possible scenario, such data could then be used for blackmailing these persons. By feeding the navigation system of flying drones with publicly available 3D models of a city, they could be sent autonomously for the targeted spying of a subject's known address.

[375] Spielberg, S. (Dir.), *Minority Report*, Twentieth Century Fox Film Corporation & DreamWorks SKG, 2002

[376] See, for example, Recon Robotics, "Recon Scout XT". http://www.reconrobotics.com/products/recon-scout_XT.cfm

[377] See, for example, the videos of the "Team Black Sheep". http://www.team-blacksheep.com/videos

[378] Flacy, M., "Men build small flying spy drone that cracks Wi-Fi and cell data", *digital trends*, 30 July 2011. http://www.digitaltrends.com/mobile/men-build-small-flying-spy-drone-that-cracks-wi-fi-and-cell-data/

Mandatory crowd sourcing

As discussed in the previous chapter, the ability to locate citizens (and/or some of the objects they own) in certain circumstances is, or will soon become, mandatory. Mobile telephony operators are required by law to be able to precisely locate their subscribers, and hand over this data to law enforcement authorities upon request. From 2015, all new vehicles sold in the EU will have to be equipped with the eCall system which will alert paramedics and the police in case of an accident and transmit the vehicle's whereabouts as well. Providers of mobile telephony are selling their customers' location data to producers of satellite navigation systems, who infer traffic jams from this information. Although the data is anonymised, the customer has nevertheless no possibility to opt out.[379]

In a similar manner, it is conceivable that telephony providers might start handing over further data recorded by their customers, either because the law requires them or due to commercial interests. Such data could then be used for novel types of surveillance assemblages. Every telephone is, for example, inherently equipped with an audio sensor – its microphone. As seen in the previous sections, law enforcement authorities in the US, and recently in Europe, have started to install sound ranging sensors in some cities for the automatic detection and localisation of gunshots. The costly part of such an operation is the deployment of the sensors throughout cities; the algorithms for filtering the sound of a firearm and for triangulating the position of the shooter are rather simple. If providers of mobile telephony were asked to run gunfire detection algorithms on the voice streams of their customers when they are making a call, the complex and costly part of gunfire detection would be easily tackled to almost the same results: most likely, there is always and anywhere someone talking on the phone. No software would need to be installed on the customer side; the algorithm would only analyse the voice streams within the premises of the providers. And the location, while not as precise as the one provided by dedicated audio sensors installed in known locations, would also be precise enough to constitute valuable information for automatically dispatched police forces. This assemblage represents a technologically feasible example for future mandatory crowd sourcing.

Smart "blackbox" for communication/SMS surveillance

As discussed in the previous sections, the surveillance of communication is becoming both easier in some aspects, and more difficult in others. However, on balance, it seems that the surveillance of communications is becoming rather more difficult than it was at the initiation of the Echelon programme of the US, UK, Canada, Australia and New Zealand, which has been credited with the ability to intercept a good deal of the worldwide radio and satellite communications.[380] Nowadays, however, fibre optic is the medium used by the vast majority of communications.[381] Such communications can only be intercepted by placing a wiretap at one of the points where such communication is being switched, making it harder for foreign intelligence agencies to access the inland communications of a third country; just pointing an antenna from their own territory towards the skies does not suffice any longer. At the same

[379] TomTom, "Real-time traffic information". http://www.tomtom.com/landing_pages/traffic_solutions/web/

[380] European Parliament, "Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))", Rapporteur: Gerhard Schmid, A5-0264/2001, 11 July 2001. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A5-2001-0264+0+DOC+PDF+V0//EN&language=EN. See also Bamford, James, *The Shadow Factory*, Anchor Books, New York, 2009, pp. 161-163.

[381] European Parliament, op. cit.

time, communication surveillance by law enforcement can also easily be avoided through the use of VoIP services such as Skype, which uses encryption algorithms that are currently considered impenetrable.[382] Finally, protesters or rioters are aware of the routine monitoring of social networks by law enforcement, and have started to warn of the usage of such media and spread the word of planned actions only by text messages sent to known friends.[383]

In this context, it is likely that law enforcement has to seek out new, smarter ways of communication surveillance. Given that the e-mail service Gmail scans its customers' e-mails for keywords and tries to find matching advertisements, it is conceivable that text messages could be scanned by the mobile telephony provider and potentially suspect messages presented to a human operator. The content of text messages could further be stored by the provider (either in plaintext or encrypted). When identical messages are being noticed in a short interval of time, indicating a possible call for public disobedience, this content would be forwarded to a human operator. As all messages have been stored, the senders and receivers would be easily found. Such "smart" communication surveillance system would not even have to be continuously turned on; it could be switched on before important political meetings, football matches or other sensitive events. Diverting all inland fibre-based communication from the telephony and Internet operators to secret services premises is another possibility; one that would allow these to eavesdrop on all the non-encrypted inland communications. Through keyword-searching algorithms and sensitivity levels set according to databases of suspected terrorists, such system could be an effective counter-terrorist measure. Using automatic universal translators (as several are under research in DARPA projects) would make it language-independent.

2.8 CONCLUSIONS AND CRITICAL PARTS

This chapter has highlighted the ways in which both current and emerging technologies are increasingly being organised into assemblages or "smart surveillance" systems, where surveillance systems are becoming integrated, multi-modal, automated, ubiquitous and increasingly accepted by the public. We have demonstrated that contemporary surveillance involves different technologies and is used in different settings, for a range of purposes. In addition to more traditional criminal justice and national security applications, we find surveillance technologies, and often systems of surveillance technologies, in public spaces, mass transit, air travel, consumer space and combined with technologies or systems associated with communication and entertainment. This means that as individuals travel back and forth to work or on errands, shop in-store or online, visit their town centre, communicate with friends and family, watch television, go on holiday, surf the Internet or even go for a hike near national borders, they are often subject to surveillance by a range of systems. As such, surveillance technologies have become part of our daily infrastructure and part of the quotidian activities that we undertake on a day to day basis. Such surveillance has "enter[ed] our daily life without notice, [and] become a common part of our socio-political and

[382] Even so, politicians and law enforcement authorities are pushing the new Internet companies to "co-operate" so that digital communications can be intercepted. See, for example, Savage, Charlie, "U.S. Tries to Make It Easier to Wiretap the Internet", *The New York Times*, 27 Sept 2010.

http://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=1&hp

[383] As, for example, the organisers of an illegal party recently did in Zurich. See Schindler, F., "Tumulte in der Zürcher Innenstadt – Polizei mit Grosseinsatz", *Tagesanzeiger*, 11 September 2011. http://www.tagesanzeiger.ch/panorama/vermischtes/Tumulte-in-der-Zuercher-Innenstadt--Polizei-mit-Grosseinsatz/story/22640435

economic relations, so that we become acclimatised or accustomed to surveillance".[384] The following chapters will develop this idea in more detail, particularly by investigating how emerging forms of surveillance are becoming pervasive in our daily lives and by examining the public's acceptance of different forms of surveillance.

Our research also demonstrates that existing and emerging technologies are becoming "smarter". Many existing surveillance systems, particularly systems that involve verification (biometrics to enable access to controlled spaces), detection and monitoring (sensors that detect explosives or other prohibited items) or information linking (credit scoring) already often involve automated decision-making and can be aggregated to identify general trends, or scaled to the level of an individual, or set of individuals, of interest. This chapter identifies automation as a particular goal of many surveillance-related research initiatives of both the EU Seventh Framework Programme and the US Defense Advanced Research Projects Agency. This trend indicates that humans will increasingly be relegated to the role of second-level decisionmakers, with a range of potential discomforts and negative impacts for individuals subject to these systems. Integrated, multi-modal systems are increasingly becoming a feature of current and emerging surveillance technologies. Currently, biometrics requires the existence of both biometric measuring algorithms *and* databases or other back-end computing systems to store and recall data. Similarly, unmanned aerial vehicles themselves are not useful for surveillance until they are fitted with cameras, sensors or other technological devices. Emerging research initiatives and technologies are set to continue this trend with systems integrating analytical algorithms with video surveillance, developing mobile sensor networks and so on.

Our review of existing and emerging surveillance shows that surveillance is becoming increasingly ubiquitous, integrated and more powerful. In the following chapters, we examine the legal regime framing surveillance, the discourse and the extent to which citizens accept the pervasiveness of surveillance. There is no doubt some surveillance yields social benefits, but equally there is no doubt that those controlling surveillance systems gain more power over those surveilled and targeted. Benjamin Goold speaks of the political dangers of surveillance and counsels that "We should resist the spread of surveillance not because we have something to hide, but because it is indicative of an expansion of state power. While individuals might not be concerned about the loss of autonomy that comes from being subjected to more and more state scrutiny, it is unlikely that many would be comfortable with the suggestion that more surveillance inevitably brings with it more bureaucracy and bigger, more intrusive government."[385] These and other issues related to smart surveillance await us.

[384] Wright, et al., op. cit., 2010, p. 344, n. 3.

[385] Goold, Benjamin J., "Surveillance and the Political Value of Privacy", *Amsterdam Law Forum*, Vol. 1, No. 4, 2009, pp. 3-6 [5]. http://www.amsterdamlawforum.org/

3 A fundamental rights analysis of smart surveillance

Mathias Vermeulen, Rocco Bellanova, Serge Gutwirth (VUB-LSTS)

Addressing 'smart' surveillance from a legal point of view is a challenging task, since there is currently no proper legal definition available for what constitutes 'smart' surveillance. It is unclear if and how such technologies are different from 'mass' or 'targeted' surveillance technologies in a security-context, and how the use of these technologies precisely affects fundamental rights. In order to provide a clearer idea about the legal frameworks that are relevant for the use of smart surveillance technologies, this contribution proceeds in three steps. Firstly we will review existing laws and principles that are relevant to the use of surveillance technologies in general. This review focuses primarily on the right to privacy and the protection of personal data, since the use of surveillance technologies is most likely to interfere with these two fundamental rights. In the second part of this contribution we will review how these laws and principles are applicable to the use of a number of smart surveillance technologies in order to assess their potential intrusiveness into a range of fundamental rights, including due process and non-discrimination. In the third and last part of this chapter we will review the ongoing legislative developments within the European Union that are relevant for smart surveillance and assess how these developments might influence the use of smart surveillance technologies.

3.1 REVIEW OF EXISTING LAWS AND PRINCIPLES APPLICABLE TO SURVEILLANCE

According to the Oxford Dictionary the word 'surveillance' was developed in the early 19th Century in France, and literally means 'watching over' something. The dictionary defines surveillance as 'close observation, especially of a suspected spy or criminal'.[386] The Cambridge Dictionary uses a wider definition and introduces another important actor besides criminals in their definition by saying that surveillance is "the careful watching of a person or place, especially by the police or army, because of a crime that has happened or is expected."[387] Surveillance is not only used to achieve a preventive goal (to deter crime), but to conduct post-facto investigations of crimes. One might get the impression from these definitions that surveillance is limited to a visual process, but it should be noted that surveillance can go beyond this visual aspect and includes interception of telecommunications ("wiretapping"), covert activities by human agents, heat-seeking instruments and other sensors, body scanners and technologies for tracking movements – to name but a few.[388] The House of Lords also makes clear that not only public actors, but also prívate actors are

[386] Oxford Dictionaries, "Surveillance," Oxford Dictionaries, http://oxforddictionaries.com/definition/surveillance.

[387] Cambridge Dictionaries, "Surveillance," Cambridge University Press, http://dictionary.cambridge.org/dictionary/british/surveillance?q=surveillance.

[388] House of Lords, "Surveillance: Citizens and the State," (London: Select Committee on the Constitution, House of Lords, 2009).

actively using surveillance technologies.[389] Privacy expert Roger Clark makes a further distinction which is helpful for this chapter. He separates the surveillance of persons in two distinct categories: 'personal' and 'mass' surveillance. The former refers to the surveillance of an identified person, and the latter category refers to the surveillance of a (large) group of people.[390]

The definitions above make clear that the use of surveillance has a strong relationship with security. The European Union has set itself as an objective to "*maintain and develop the Union as an area of freedom, security and justice, in which the free movement of persons is assured in conjunction with appropriate measures with respect to external border controls, asylum, immigration and the prevention and combating of crime."*[391] Such 'appropriate measures' include, *inter alia*, the (promotion of the) development of various surveillance and detection technologies, which can be used to prevent and combat (organized) crime, in particular terrorism.[392] The European Union, and its main 'executive' actors such as the Commission, recognizes that many of these technologies are "inherently intrusive" into privacy or can pose a challenge to freedoms and rights.[393]

In this context, the 'smartness' of surveillance can become polysemic. On the one hand, it can mean that surveillance practices are able to achieve their aims without being noticed by the person or the group that is monitored (or are much more effective at the same level of intrusiveness). On the other hand, one of the meanings of 'smart' surveillance in a legal context could rather lie in the fact that the (use of a) surveillance technology is 'privacy-proof' and/or 'data protection-proof'. Consequently it is useful to analyze the most important bodies of law concerning privacy and data protection, including in particular the requirements of the two most important instruments: the European Convention on Human Rights and the EU's Data Protection Directive.

Privacy is recognised as a right in different major international legal instruments. The Universal Declaration of Human Rights[394] establishes it in Article 12.[395] The International Covenant on Civil and Political Rights[396] devotes its Article 17 to privacy.[397] The European

---

[389] Ibid.

[390] Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms," http://www.rogerclarke.com/DV/Intro.html.. Other insights on the evolution and nature of surveillance practices can be drawn from authors such as Gary T. Marx (on the features of "new" surveillance and the evolution towards a "maximum surveillance society") Gary T. Marx, "La Société De Sécurité Maximale," *Déviance et société* 12, no. 2 (1988); Gary Marx, "What's New About the "New Surveillance"? Classifying for Change and Continuity," *Surveillance & Society* 1, no. 1 (2002)., David Lyon (on the increasing relevance of practices of "social sorting") David Lyon, ed. *Surveillance as Social Sorting. Privacy, Risk and Digital Discrimination* (London: Routledge,2003)., and Michel Foucault (the description of "*dispositifs de sécurité*", which seems particular relevant in the analysis of the function of data mining and knowledge generating systems) Michel Foucault, *Security, Territory, Population. Lectures at the Collège De France 1977-1978* (New York: Picador, 2007).For a more comprehensive introduction to surveillance and surveillance practices, please cf., *in extenso*, Chapter 1.

[391] Article 2 Treaty of the European Union (TEU)

[392] See also Article 29 TEU.

[393] European Commission, "Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and Other Security Authorities. COM(2006) 474 Final," (Brussels: European Commission, 2006), 4.

[394] Adopted and proclaimed by General Assembly resolution 217 A (III) of 10 December 1948.

[395] Art. 12: "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attack*s".

[396] Adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of 16 December 1966.

Convention of Human Rights (ECHR)[398] recognises the right to privacy in its Article 8, whose scope seeks to protect four different, not mutually exclusive, areas of personal autonomy: private life, family life, the home and one's correspondence. The Charter of Fundamental Rights of the European Union[399] explicitly recognises the right to privacy in Article 7 in the same wordings as art. 8 ECHR.[400]

The right to privacy protects the fundamental political values of democratic constitutional states as it guarantees individuals their freedom of self-determination, their right to be different and their autonomy to engage in relationships, their freedom of choice, their autonomy as regards their sexuality, health, social behaviour, and so on. It guarantees each person's uniqueness, including alternative behaviour and the resistance to power at a time when it clashes with other interests.[401] By default privacy prohibits interferences of the state and private actors in the individuals' autonomy: it shields them off from intrusions. The scope and reach of privacy are un(der)determined: it is up to judges to decide when privacy interests are at stake and when their protection can rightfully be invoked. Legislators can also intervene to protect particular privacy interests, for example through the enacting of professional secrets, the secrecy of communications or the inviolability of the home.

Art. 8 of the Charter of Fundamental Rights of the European Union recognizes the fundamental right to the protection of personal data.[402] The introduction of this article in the 2000 Charter has a long history: it was inspired by the Guidelines of the Organization of Economic Cooperation and Development governing the protection of privacy and transborder flows of personal data[403], the Convention for the Protection of Individuals with Regards to the Automatic Processing of Personal Data ('Convention 108') of the Council of Europe[404] and by EU legislation, including the EU's Data Protection Directive.[405]

Data protection is both broader and more specific than the right to privacy since it does not only aim at concretizing the protection of privacy, but simply applies every time personal data are processed. The application of data protection rules does not require to answer the question

---

[397] Art. 17: "*1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks"*.

[398] Council of Europe. European Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocol No. 11, Rome, 4 November 1950. Note that the EU must generally respect the fundamental rights as guaranteed by the ECHR by virtue of Article 6(2) of the Treaty of the European Union.

[399] OJ C 364, 18.12.2000, pp. 1-10.

[400] Art. 7: "*Everyone has the right to respect for his or her private and family life, home and communications*".

[401] Paul De Hert and Serge Gutwirth, "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power," in *Privacy and the Criminal Law*, ed. Eric Claes, Antony Duff, and Serge Gutwirth (Antwerp/Oxford: Intersentia, 2006), 70.

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

[403] The guidelines of the Organization of Economic Cooperation and Development governing the protection of privacy and transborder flows of personal data of Sep. 23 1980.

[404] Council of Europe. Convention for the protection of individuals with regard to automatic processing of personal data, European Treaty Series, no. 108 of 28 January 1981.

[405] 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, *OJ* L281/31 of 23.11.95.

of the existence of a violation of privacy: data protection applies when the conditions drawn up by the legislator are fulfilled. By default, data protection rules are not prohibitive, but they 'channel' and control the way personal data are processed: such data can only be legitimately processed if some conditions pertaining to the transparency of the processing and the accountability of the data controller are met.

Even if they are intertwined and often overlap, and even if the word 'privacy' is frequently used to mean data protection, the right to privacy and the right to data protection are separate fundamental rights, as has clearly been expressed in the Charter of Fundamental Rights of the European Union. As a consequence, a study on the fundamental rights aspects of smart surveillance should not limit its scope to data protection issues *strictu sensu* (e.g. issues related to the 'processing of personal data') but must also focus on those applications of smart surveillance that affect the fundamental values that are embodied and protected by the right to privacy, which can be affected by the processing of data that are not immediately seen as 'personal', such as traffic and location data.[406]

3.1.1 General principles on the use of surveillance technologies according to the article 8 jurisprudence of the European Court of Human rights

Rather than speaking about surveillance in general, the European Court of Human Rights has ruled that the use of a variety of specific surveillance-measures constitutes an interference with the right to private life as articulated in article 8 of the European Convention of Human Rights.[407] The past 30 years police interception of communications,[408] including the interception of messages sent to an applicant's pager,[409] the judicial interception of communications,[410] bugging of apartments,[411] the recording of voices,[412] the disclosure to the media of footage filmed in a street by closed-circuit television (CCTV),[413] video recordings of a person at her workplace without prior notice,[414] the monitoring of e-mails[415] and GPS monitoring,[416] were all found to constitute interferences with article 8. More generally, the Court has ruled that the mere storing of information relating to an individual's private life by a public authority amounts to an interference; the subsequent use of this stored information

[406] EU Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector acknowledged this for the first time on EU level by offering a degree of protection to traffic and location data.

[407] Article 8 states that:

> (1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[408] See, among others, Malone vs UK, August 1984, Series A no. 82, p. 30, § 64, Khan vs. the United Kingdom. App. N°. 35394/97, 12 May 2000.

[409] Taylor-Sabori v. the United Kingdom (App. N°. 47114/99), 22 January 2003, § 17-19.

[410] See, Kruslin vs France (App. N° 11801/85), 24 April 1994; Halford vs the United Kingdom (App.N ° 20605/92, 25 June 1997).

[411] See Affaire Vetter c. France (App. N° 59842/00), 31 May 2005, §20.

[412] Case of P.G. and J.H. v. the United Kingdom (Application no. 44787/98), 21 September 2001, §60.

[413] See Peck v. the United Kingdom (App. n° 44647/98), 28 January 2003, § XX.

[414] Admissibility decision in the case of Karin Köpke v. Germany, (App. N°. 420/07), 5 October 2010,

[415] Copland v. the United Kingdom (App. N° 62617/00), 3 April 2007.

[416] Uzun v. Germany (App. N°35623/05), 2 September 2010.

has no bearing on that finding.[417] Last but not least, the Court has indicated that such interference exists even when an individual cannot point out that they were individually subjected to it.[418]

Such an interference with the right to privacy is as such not per se illegal, according to the Convention and the Court, if the use of the surveillance measure took place in accordance with the law, pursued one or more of the legitimate aims referred to in article 8.2 of the Convention and is "necessary in a democratic society" in order to achieve the aim or aims.

Legality requirement

For measures of surveillance to be compliant with the ECHR, they must be based on a particularly precise domestic law, which has to give citizens an adequate indication of the conditions and circumstances in which the authorities are empowered to resort to such measures.[419] The law should be accessible to the person concerned, who must be able to foresee its consequences for him. When secret surveillance measures are to be used, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: (1) the nature of the offences which may give rise to the use of the measure; (2) a definition of the categories of people against whom the measures can be used; (3) a limit on the duration of the measure; (4) the procedure to be followed for examining, using and storing the data obtained; (5) the precautions to be taken when communicating the data to other parties; and (6) the circumstances in which recordings may or must be erased or the tapes destroyed.[420] The Court later added two other criteria, namely (7) the circumstances in which recordings may or must be erased or destroyed[421] and (8) the existence of either a form of judicial control or control by an independent body over the body issuing authorizations of the measure.[422] Only when these criteria are fulfilled, the Court is satisfied that domestic law provides an adequate protection against arbitrary interference with article 8. The Court has stated that it does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other.[423]

It has to be noted that the court's case-law was developed around the use of secret surveillance measures of telecommunications, and according to the Court less stringent criteria apply to the quality of laws that regulate methods of surveillance that are "neither visual nor acoustical" and that are used "to detect the perpetrator's whereabouts".[424] The court does not require that the law specifies a limit on the duration of such monitoring for instance.[425]

---

[417] Leander v. Sweden, (App. N° 9248/81), 26 March 1987; Kopp v. Switzerland, (App. N° 23224/94), 25 March 1998. Amann vs. Switzerland, (App. N° 27798/95), 16 February 2000.

[418] Klass v. Germany, (App. N° 5029/71), 6 September 1978, § 34.

[419] Weber and Saravia vs. Germany, (App. N°. no. 54934/00), 29 June 2006, § 94.

[420] Idem at § 95.

[421] Iordachi v. Moldova, (App. N°. 25198/02), 10 February 2009, § 39.

[422] Idem, § 40.

[423] Liberty vs UK, (App N° 58243/00), 1 July 2007, § 63.

[424] Uzun vs Germany, (App N°35623/05), 2 September 2010, § 68.

[425] Idem, § 69.

Since the risk of arbitrary use is especially evident when the executive exercises its powers in secret, it is understandable that stricter measures apply to the use of secret surveillance measures. However, it can be argued that the Court missed an opportunity to take into account the emerging importance of the concept of locational privacy, which may be defined as the ability of an individual to move in public spaces with the expectation that their location will not normally be systematically and secretly recorded for later use.[426] Earlier the Court has affirmed that a person's private life may extend outside a person's home or private premises. In the Perry case, the Court indicated that there is a zone of interaction of a person with others, even in a public context, which may fall within the scope of private life.[427] The Court has accepted further in a number of cases that public information "can fall within the scope of private life where it is systematically collected and stored in files held by the authorities".[428] At the same time however, the monitoring of the actions of an individual in a public place by the use of photographic equipment that does not record the visual data does not, as such, give rise to an interference with the individual's private life.[429]

"Necessary in a democratic society": The never-ending debate on proportionality

The second lid of Article 8 of the ECHR provides the possibility to restrict the right to privacy when there's a legitimate aim, such as the interest of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. In general the Court has stated that an interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are "relevant and sufficient". Regarding the notion of "necessary", the European Court of Human Rights held in the Handyside case that whilst the adjective 'necessary' is not synonymous with "indispensable", it has neither the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable".[430]

Thirty years ago the European Court of Human Rights said that States must be able, in order to counter effectively "sophisticated forms of espionage and terrorism (…) to undertake the secret surveillance of subversive elements operating within its jurisdiction".[431] But it made at the same time clear that "Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate.[432]" In the case of Malone vs UK then judge Pettitti issued a concurring opinion with the majority in which he emphasized that one of the ways in which the Court fulfilled its role was by "investing Article 8 with its full dimension and by limiting the margin of appreciation especially in those areas where the individual is more and more vulnerable as a result of modern technology".[433] More

[426] Mathias Vermeulen, "Unilateral Exceptions to Fundamental Rights in the Use of Detection Technologies in the Fight against Terrorism: Permissible Limitations of the Right to Privacy (Detecter Deliverable D4.3)," (Birmingham: University of Birmingham, 2011), 11.

[427] Perry vs United Kingdom, (App. N° 63737/00), 17 July 2003, §36.

[428] See Rotaru v. Romania, (App N°. 28341/95), 4 May 2000, § 43; Burghartz v. Switzerland, (App. N° 16213/90), 22 February 1994, § 24; Halford vs the United Kingdom (App.N ° 20605/92, 25 June 1997), §44; Amann v. Switzerland, (App. N°. 27798/95), 16 February 2000, § 44.

[429] Herbecq and the association "Ligue des droits de l'homme" v. Belgium, (App. No's. 32200/96 and 32201/96), 14 January 1998.

[430] Handyside v. United Kingdom, (App. N° 5493/72), 7 December 1976, § 48.

[431] Klass v. Germany, (App. N° 5029/71), 6 September 1978, § 48.

[432] Idem, §49.

[433] Malone vs. United Kingdom, (App N° 8691/79), 2 August 1984, Petitit concurring opinion.

recently the Court specified that the protection of article 8 would be "unacceptably weakened" if the use of modern scientific techniques in the criminal-justice system were allowed "at any cost" and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests.[434]

The Court often does not take a very close look at the potential benefits of surveillance technologies, for instance through looking at statistical data that indicate how many times a given technology was used, and to how many convictions the use of this technology was material.[435] Until now the Court has used in two cases statistical figures to criticize the proportionality of phone taps. It concluded that Bulgaria used phone tapping disproportionately after comparing the amount of tapping that the executive issued over a period of 2 years (10.000 between 1999 and 2001) with the number of warrants the UK issued in a period of 10 years (400 between 1969 and 1979). The Court reached a similar conclusion in a case against Moldova, after it obtained material that indicated that Moldova issued almost 7000 interception warrants between 2005 and 2007. Here as well the Court stated that "figures show that the system of secret surveillance in Moldova is, to say the least, overused, which may in part be due to the inadequacy of the safeguards contained in the law.[436]

The right to data protection in the ECtHR's caselaw

The European Convention on Human Rights does not have any provision explicitly referring to the protection of personal data, but the Court has been giving increased support to data protection principles developed through other instruments.[437] The ECtHR case law has notably referred to the Council of Europe Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981(Convention 108). In Z v. Finland the ECtHR noted that the protection of personal data was of fundamental importance to a person's enjoyment of his or her right to respect for private life.[438] The Court has indicated that the mere storage of data concerning an individual's private life may amount to an interference within the meaning of Article 8; the Court has taken the view that "the subsequent use of the stored information has no bearing on that finding".[439] Although the Strasbourg organs have acknowledged that the protection of personal data is an issue that can

[434] S and Marper, (App. nos. 30562/04 and 30566/04), 4 December 2008, § 112.

[435] However, it is interesting to note that the European Agency for Fundamental Rights (FRA), in its 2011 opinion on the EU PNR system proposal, has advocated for the creation of "suitable aggregate statistics" European Union Agency for Fundamental Rights - FRA, "Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Directive on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime (COM(2011) 32 Final)," (Vienna: FRA, 2011), 9. According to the Agency, such statistics would provide a solid basis to evaluate the risk of indirect discrimination and help to assess the efficiency of the PNR system. It suggests to create statistics on a) the total number of persons whose PNR data were collected and exchanged; b) the number of persons identified for further scrutiny; c) number of subsequent law enforcement actions; d) number of persons found to have been unjustifiably flagged as suspicious by the PNR system, European Union Agency for Fundamental Rights, "Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Directive on the Use of Passenger Name Record (PNR) Data for the Prevention, Detection, Investigation and Prosecution of Terrorist Offences and Serious Crime (COM(2011) 32 Final)," 9.

[436] Iordachi v. Moldova, (App. N°. 25198/02), 10 February 2009, § 52.

[437] Murphy and Ó Cuinn describe the Court's approach towards data protection as generally "very robust"; Thérèse Murphy and Gearóid Ó Cuinn, "Works in Progress: New Technologies and the European Court of Human Rights," *Human Rights Law Review* 10, no. 4 (2010): 628..

[438] Z. vs. Finland, (App. N° 22009/93), 25 February 1997. See also, notably: Rotaru v. Romania, (App. N°. 28341/95), 4 May 2000, §§ 43-44 and Amann v. Switzerland, (App. N°27798/95), 16 February 2000, §§ 65-67.

[439] Leander v. Sweden, (App. N° 9248/81), 26 March 1987; Kopp v. Switzerland, (App. N° 23224/94), 25 March 1998. Amann vs. Switzerland, (App. N° 27798/95), 16 February 2000.

fall within the scope of Article 8 ECHR, they have never held that all aspects of the processing of personal data are worthy of protection under the right to privacy.[440]

3.1.2 General principles on the use of surveillance technologies in EU law

While the European Court of Human Rights has dealt with the protection of personal data as an integral part of the right to privacy, at EU level the right to data protection is seen as an autonomous right[441]: personal data are protected by the law even if the right to privacy is not at stake.[442] Or, as article 8 of the Charter of Fundamental Rights, unambiguously states: "everyone has the right to the protection of their personal data".[443] This right does not prohibit processing of personal data, but formulates the conditions under which it is legitimate. Such data must be processed fairly for specified purposes[444] and on the basis of the consent of the person concerned or some other legitimate basis lay down by law. Everyone has the right of access to data that has been collected concerning him or her, and the right to have it rectified. Last but not least, the compliance of these rules has to be subjected to control by an independent authority.[445]

Since the adoption of the Lisbon Treaty the provisions of the Fundamental Rights Charter will have direct effect. Importantly, the new article 16 of the Treaty on the Functioning of the European Union (TFEU) duplicates article 8.1 in the body of the TFEU as a provision of general application: it applies to all processing of data within the EU[446], be it in the private sector or the public sector, including the former third pillar. Article 16 TFEU obliges the European Parliament and Council to lay down rules on data protection in all areas of European Union law. It remains to be seen of course whether this provision will be used to include the fundamental principles of data protection into one comprehensive legal framework.

The Data Protection Directive

Before the Charter of Fundamental Rights was adopted all European Member states had already implemented the more detailed Data protection Directive,[447] which aimed to

---

[440] On the ECtHR assessment of the relation between the right to privacy as established by Article 8 of the ECHR and the protection of personal data, see also: I v. Finland, (App. no. 20511/00), 17 July 2008 (in particular, §§ 35, 38 and 40).

[441] See the judgment of the ECJ in the Promusicae case. Case C-275/06, Promusicae, [2008] ECR I-271, para 63. Elevating the right to data protection as an autonomous right has not been uncontroversial. See for instance: Lucas Bergkamp, "EU Data Protection Policy. The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy in an Information-Driven Economy," *Computer Law & Security Report* 18, no. 1 (2002): 33..

[442] Joined cases C-465/00, C-138 & 139/01, Österreichischer Rundfunk and Others, [2003] ECR I-4989.

The Court furthermore recalled that the expression private life must not be interpreted restrictively and that there is no reason of principle to justify excluding activities of a professional nature from the notion of private life.

[443] Article 8.1 Charter of Fundamental Rights.

[444] The purpose specification principle can be seen as equivalent to the requirement of foreseeability as an element of the quality of law test of Article 8.2 ECHR. See Opinion of the General Advocate J. Kokott, 18 July 2007, ECJ Case C-275-06, point 53.

[445] Article 8.2 Charter of Fundamental Rights

[446] However, Protocol 22 to the Treaty makes clear that the UK, Ireland and Denmark will not always be bound by the rules laid down on the basis of article 16. Protocol No. 22, O.J. 2008 C 115/299.

[447] 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, OJ L281 of 23.11.1995, p. 31

harmonize the different national rules on the protection of personal data[448], and which included more details on the conditions for the processing of personal data. A first cluster of conditions related to the quality of the data. Personal data (1) must be processed fairly and lawfully; (2) should be collected for specified, explicit and legitimate purposes, and not further processed in a way incompatible to those purposes;(3) should be adequate, relevant, and not excessive in relation to the purposes for which they are collected and/or further processed;(4) accurate, up to date, and (5) kept for no longer than is necessary for the purposes for which they were collected or processed.[449] Personal data may be processed only if the data subject has given his consent; or if processing is necessary for the performance of a contract to which the data subject is party.[450] According to the Directive, Member States have to prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life, but has a limitation clause, which states, inter alia, that this prohibition does not apply if the data subject has given his explicit consent to the processing of those data,[451] or the processing relates to data which are manifestly made public by the data subject.[452] Furthermore, the Directive requires that information should be provided to the data subject,[453] and establishes a right to access to data[454] and a right to object.[455]

Importantly, Article 15 grants a person the right "not to be subject to a decision[456] which produces legal effects concerning him or significantly affects him and which is based solely[457] on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc". According to Bygrave article 15 does not seem to prohibit automated profiling: "It just directs each EU Member State to confer on persons a right to prevent them being subjected to such decision-making".[458] This would imply that as long as this right is not exercised, the automated decision-making process is not illegal. But in this reasoning the legitimacy of a purely automated decision would seem to be dependent of the *implicit* consent of the concerned subject: if you do not object, you consent, and you thus make the automated decision legitimate. This position is hard to maintain, because the main problem with automated decisions is precisely that the individual is *not* consulted, and it is also sharply at odds with the Directive's understanding of 'consent' as a 'freely given specific and informed indication

[448] Article 2(a) of the Data Protection Directive (DPD) clarifies that 'personal data' means "any information relating to an identified or identifiable natural person ('data subject'); 'an identifiable person' is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity". On the notion of personal data, cf. Article 29 Data Protection Working Party, "Opinion 4/2007 on the Concept of Personal Data," (Brussels: Article 29 Data Protection Working Party, 2007)..

[449], Article 6

[450] DPD, Article 7.

[451] Idem, Article 8(2)1.

[452] Idem, Article 8(2)5.

[453] Article 10.

[454] Article 12.

[455] Article 14.

[456] Such a 'decision' would also include the (automated) logical processes of computer software. Cf. Lee A. Bygrave, "Minding the Machine: Article 15 of the Ec Data Protection Directive and Automated Profiling," *Computer Law & Security Report* 17(2001): Lee A. Bygrave (2001), "Minding the machine: Article 15 of the EC Data Protection DirectiveDirective and Automated Profiling", Computer Law & Security Report, No. 17, pp. 17-24..

[457] This notion seems to refer to a situation in which a person fails to actively exercise any real influence on the outcome of a particular decision-making process. Idem.

[458] Idem.

of his wishes'. The Belgian legislator, for example, has understood the Directive in the same way since the Belgian law on data protection, implementing the Directive, uses unambiguously prohibitive wordings:

> "A decision resulting into legal effects for a person or affecting him seriously, may not be taken purely on the basis of automatic data processing that is destined for the evaluation of certain aspects of his personality. The prohibition laid down in the first section is not applicable if the decision is taken in the context of an agreement or if it has its ground in a provision laid down by or by virtue of a law, decree or ordinance. In such agreement or provision appropriate measures shall be taken for the protection of the legitimate interests of the data subject. At least he shall be allowed to bring up his standpoint in a useful way".[459]

In Chapter III the Data Protection Directive provides for the judicial remedies to be made available to every person that his rights have been breached[460] and envisages the possibility of compensation for the damage suffered.[461] The Directive regulates the transfer of data to third countries, which is permitted if the third country in question ensures an adequate level of protection.[462] Finally, it stipulates that each Member State has to set up a supervisory authority responsible for monitoring the compliance within its territory with the provisions of the Directive.[463] The European Commission is currently revising the Directive and will propose new legislation in 2011 (cf. infra, section 3.2).[464]

Data protection in the area of freedom, justice and security

Directive 95/46/EC is meant as a general legal framework, which can be complemented by specific regimes for data protection for specific sectors. The Data Protection Directive does not apply to the processing of personal data "concerning public security, defense, State security, and the activities of the State in areas of criminal law,[465] even after the entering into force of the Lisbon Treaty which introduced article 16 TFEU. Article 10 of Protocol No. 36 on transitional provisions provides that the legal effects of all acts adopted before the entry

---

[459] Art. 12 bis of the consolidated text of the Belgian law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data as modified by the law of December 11, 1998 implementing Directive 95/46/EC -- *Unofficial English translation by K. Buyens, updated by Mieke Loncke*, cf.: http://www.law.kuleuven.ac.be/icri/documents/12privacylaw.php). See also: Wim Schreurs et al., "*Cogitas, Ergo Sum*. The Role of Data Protection Law and Non-Discrimination Law in Group Profiling in the Private Sector," in *Profiling the European Citizen*, ed. Mireille Hildebrandt and Serge Gutwirth (Dortrech: Springer, 2008), 254-55..

[460] Article 22.

[461] Article 23.

[462] Articles 25 and 26. Cf., *in extenso*: Article 29 Data Protection Working Party, "Working Document: Transfers of Personal Data to Third Countries: Applying Articles 25 and 26 of the EU Data Protection Directive," (Brussels: Article 29 Data Protection Working Party, 1998)..

[463] Article 28.

[464] In November 2010 the Commission issued a communication on the issue, outlining a range of broad principles which it would take into account during the revision; European Commission, "Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A Comprehensive Approach on Personal Data Protection in the European Union," (Brussles: European Commission, 2010)..

[465] Article 3(2). The European Court of Justice has clarified that the exception of Article 3 (2) applies only to the activities which are expressly listed there or which can be classified in the same category. Case C-101/01 Bodil Lindqvist [2003] ECR I-12971. O.J. 2008, L 350/60. But at the same time it held in the PNR judgment that Article 3(2) is also applicable when the transfer of data "falls within a framework established by the public authorities that relates to public security". Such a framework might include activities undertaken by private actors. Joined cases C-317 & 318/04, European Parliament v. Council and Commission, [2006] ECR I-4721 at 58.

into force of the Lisbon Treaty shall be preserved, until the acts are repealed, annulled or amended. This includes the 2008 Council Framework Decision on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters,[466] even if it may currently be at odds with article 16 TFEU.[467]

The Framework decision mirrors generally the provisions of the data protection Directive.[468] Thus, it provides for the principles of lawfulness, proportionality and purpose limitation for the collection and the processing of personal data by the competent authorities;[469] the rectification, erasure and blocking of data;[470] the rights of the data subjects, such as the right of access,[471] the right of rectification, erasure or blocking,[472] the right to compensation;[473] and, the establishment of national supervisory authorities, responsible for advising and monitoring the application of the framework decision within the territory of each Member State.[474] It is important to note that the Framework Decision applies only to personal data that are exchanged within the framework of police and judicial cooperation between Member States for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. The Decision therefore does not cover the collection and processing of personal data at a national level, when personal data originate within the Member State which uses them. Specific conditions on the use of personal data which were established by acts adopted in the former third pillar take precedence over the provisions of the Framework Decision as well. As a result, the current situation in the former third pillar can be described as "a patchwork of data protection regimes", which are applicable in different situations.[475]

The most important article of the 2008 Council Framework Decision for the purposes of this article, is article 7, which states clearly that "a decision which produces an adverse legal effect for the data subject or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to the data subject shall be permitted only if authorised by a law which also lays down measures to safeguard the data subject's legitimate interests." As we will see, many of the smart surveillance technologies described below focus exactly on automated recognition of individuals, or specific actions of individuals. Still, it remains unclear what "measures" could be envisaged by the legislator, and which 'legitimate interests' of the data subject should be protected.

---

[466] Council Framework Decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters

[467] See for instance: H. Hijmans and A. Scirocco, "Shortcomings in EU Data Protection in the Third and the Second Pillars. Can the Lisbon Treaty Be Expected to Help?," *Common Market Law Review* 46(2009)..

[468] For a thorough overview of the Framework Decision, cf. Paul De Hert and Vagelis Papakonstantinou, "The Data Protection Framework Decision of 27 November 2008 Regarding Police and Judicial Cooperation in Criminal Matters – a Modest Achievement However Not the Improvement Some Have Hoped For," *Computer Law & Security Review*, no. 25 (2009)..

[469] Article 3.

[470] Article 4.

[471] Article 17.

[472] Article 18.

[473] Article 19.

[474] Article 25.

[475] Cf. Article 29 Data Protection Working Party and Working Party on Police and Justice, "The Future of Privacy. Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data," (Brussels: Article 29 Data Protection Working Party, 2009), 8.

The E-Privacy Directive

Directive 2002/58/EC62 concerning the processing of personal data and the protection of privacy in the electronic communications sector (the 'e-Privacy Directive') complements the provisions of the Data Protection Directive and creates de facto a specific regime of data protection.[476] Article 5(1) obliges Member States to ensure the confidentiality of communications and the related traffic data through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorized to do so. Furthermore, traffic data relating to subscribers and users processed and stored by the provider of a public communications network must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication.[477]

However, here we find a limitation clause for state security purposes as well. Article 15 enables Member States to adopt legislative measures to restrict the scope of the rights provided for in the Directive "when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system". The Data Retention Directive (see below) added a new paragraph 1(a) to article 15 which stated that this article shall not apply to data specifically required Article 1(1) of that Directive.[478]

The Data Retention Directive

In 2006 the Data Retention Directive was adopted at EU level.[479] There was quite some disagreement about the legal basis on which the Directive was founded, but the European Court of Justice held that it was adopted on the appropriate basis since both its aim and its content fell under article 95 EC.[480] Its aim was to harmonize Member States' provisions concerning the obligations of the providers of publicly available electronic communications services and public communications networks to the retain certain data which are generated or processed by them, in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious[481] crime (…), as defined by each Member State in its national law.[482] The categories of data to be retained are laid down in Article 5 of

[476] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L201 of 31.07.2002, p.37.

[477] Article 6.

[478] Cf. Eleni Kosta and Peggy Valcke, "Retaining the Data Retention Directive," *Computer Law & Security Report* 22, no. 5 (2006)..

[479] Directive 2006/24/EC of the European Parliament and the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, OJ L 105 of 13.4.2006

[480] Case C-301/06 Ireland v. European Parliament and Council, Judgment of the Grand Chamber of 10 February 2009, § 57.

[481] The use of the term 'serious' has been criticized as being too vague. Cf., for instance, the report of the House of Lords European Union Committee, which notes that: "It may be difficult to draw a satisfactory line between serious and less serious crime, and a regular pattern of smaller crimes may sometimes amount to serious crime…"; House of Lords, "After Madrid: The Eu's Response to Terrorism. Report with Evidence," (London: House of Lords, European Union Committee, 2005), 18.

[482] Article 1(1).

the Directive. They consist of: (a) data necessary to trace and identify the source of a communication; (b) data necessary to identify the destination of a communication; (c) data necessary to identify the date, time and duration of a communication; (d) data necessary to identify the type of communication; (e) data necessary to identify users' communication equipment or what purports to be their equipment; and (f) data necessary to identify the location of mobile communication equipment. No data revealing the content of the communication may be retained[483], only traffic and location data.[484] The Directive stipulates further that the retention period will be between six months and two years starting from the date of the communication (Article 6). However, a Member State facing particular circumstances may request an extension of the maximum retention period. In this case, it is obliged to notify the Commission and inform the other Member States of the measures taken and state the grounds for introducing them (Article 12).

Article 6 contradicts the principled position of article 8 of the Data Protection Directive as it states that "the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership and the processing of data concerning health or sex life shall be permitted only when this is strictly necessary and when the national law provides adequate safeguards". This was one of many reasons that made the (implementation of) the Directive controversial. Various court cases have emerged on the national level, which took decisions that ranged from annulling orders that provided police forces with retained data[485] to declaring the laws that implemented the Directive unconstitutional in their entirety.[486] The data retention Directive is currently being reviewed (cf. infra, section 3.3).

3.2 REVIEW OF EXISTING LAWS AND PRINCIPLES APPLICABLE TO SURVEILLANCE

The Sapient project defines a smart surveillance system as "being capable of extracting application-specific information from captured information (be it digital images, call logs or electronic travel records) in order to generate high-level event descriptions that can ultimately be used to make automated or semi-automated decisions." To explore the legal dimension of these technologies, we will analyze different examples of 'smart surveillance', which can be grouped into three categories.[487]

The first category of smart surveillance technologies relates to the emergence of new image analysis algorithms in CCTV-systems which enable their automated operation, for instance by

[483] Article 5 (2).

[484] For definitions of location and traffic data see articles 2(b) and 2(c). For a better understanding of 'traffic data', and how this can easily be seen as personal data in an online setting, cf. Caroline Goemans and Jos Dumortier, "Enforcement Issues: Mandatory Retention of Traffic Data in the EU: Possible Impact on Privacy and Online Anonymity," in *Digital Anonymity and the Law. Tensions and Dimensions*, ed. Chris Nicoll, Corin Prins, and M. J. M. van Dellen (The Hague: T.M.C. Asser Press, 2003).

[485] EDRI, Data retention law provisions declared unlawful in Cyprus, 9 February 2011, available at http://www.edri.org/edrigram/number9.3/data-retention-un-lawful-cyprus.

[486] Romania, Constitutional Court Decision no.1258, 8 October 2009, available at http://www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention.html; Germany, Vorratsdatenspeicherung [Data retention] BVerfG 2 March 2010, 1 BvR 256/08. Available at: http://www.bundesverfassungsgericht.de/entscheidungen/rs20100302_1bvr025608.html. For a detailed analysis of the latter case, cf. de Vries, 2011 #14}

[487] Cf. David Wright et al., "Sorting out Smart Surveillance," *Computer Law & Security Review* 26, no. 4 (2010): 343-54..

adding extra analytical tools to CCTV camera's which detect 'suspicious' objects or 'suspicious' behavior. An operator would only be alerted when such an activity takes place.
A second category of smart surveillance technologies relates to the inclusion of new sensor systems that go beyond visual surveillance. A case in point here are 'smart meters' in private homes, which measure individual power use and send these data to a central server. Such data may reveal for instance huge energy consumption (such as infrared lamps used in growing marijuana plants) or indicate times when a user is at home. Another example would be the use of body scanners in airports, which allow the detection of certain concealed items.
A last category of 'smart surveillance' tools consist of new data integration capabilities with advanced profiling and data mining techniques. So called 'interoperable' databases that allow to cross-reference 'traditional' surveillance methods with multiple 'heterogeneous' sources are an example here. Another example are systems able to generate knowledge out of an incoming set of data, both by matching these data against pre-determined (external) profiles, and by using the incoming data to update existing profiles and generate new one (not only external, but also "internal"). Measures such as the passengers profiling schemes designed in the EU-US and EU Passenger Name Records proposals are relevant examples.

3.2.1 Fundamental rights aspects of new image analysis algorithms in smart CCTV systems

A number of FP7 projects are currently developing smart surveillance systems which automatically detect user-defined[488] 'threats' or 'abnormal behaviour' in public places. The system will alert then the CCTV operator who has to decide if any and if so what actions to take. As such, these smart surveillance technologies primarily aim to tackle the information overload that data controllers are subjected to by alerting them to potentially interesting information. Hereby a third function is added to the use of CCTV cameras: CCTV cameras are not only used as a deterring measure against crime or as a post-facto investigative tool, but they can also be used for preventive purposes.

We will discuss two main projects in this chapter: ADABTS (Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces)[489] and INDECT (Intelligent information system supporting observation, searching and detection for security of citizens in urban environment).[490] Where relevant we will also discuss the SAMURAI (Suspicious and Abnormal behaviour Monitoring Using a netwoRk of cAmeras & sensors for sItuation awareness enhancement) project.[491] The decision to select these three P7 projects was based on various European news reports that these three projects were engaging in fundamental-rights intrusive activities.[492]

All three projects have similar aims. The ADABTS project aims to "facilitate the protection of EU citizens, property and infrastructure against threats of terrorism, crime and riots by the

[488] For a general technical overview, cf. Arun Hampapur et al., "Smart Surveillance: Applications, Technologies and Implications," *Information, Communications and Signal Processing* 2(2003)..

[489] For more info see https://www.informationsystems.foi.se/~adabts-fp7

[490] For more info see http://www.indect-project.eu/

[491] For more info see http://www.samurai-eu.org

[492] Wilmer Heck, "EU to Monitor Deviant Behavior in Fight against Terrorism," *Der Spiegel*, 21.10.2009 2009; Ian Johnston, "EU Funding 'Orwellian' Artificial Intelligence Plan to Monitor Public For "Abnormal Behaviour"," *The Telegraph*, 09.12.2011 2009.. See in general: Ben Hayes, "Neoconoption - the EU Security-Industrial Complex," (London: Statewatch, 2009)..

automatic detection of abnormal human behaviour".[493] On the basis of the use of "video and acoustic sensors" ADABTS plans to create models that will enable the 'prediction of the evolution of behaviour, so that potentially threatening behaviour can be detected as it unfolds, thus enabling pro-active surveillance".[494] INDECT's ambitious aim is to design a system which enables the 'intelligent' processing of "all information and automatic detection of threats and recognition of abnormal behavior or violence". It specifies that this includes the "intelligent monitoring of objects and urban areas for the purpose of automatic detection of (potential) threats related to crime, terrorism and violent acts".[495] Also SAMURAI wants to create an "intelligence surveillance system for monitoring people and vehicle activities" especially at critical infrastructure locations. By "improving these current CCTV systems" the main social impact of SAMURAI according to the project will be the "increased public confidence in security systems in public places".[496]

On the basis of a list of indicators of a threat or 'abnormal behaviour' the CCTV operator is alerted. The FP7-projects stress in various forms that these indicators are provided by the end-users (the police, or a public authority) or on the basis of 'objective scientific analysis'. INDECT loosely defines 'abnormal behaviour' as behaviour which is 'potentially dangerous to society', or 'related to crime', such as 'the using of knifes or guns, or unattended luggage in public places'. This aspect of smart-surveillance seems to be less problematic, since it only tries to detect and or track potentially dangerous tools in public places. But INDECT also tries to detect potentially dangerous situations and behaviour on the basis of parameters that are set by the end-users of the project i.e police departments. After some criticism in the press and even the European Parliament[497] INDECT was keen to point out that it did not introduce the terms 'suspicious' or 'abnormal' behavior.[498] ADABTS identified the needs of various end-users through interviews with not only police, but also CCTV operators and security managers in airports, town centers, shopping malls, football stadia.[499] It further made an effort to identify "objective data on abnormal behavior" based on concepts for instance from clinical psychology.[500] Distinct and visible behaviour, such as all "whole-body behaviours (including movement about a space, excessive body gestures or gait)", were identified as well as behaviours that are "less obvious (such as signs of stress, rapid eye movements, blinking, mumbling and perspiration)".[501]

Both ADABTS and INDECT add microphones to CCTV cameras in order to achieve these aims. In INDECT a CCTV-operator will automatically be alerted when 'dangerous sounds' are heard, such as "gunshots, explosions, screams, crying for help in European languages,

[493] Enterprise and Industry European Commission, "Dg Enterprise and Industry, Towards a More Secure Society and Increased Industrial Competitiveness - Security Research Projects under the 7th Framework Programme for Research, Security," (Brussels: European Commission, 2009), 6..

[494] Idem.

[495] Idem at 52.

[496] Idem at 70.

[497] The past two years more than 20 written questions have been asked by MEP's about this project in the European Parliament.

[498] D0.6 Indect at p.21. It states that "in our case we clearly understand abnormal behaviour as "criminal behaviour", and especially as "behaviour related to terrorist acts, serious criminal activities (e.g.: murders, bank robberies, someone leaving the luggage in the airport with the bomb) or criminal activities in the Internet (e.g.: child pornography). We will produce the tools to avoid such situations."

[499] ADABTS WP 2 p.7.

[500] ADABTS, D3.1 p.2.

[501] ADABTS, D3.1 p.

breaking glass".[502] One of the features of the ADABTS project is that CCTV cameras would also be able to analyze the pitch of people's voices as this might be an indicator of 'abnormal behaviour'.[503] The SAMURAI project does not use or records sounds as it uses camera's from medium and long range distance, and differs further from INDECT and ADABTS in that it not only uses CCTV camera's, but also aims to employ "networked heterogeneous sensors" i.e positioning sensors and wearable audio or video sensors.[504]

ADABTS and INDECT are keen to stress that they are just "research projects" and can in no way be held responsible for the exact application of their technologies. INDECT stresses that if EU Member States want to use this type of technology, they must comply with all relevant EU fundamental rights.[505] ADABTS has a "legal and ethical part" of the "user needs work package", but its legal and ethical analysis similarly only covers the legal and ethical restrictions on its tests and research-activities, and does not go dig deeper into the legal implications of the use of their new surveillance technologies. According to ADABTS, their research fits better into the category of "scientific (visual) ethnographic or anthropological studies" rather than surveillance, since they are using video data only for research purposes and "the immediate intention is not the prevention of crime or improvement of security.[506]"

Data protection principles

Applying European data protection principles to the use of these smart surveillance technologies is not obvious for two reasons. The Data Protection Directive is not applicable to data processing with the purpose of crime prevention, which is the main rationale for the use of these new surveillance technologies. Equally, as already stated above, the 2008 Framework Decision does not cover the collection and processing of personal data at a national level, which leaves the regulation of these new technologies predominantly as a matter of domestic data protection law which has subtle differences among different jurisdictions. In a few countries the processing operations performed for security purposes are for instance also subject to safeguards as outlined with Council of Europe Convention no. 108/1981.

On the European level the Working Part 29 has asserted that the principles of the Data Protection Directive apply to any information – including sound and image information – concerning "an identified or identifiable person", by any type of surveillance technology.[507] INDECT assures that personal data such as "the faces of persons, or care plate numbers" are anonymized through encryption. According to INDECT, this enables the CCTV-operator to review events "without violating privacy rights."[508] While this kind of anonymization is to be preferred from a privacy point of view, it must be noted that this type of information is still considered as personal data, since the image can be de-anonymized by a public authority for the purposes of investigating a crime for instance.[509] Since ADABTS assume that the images

[502] Indect deliverable 6.01, p.12.

[503] Source?

[504] Adabts D3.1 at 40.

[505] Indect deliverable 6.01

[506] ADABTS WP2 at 68.

[507] Cf. Article 29 Data Protection Working Party, "Opinion 4/2004 on the Processing of Personal Data by Means of Video Surveillance," (Brussels: Article 29 Data Protection Working Party, 2004), 15..

[508] Indect Deliverable 0.6 p.12.

[509] The WP 29 states that identificability within the meaning of the Directive may also result from matching the data with information held by third parties, or else from the application, in the individual case, of specific techniques and/or devices; Article 29 Data Protection Working Party, "Opinion 4/2004 on the Processing of Personal Data by Means of Video Surveillance," 15..

of its cameras will be "good enough to identify the persons in the scene" it will always trigger data-protection concerns.[510] Furthermore, it is reasonable to assume that images would not qualify as 'personal data' if the subjects are generally not identifiable due to insufficient original image quality.

If personal data is processed, it has to be done in accordance with the national law of the country where it is used. The Article 29 points out that the data controller must be aware that certain public functions may only be exercised under the law by specific, non-administrative bodies such as, in particular, law enforcement agencies.[511] This is of importance, since the end-users of these smart surveillance technologies consist of a much bigger group than such agencies. INDECT and ADABTS make it clear that various private actors could be interested in their technologies.

As regards the limitation of purposes, the deployment of these systems should first be limited to cases where alternative means and/or security measures prove clearly insufficient or inapplicable in view of the purposes of the processing. [512] The Article 29 WP has pointed out that surveillance performed on "grounds of actual public security requirements, or else for the detection, prevention and control of criminal offences" should respect the requirements of Article 8 ECHR. In particular, it points out that the use of such measures has to be proportionate "to the prevention of concrete risks and specific offences – e.g., in premises that are exposed to such risks, or in connection with public events that are likely reasonably to result in such offences."[513] As a matter of best practice it can be pointed out that the Italian guidelines on video surveillance point out that the use of these systems should be limited to situations where there is "actual, proportionate requirements concerning prevention or suppression of concrete, specific dangers as impending on a good – this is the case, for instance, of premises exposed to actual dangers or events that can reasonably produce prejudicial effects." This for instance leads this authority to conclude that "it is unlawful to perform pervasive video surveillance of whole areas in a city – perhaps imaged in full and without intermission in the absence of adequate requirements e if the conditions referred to above are not fulfilled".[514]

In order for the data processing to be proportionate, the collection of personal data should be limited to what is necessary to achieve the purpose for which the data are gathered and further processed. The technology used should be adequate in respect of the purposes sought, which entails a sort of 'data minimization' duty on the controller's part.[515] The three FP7-projects mentioned here would only alert the operator to 'suspicious events', 'normal' behavior would not be noticed or stored.[516] Indect for instance states that their technology will not be used for "mass surveillance" purposes – "only for cases where justified reasons for interfering with the exists". As such, these surveillance systems are even more targeted – or 'smarter' than 'normal' surveillance technologies.

Right to privacy

[510] Adabts WP2 at 69.

[511] Article 29 WP, 2004 opinion, pp.16-17.

[512] Article 29 WP, 2004 opinion, p.18.

[513] Article 29 WP, 2004 opinion p.13.

[514] As quoted in Fanny Coudert, "When Video Cameras Watch and Screen: Privacy Implications of Pattern Recognition Technologies," *Computer Law & Security Review* 26, no. 4 (2010): at 382.

[515] Article 29 WP, 2004 opinion, at 19.

[516] Check source.

A key feature of smart surveillance techniques is that they are used to monitor identifiable persons as they are moving in public places (or at least in publicly accessible premises). According to the Article 29 WP, such an individual in transit may well expect a lesser degree of privacy, "but not expect to be deprived in full of his rights and freedoms as also related to his own private sphere and image.[517] The European Court of Human Rights has earlier indicated that camera surveillance in public places where no visual data is recorded does not as such interfere with the individual's private life.[518] Only when materials obtained through such devices are made public in a manner or degree beyond that normally foreseeable an interference with the right to privacy can occur.[519]

On the basis of these precedents it seems that the right to privacy is only triggered to the extent it protects personal data. However, it could also be argued that the use of these systems might affect underlying goals of the right to privacy such as the protection of dignity and the preservation of individual autonomy, which ensure a person is able to exercise other fundamental rights.[520] Freedom of expression and the right to association for instance all require privacy to be able to develop effectively.[521] Goold for instance stresses the political value of privacy by saying that "without privacy, it is much harder for dissent to flourish or for democracy to remain healthy and robust".[522] This is an important point to make since the right to privacy is quite often only described in individualistic terms, which makes it an easy target for proponents of 'balancing' privacy with the greater societal good of security. It might be argued that this political value of privacy might be affected by the abuse of smart surveillance technologies. It would not require much imagination to see the potential of such technologies for authoritarian regimes, which could use it to detect and respond to any early sign of protest.

Right of non-discrimination

Central to the use of smart surveillance technologies is the ability to sort one group or person from another, so that they can be treated differently. Since 9/11 there has been for instance a clear move to categorize people on the basis of the potential threat they might pose.[523] As such, the use of these smart CCTV-systems resembles very closely so-called 'predictive data-mining', which aims to predict events based on patterns or 'classifiers' that were determined using known information.[524]

The ADABTS project has conducted research into such indicators, or classifiers for abnormal behavior or threatening activities such as fighting or pick-pocketing. According to the project there seem to exist some behavioral patterns that can indicate future abnormal and threatening

[517] Art 29 WP 2004, p.5

[518] Perry vs United Kingdom, (App. N° 63737/00), 17 July 2003, §38.

[519] Peck v. the United Kingdom (App. n° 44647/98), 28 January 2003, §62: "to an extent which far exceeded any exposure to a passer-by or to security observation".

[520] source

[521] Cf. the report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin. UN Doc A/HRC/13/37, 28 December 2009, at § 33.

[522] Benjamin J. Goold, "Surveillance and the Political Value of Privacy," *Forum American Bar Association* 4, no. 1 (2001): 5.

[523] Security practices such as the full digitalization of the analysis of all US-bound Passenger Name Records, or the establishment of no-fly and black lists are explicit examples of this trends towards "social sorting", cf. *in extenso*: Lyon, ed. *Surveillance as Social Sorting. Privacy, Risk and Digital Discrimination*..

[524] Schermer, 2011, 46

behavior with "sufficient accuracy."[525] Nevertheless, ADABTS points out that the qualification of behavior as 'abnormal' is different for different times, locations, cultures or types of threat.

> "Specific abnormal behaviour when focusing on terrorism can, for example, be mumbling prayers, or buying a one way ticket at an airport. Then again, specific abnormal behaviour when focusing on pick pocketing can be a person stepping into the back of a line, leaving when standing in the middle of the line and getting in the back of the line a little while later."[526]

The behaviors extracted can also not be seen to be complete without 'supplementary appearance indicators' – the way the person dresses for instance.[527] ADABTS contends further that the decision on the response to an actual or potential threat can only be assessed when a "combination of abnormal behaviours, either observed together or sequentially" are perceived.[528]

When the classification of a situation of a person as 'abnormal' is dependent on such a wide variety of factors, the accurate classification of situations and persons becomes extremely difficult, if not impossible. Even more, there exists a risk that the use of certain indicators can amount to discrimination by singling out individuals or social groups for adverse treatment on the basis of incorrect or misleading assumptions.[529]

Article 14 of the European Convention stipulates that: "[the] enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status".

Despite the fact that this article does not contain a general prohibition of discrimination[530], the existence of the 'or other status' formulation indicates that the application of this prohibition of discrimination is virtually unlimited.[531] For this non-discrimination provision to apply, a person or a group of persons needs to show that they are subject to a difference in treatment without there being an objective and reasonable justification compared to another person or a group in an analogous situation. No difference in treatment which is based exclusively or to a decisive extent on a person's ethnicity for instance would be justifiable.

However, it is also possible that apparently neutral or objective criteria, such as specific movements, are used as classifiers in smart CCTV programs, which in practice would disproportionally affect the right to privacy of individuals of a specific group. For instance,

---

[525] Adabts WP02, p.111.

[526] ADABTS, D3.1, p. 20.

[527] ADABTS D3.1 at p. 6.

[528] ADABTS, D3.1, p. 2.

[529] House of Lords, "Surveillance: Citizens and the State," 14..

[530] An additional protocol, Protocol 12, has also been drafted and has been ratified by 17 member states of the Council of Europe (Albania, Andorra, Armenia, Bosnia, Croatia, Cyprus, Finland, Georgia, Luxembourg, Montenegro, the Netherlands, Romania, San Marino, Serbia, Spain, Macedonia and Ukraine). This protocol states that "any right set forth by law" (as opposed to the rights in the Convention) shall be secured without discrimination.

[531] Article 21(1) of the Charter of Fundamental Rights of the European Union adds explicitly that discrimination on the basis of genetic features, disability, age or sexual orientation are prohibited as well. Article 21(2) prohibits discrimination on the basis of national origin "within the scope of application of the Treaty establishing the European Community and of the Treaty on European Union".

discrimination might occur if a smart CCTV-camera alerts an operator frequently on the basis of suspicious movements which are in fact linked to practicing a specific faith.

Presumption of innocence as an element of the right to fair trial

Finally, we briefly have to observe the impact that the use of these smart technologies have on the presumption of innocence. Article 6(2) of the European Convention of Human Rights makes clear that this essential principle of the right to fair trial applies only to those persons which are *charged with a criminal offence.* Therefore – in a legal sense – this principle refers only to a procedural guarantee in the context of criminal trials. This concept is relevant however when discussing the features of smart surveillance technologies. As Bygrave has noted humans attach a lot of weight to the "apparently objective and incontrovertible character" of the results a specific technology produces. Bygrave fears that humans are too prone to accept the validity of decisions made by technologies at face value, thereby abdicating their own investigatory and decisional responsibilities.[532] This could have implications for 'false positives' for instance, where persons suspected of trying to commit a crime will have to convince security officers that they did not have such an intention. Lastly, even the ADABTS project notes that "video surveillance and other forms of informational surveillance could provide the feeling that everybody is guilty until proven innocent, which could mean a considerable interference with personal freedom".[533]

3.2.2 Fundamental rights aspects of new sensor systems: the case of body scanners

A second category of smart surveillance technologies relates to the inclusion of new sensor systems that go beyond visual surveillance, and which are able to detect more concealed issues such as huge energy consumption (in the case of smart meters) or hidden explosives (in the case of body scanners). We chose to focus on the use of body scanners, because an analysis of this technology is more relevant from a security point of view. The main fundamental rights problem with smart meters seems to be the centralization of data that reveals personal energy consumption, which discloses the attributes and behavior of a person or a group of persons.[534] Every 15 minutes the energy consumption of a house is transferred to a third party (often the so called distribution systems operator), which might disclose for example when people get up in the morning, when they go to sleep, when they are at home. A smart meter would enable the systems operator to remotely control functionalities of the meter.[535] Relevant in a security context is that the centralization of such information could be an interesting target for burglars (who could learn when people are away or on holiday) or terrorists, who could sabotage the energy provision of a substantial number of households.[536]

After the failed 'underwear bomber' plot on Christmas Day 2009 the discussion to introduce body scanners was restarted again in the EU. Proponents pointed out that traditional walk-

[532] Bygrave, "Minding the Machine: Article 15 of the Ec Data Protection Directive and Automated Profiling.".

[533] ADABTS WP02, p. 130.

[534] Smart meters are fitted with sensors and linked through a network to a system that collects, collates and analyses consumption data in order to match generation and consumption of energy as closely as possible, thus leading to energy savings and avoidance of power cuts, etc…

[535] For more details regarding the data protection aspects of such meters, cf. Rainer Knyrim and Gerald Trieb, "Smart Metering under EU Data Protection Law," *International Data Privacy Law* 1, no. 2 (2011).

[536] See for instance: Colette Cuijpers and Bert-Jaap Koops, "Het Wetsvoorstel 'Slimme Meters': Een Privacytoets Op Basis Van Art. 8 Evrm," (Tilburg: Universiteit van Tilburg, 2008), 25..

through metal detectors failed to detect the explosives that Umar Farouk Abdulmutallab was hiding in his underwear. Consequently, a new type of scanner should be introduced as a screening measure which could detect this kind of materials in order to prevent terrorist attacks.[537] Body scanners produce an image of the body of a person showing whether or not objects are hidden in or under his clothes. There exist various technologies of body scanners, which are based on millimeter wave, backscatter or T-rays. The image that most of these scatters produce resembles a photographic negative.

When the European Commission tried to introduce the use of these scanners as a screening method in 2008, the European Parliament however objected to the introduction of these scanners without any safeguards attached to their use, since these machines had "a serious impact on the right to privacy, the right to data protection and the right to personal dignity, and therefore needs to be accompanied by strong and adequate safeguards".[538] The Parliament defined body scanners as "machines producing scanned images of persons as if they were naked, equivalent to a virtual strip search."[539] It has to be pointed out that newer body scanners do not produce this kind of images, but instead only show a standardized body image (a so-called 'mimic board'), which indicates the exact place on the body where a prohibited object is located.[540]

Data protection concerns

In section 2.1.1 we already highlighted the fact that data protection law will only protect personal data to the extent that the gathered data by the body scanner relates to an identifiable person. An individual will be identifiable by an image produced by a body scanner only if the quality of the image is good enough to allow this identification. Some scanners produce images that anonymize the person going through such a scanner by blurring the head of the person, or by using a standardized silhouette rather than an actual picture. When a standardized silhouette is used, a person won't be identifiable anymore, but this is not necessarily the case with the blurring of images. As the Fundamental Rights Agency notes: "Only in the case where an image can be rendered anonymous *and* any reference to the person neutralised, the use of body scanners would not constitute the processing of personal data and, accordingly, not be an interference with the protection of personal data."[541] Nevertheless it could be argued that the body scanner is still processing personal data, as a link is established between the data provided by the body scanner and the individual who is being screened. Based on this information provided by the body scanner, an evaluation of the threat will be conducted which will result in an impact on the individual in the form of a release or an additional 'pat down'. At present, the European Commission shares the opinion that the processing of unidentifiable persons by body scanners "falls under EU legislation on data protection."[542]

---

[537] See for instance: Noah Scachtman, "Underwear Bomber Renews Calls for 'Naked Scanners'," *Wired*, 28.12.2009 2009.

[538] European Parliament, "European Parliament Resolution of 23 October 2008 on the Impact of Aviation Security Measures and Body Scanners on Human Rights, Privacy, Personal Dignity and Data Protection," (Strasbourg: European Parliament, 2008).

[539] Ibid.

[540] Vermeulen, Detecter deliverable 6.3 at p.23.

[541] European Union Agency for Fundamental Rights - FRA, "The Use of Body Scanners: 10 Questions and Answers," (Vienna: FRA, 2010), 6.[*Emphasis added*]

[542] European Commission, "Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU Airports," (Brussels: European Commission, 2010), 11..

Since the use of body scanners has impact on the protection of personal data, it may only be authorized if it is adequately regulated by law. According to the Fundamental Rights Agency, this implies that the procedural rights of the data subject (e.g., right to information about the identity of the controller and about the purposes of the processing for which the data are intended, the right of access to data, and the right to rectification) should be spelled out explicitly in any instrument prescribing the processing of personal data by the use of body scanners. The effective exercise of these rights under personal data protection law requires that the data subject be clearly informed about the procedures which should be followed and, for instance, about the respective duties of the authorities using body scanners. If not, they are not in a position to give their informed consent about the data processing measure.[543] This is especially important for those body scanners that produce images which reveal sensitive personal data relating to an individual's health or sexual life.

Since the use of body scanners is based also on European law, the minimum rules on the use of body scanners should also be spelled out by European law. Most European countries did not yet establish a proper legal basis for the use of body scanners. At best, laws include blanket clauses on security screening at airports.[544] A European framework should limit the type of body scanners that could be used as a screening measure, and guarantee more uniform standards in relation both to security and to respect for individual rights.

The right to privacy

The most intrusive type of body scanner shows a person in a way that is normally reserved for the private sphere. Objections to this type of scanner do not only revolve around revealing nudity, because these scanners also would reveal intentionally concealed physical features (for instance of transsexuals) or medical information (such as evidence of a mastectomy) which people generally prefer not to be revealed.[545]

Such an interference with the right to privacy could be legitimate to increase airport security, but it remains questionable whether the introduction of this type of scanners would be really necessary in a democratic society. According to the Commission the end pursued is 'a higher security level' because 'non-metallic items' such as liquid or plastic explosives will be able to be detected.[546] This is questionable however, and many experts have questioned the efficiency of body scanners. Many (airport) security experts have questioned the effectiveness of the scanners. A former chief security officer at the Israel Airport Authority said that many explosives could pass a body scanner, while other experts have pointed out that body scanners are unlikely to detect the type of explosives or liquid bombs that were used successfully in the 2005 London bombings, and unsuccessfully in the foiled plots against airlines in 2006 and 2009.[547] Indeed, as Martin Scheinin points out, it is telling that the discussions on introducing body scanners come and go, which suggests that "governments' interest in them might be

[543] European Union Agency for Fundamental Rights - FRA, "The Use of Body Scanners: 10 Questions and Answers," 9.

[544] Vermeulen, D6.1, p.16.

[545] European Union Agency for Fundamental Rights - FRA, "The Use of Body Scanners: 10 Questions and Answers," 4.

[546] European Commission, "Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU Airports.".

[547] Vermeulen D6.1, p. 23.

linked more to reacting to occasional events than to the intrinsic security benefit of the machines."[548]

If the introduction of body scanners would be really necessary to increase security, it should be used as a mandatory first screening measure. Since using the most intrusive type of body scanners could result in a violation of the right to non-discrimination (see below) body scanners could only be used as a secondary screening measure. While the introduction of choice seemingly reduces the interference with fundamental rights it at the same time tilts the balance of the necessity test to the opposite direction (as the possibility of choice may frustrate the whole purpose of the interference which therefore becomes unnecessary).

Right of non-discrimination

The use of body scanners which produce 'naked images' could result in direct discrimination if these scanners are used as a mandatory first screening measure. As the Fundamental Rights Agency points out: "Under certain religious traditions within Orthodox Judaism or Islam for instance, men and women cannot reveal body parts considered to have sexual connotations. The use of a body scanner could make it impossible for adherents of such traditions to travel when no alternative is offered, which would violate the right to freedom of movement and the prohibition of discrimination."[549]
Discrimination could also occur where the use of any type of body scanners occurs on a discretionary basis and their use either intentionally or in fact amounts to profiling resulting in one or more particular social group being disproportionately targeted.[550] In order to avoid such profiling, it would be necessary to closely monitor who in fact is singled out to go through the scanner.[551]

3.2.3 The Passenger Name Records System(s)

The Passenger Name Record (PNR) 2007 agreement

PNR has gained an enormous relevance in both symbolic and practical terms. It has been the object of several international agreements, national measures, political and institutional clashes as well as the subject of strong academic interest. [552] PNR data is unverified

[548] Gloria González Fuster and Rocco Bellanova, "Body Scanners - Inex Evening Round-Table," (Brussels: INEX/CEPS, 2011), 3..

[549] See for instance ECtHR, App. 27417/95, Cha'are Shalom Ve Tsedek v. France, (27/02/2000), §§ 80-81.

[550] United Nations General Assembly (2007), Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin (A/HRC/4/26), §§ 34 and 41.

[551] Cf. European Union Agency for Fundamental Rights - FRA, "Towards More Effective Policing Understanding and Preventing Discriminatory Ethnic Profiling: A Guide," (Luxembourg: Publications Office of the European Union, 2010)..

[552] Among recent academic works focusing on PNR systems and issues, cf. Evelien Brouwer, "The EU Passenger Name Record System and Human Rights. Transferring Passenger Data or Passenger Freedom?," in *CEPS Working Document* (Brussels: CEPS, 2009); Peter Hobbing, "Tracing Terrorists: The EU-Canada Agreement in PNR Matters," (Brussels: Centre for European Policy Studies, 2008); Patryk Pawlak, "Made in the USA? The Influence of the US on the Eu's Data Protection Regime," (Brussels: Centre of European Policy Studies, 2009); Els De Busser, "EU Data Protection in Transatlantic Cooperation in Criminal Matters: Will the EU Be Serving Its Citizens an American Meal?," *Utrecht Law Review* 6, no. 1 (2010); Vagelis Papakonstantinou and Paul De Hert, "The PNR Agreement and Transatlantic Anti-Terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic," *Common Market Law Review* 46, no. 3 (2009).. Many civil liberties' watchdogs and advocates regularly publish reports and documentation related to PNR: cf. Statewatch, "Observatory on the Exchange of Data on Passengers (PNR) with USA," Statewatch.org,

information provided by passengers and collected by carriers for enabling reservations and carrying out the check-in process.[553] Such data are generally not stored in airlines' databases, but in the databases of Computerized Reservation Systems.[554] Given their commercial purposes, PNR data contain several kind of information, ranging from travel-related information to very personal and relational data (the meals' options of the passenger or its credit card number, but also addresses and information on other passengers and travel agents). The 2007 EU-US PNR agreement[555] is the third agreement signed, after the termination of the first imposed by the ruling of the European Court of Justice in 2006, and the expiration of the (second) interim one in 2007.[556] Note that the 2007 agreement has been recently re-discussed and re-negotiated. and it will eventually be approved according to the new Lisbon procedures, given that the Member States' ratification process was not finalized before the entry into force of the Lisbon Treaty.[557] The text of the 2011 EU-US PNR agreement has been signed by the Council by mid December 2011, but the consent from the European Parliament is still pending.[558]

The PNR agreement is composed by a set of three documents: the first is the agreement itself, while the other two are the letters exchanged between the US and the EU. A more detailed presentation of the data processing practices subsumed by the PNR agreement can be re-traced in other types of documents, such as the DHS Privacy Office impact assessments, the US system of records notifications (SORN) and the European Commission report on the EU-US joint review. PNR data are stored and processed in the so-called ATS-P, a separate module of the Automatic Targeting System for the screening of passengers.[559] There PNR data are cross-referenced with other information, including ESTA data, Advanced Passenger Information System records, TECS Enforcement records, National Crime Information Center wants and warrants. According to the Commission report on the 2010 PNR joint review, the data is also "run against scenario-based targeting rules to identify persons that could pose a risk to security but who were previously "unknown" to DHS. Following this automated processing, officers at the National Targeting Center-Passenger (NTC-P) process the data of the passengers who have been identified as a result of the automated processing in order to carry out additional checks on them. This process leads to either the clearing of the

---

http://www.statewatch.org/pnrobservatory.htm; Electronic Privacy Information Center - EPIC, "Air Travel Privacy," EPIC.org, http://epic.org/privacy/airtravel/..

[553] European Commission, "Communication from the Commission. On the Global Approach to Transfers of Passenger Name Record (PNR) Data to Third Countries," (Brussels: Euroepan Commission, 2010), 3.

[554] Edward Hasbrouck, "What's in a Passenger Name Record (PNR)?," in *The Practical Nomad* (2009).

[555] Agreement between the European Union and the United States of America on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the United States Department of Homeland Security (DHS) (2007 PNR Agreement), OJ L204/17, 4.8.2007.

[556] The first EU-US PNR agreement was annulled by the European Court of Justice because of the wrong legal base of the agreement, cf. *European Parliament V Council of the European Union (Case C-317/04) and Commission of the European Communities (Case C-318/04). Joined Cases C-317/04 and C-318/04*,(2006).

[557] Also the other two PNR agreements signed by the EU will also be re-negotiated, the EU-Canada because it expired and the EU-Australia for the same reasons of the EU-US one. In October 2010, the "the three mandates should be identical in content and adopted at the same time; (…) [and] once the mandates are adopted, negotiations with the three partner countries should start simultaneously", Council of the European Union, "Press Release. 3034th Council Meeting Justice and Home Affairs. Luxembourg, 7-8 October 2010," (Luxembourg: Council of the European Union, 2010), 11.

[558] Council of the European Union, "Agreement between the United States of America and the European Union on the Use and Transfer of Passenger Name Records to the United States Department of Homeland Security," (Brussels: Council of the European Union, 2011).

[559] Cf. DHS Privacy Office, "2009 Data Mining Report to Congress," (Washington, D.C.: Department of Homeland Security, 2009).

identification or to the confirmation of the identification. Additional manual checks are carried out as regards such identified persons in order to establish whether they seem to have any associates traveling with them".[560]

Therefore, as also confirmed by the DHS Privacy Office reports on data mining,[561] the PNR processing is a set of profiling operations carried on the totality of US-bound travelers (including US citizens). Identification is done not only through the comparison with established lists, but also by association and construction of "risk" profiles.[562] Another important element to be underlined is the ability to obtain and process information at a "distance", both in spatial and temporal terms. Indeed, PNR data should be sent up to 72 hours before the departure of the flight, and thus the processing of personal data and the eventual secondary screening or prohibition of boarding, could happen when the individual is not yet in movement or has not yet reached the destination.

EU-wide PNR system

The main purpose of the Commission Proposal for a EU-wide PNR system is not dissimilar to those of the PNR international agreements. In particular, the aim is to make available PNR data to "competent authorities" for the "purpose of preventing and combating terrorist offences and organized crime, as well as the collection and retention of those data by these authorities and the exchange of those data between them".[563] This proposal was present few months after the conclusion of the last EU-US PNR agreement, and the first public draft was discussed and modified in a first series of rounds till October 2009.[564] Then, the framework decision proposal has been left aside, waiting for the entry into force of the Lisbon Treaty and the relevant change in the decision-making procedure. The most important part of the proposal resides in the competences of the so-called Passenger Information Units (PIUs) and the types of data processing that they are supposed to carry on. Indeed, PIUs shall be responsible for the collection of PNR data, the deletion of "special categories of personal data", as well as the analysis of data and the risk-assessment of passengers.[565] Finally, the PNR data of individuals "assessed" by PIUs, should be transmitted to the "competent authorities of Member States".[566] The processing of PNR data is done in order to select

[560] European Commission, "Report on the Joint Review of the Implementation of the Agreement between the European Union and the United States of America on the Processing and Reansfer of Passenfer Name Record (PNR) Data by Air Carriers to the United States Department of Homeland Security (Dhs). 8-9 February 2010," (Brussels: European Commission, 2010), 14.

[561] Cf. DHS Privacy Office, "2009 Data Mining Report to Congress."

[562] Furthermore, "[w]hile the risk-based rules are initially created base don information derived from pas investigations and intelligence (rather than derived through data mining), data mining queries of data in ARS and its source databases may be subsequently used by analysts to refine or further focus those rules to improve the effectiveness of their application", Ibid., 10.

[563] Art.1, European Commission, "Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes," (Brussels: European Commission, 2007), 12-13. Also the quality and quantity of personal data to be processed within the PNR data is the same of the EU-US and EU-Australia agreements, cf. European Commission, "Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes," 25.

[564] For an extensive analysis of the 2007 EU PNR Commission Proposal, cf. Franziska Boehm, "EU PNR: European Flight Passengers under General Suspicion - the Envisaged European Model of Analyzing Flight Passenger Data," in *Computers, Privacy and Data Protection: An Element of Choice*, ed. Serge Gutwirth (Dordrecht: Springer, 2011).

[565] Art.3, European Commission, "Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes," 14.

[566] Art.3(4), Ibid.

passengers that require "further examination", with the purpose "to identify persons who are or may be involved in a terrorist or organized crime offence, as well as their associates".[567] However, the processing of PNR data has other three purposes: "to create and update risk indicators for the assessment of such persons; to provide intelligence on travel patterns and other trends relating to terrorist offences and organized crime; to be used in criminal investigations and prosecutions of terrorist offences and organized crime".[568] Thus, without explicitly mentioning it, the EU-PNR proposal promotes the introduction of the first EU system of profiling for law-enforcement. The safeguards proposed are of three kinds: (i) the PIUs' duty to delete "special categories of information"; (ii) the applicable national law guarantees in respect to risk-assessment procedures; and (iii) applicable EU data protection rules.[569] Notwithstanding these three layers, the Commission proposal was heavily criticized for not providing adequate safeguards, especially in terms of protection of personal data and privacy,[570] as well as in terms of risk of discrimination.[571] Furthermore, the possible re-introduction of internal controls and borders within the EU was also discussed in relation to its possible scope.[572] From the point of view of practices of data processing, the main interrogatives raised by the Commission Proposal concern the actual functioning of the processing; the establishment of criteria for conducting risk-assessment left to national laws; and the eventual limits for the use of profiles by Member States' agencies.[573]

Data protection concerns

Until the adoption of the 2008 Framework Decision it was clear that the processing of PNR-data took place in a legal 'no mans land'. The processing of PNR by European aircrafts clearly was subjected to the Data Protection Directive, but the eventual processing of the same data by law-enforcement and other public security bodies lacked a specific regulation up until then. This ambiguity was exacerbated by confusion about what the exact legal relationship was between the main agreement, and the two set of letters between the EU and the US.[574] While the 2008 Framework Decision solved this particular problem, difficulties in determining the exact legal framework remain since at least two other legal regimes still apply: the aforementioned data protection directive (for the data collection by the aircrafts) and national data protection law (for the data transfers between the PIU and the national law enforcement authority).

---

[567] Art.3(5), Ibid.

[568] Art.3(5), Ibid., 14-15.

[569] During the series of negotiations, instead of the application of the general EU data protection framework for law enforcement initially foreseen, was drafted a specific, *ad hoc*, data protection framework for the measure.

[570] Cf. Paul De Hert and Vagelis Papakonstantinou, "The EU PNR Framework Decision Proposal: Towards Completion of the PNR Processing Scene in Europe," Computer Law & Security Review 26 (2010): 374-76, European Data Protection Supervisor - EDPS, "Opinion on the Draft Proposal for a Council Framework Decision on the Use of Passenger Name Records (PNR) Data for Law Enforcement Purposes," (Brussels: EDPS, 2007)

[571] Cf. Brouwer, "The EU Passenger Name Record System and Human Rights. Transferring Passenger Data or Passenger Freedom?," 20-24; European Union Agency for Fundamental Rights - FRA, "Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) Data for Law Enforcement Purposes," (Vienna: FRA, 2008), 10-13.

[572] European Union Committee House of Lords, "The Passenger Name Record (PNR) Framework Decision," (London: House of Lords, 2008).

[573] Cf. art.3(3), European Commission, "Proposal for a Council Framework Decision on the Use of Passenger Name Record (PNR) for Law Enforcement Purposes," 14.

[574] Cf. Papakonstantinou and De Hert, "The PNR Agreement and Transatlantic Anti-Terrorism Cooperation: No Firm Human Rights Framework on Either Side of the Atlantic," 909.

The draft PNR Framework Decision will eventually apply to the data transfers by the airline companies to the PIUs as well. Various commentators, including the Fundamental Rights Agency, the EDPS and the European Parliament have made clear that the legal rules dealing with the collection and use of passenger data, the competences of the PIUs, the powers of national authorities and authorities of third countries, the rights of data subjects and data protection authorities are still insufficiently clear and precise.[575]

Both the EU PNR system as the current EU-US agreement are also problematic in terms of their respect for the purpose limitation principle. In principle the use of PNR data is limited to member states' activities against terrorist or other serious crimes. But it seems that the EU's proposed PNR-system raises at least four question marks in this context. Firstly, the draft text widens the range of activities for which PNR-data can be used (i.e "the prevention, investigation, detection or prosecution" of terrorist offences or serious crime.) Article 4(5) of the draft allows the further use of PNR data for other offences, when these offences or "indications thereof" are detected during the enforcement action with regard to terrorist offences or serious crime. Thirdly, as Brouwer notes, "although the definitions of 'terrorist offences' and 'serious crime' refer to the definitions as adopted in earlier Framework Decisions on combating terrorism, organised crime, and on the European Arrest Warrant, it seems unclear at this moment whether these latter instruments have actually led to a more harmonised approach in this field." Last but not least, the draft would also allow the use of PNR data for "integrated border management" purposes. [576]

As a consequence thereof, the European Data Protection Supervisor and the Agency of Fundamental Rights confirm that passengers become de facto subject of proactive investigation methods "on the basis of a mix of in concreto and in abstracto information, including standard patterns and abstract profiles." [577] The main concern of both the EDPS and the FRA relates to the fact that decisions on individuals will be taken on the basis of a comparison with patterns and criteria established using the data of passengers in general. According the FRA "This results in a situation in which it is not possible for any individual to know which use shall be made of his/her PNR data, a situation incompatible with the requirement of "foreseeability" imposed under Article 8(2)".[578] The EDPS further adds that it is "extremely difficult for individuals to defend themselves against such decisions."[579]

Right to non-discrimination

The Commission recognizes that the flagging of passengers could violate the right of non-discrimination, and has consequently inserted a non-discrimination clause in the agreement.[580] Such a clause however is not likely to halt indirect discrimination which can be the result of sorting individuals on the basis of data such as food preferences, which may reveal a person's

[575] European Data Protection Supervisor Opinion on the draft proposal for a Council framework decision on the use of Passenger Name records (PNR) for law enforcement purposes, OJ 2008, C110/01; European Parliament, Resolution of 20 November 2008 on the proposal for a Council framework decision on the use of Passenger Name records (PNR) for law enforcement purposes, B6-0615/2008; Opinion of the European Union Agency for Fundamental Rights on the Proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) data for law enforcement purposes, 28 October 2008.

[576] Brouwer, "The EU Passenger Name Record System and Human Rights. Transferring Passenger Data or Passenger Freedom?," 20.

[577] EDPS opinion at 19.

[578] FRA opinion at 13.

[579] EDPS opinion at 22.

[580] Check

faith for instance. The Fundamental rights agency has also made clear that profiling as such is *always* based on mechanisms that differentiate between different groups of persons on the basis of specific criteria. In the aforementioned opinion on the draft PNR Framework Decision, the FRA underlined the adverse effects of profiling, alienating and victimizing certain ethnic and religious groups, which engender a deep mistrust of the police.[581]

3.3 "LAW ON THE MOVE": CURRENT EU LEGISLATIVE EVOLUTIONS

The steady increase in the quality and the quantity of surveillance and security measures involving the processing of information, and in particular personal data, is generally considered by many institutional actors, academics and civil society representatives as one of the most important challenges to the rights to privacy and data protection. Furthermore, given the technological density and transnational and transversal scope of many of these measures, it can be argued that the legal framework that regulates the right to privacy and data protection needs to be further developed.

In the EU, such arguments focus in particular on attempts to rethink and improve the right of data protection, thereby seizing the legislative opportunities provided by the Lisbon Treaty, and the new legal basis offered by art.16 TFEU, and the related entry into force of the EU Charter of Fundamental Rights. While no substantial legislative modifications have been introduced yet, important debates are taking place at EU level. Probably the most important initiative deals with the revision of the Data Protection Directive. This process was launched by the European Commission in 2009, by the opening of formal consultations and tendering of experts' studies. In 2010 the Commission released a Communication on a new approach on personal data protection, which was also discussed by EU institutions and relevant stakeholders. A formal legislative proposal from the Commission is finally expected by the beginning of 2012. As discussed below, some of the elements of these discussions are particularly relevant to understand how new legislative measures could tackle and "influence" smart surveillance, or, at least, can highlight how key actors frame the related challenges and objectives.

Besides this discussion, it is worth to note that other discussions are taking place in the EU *fora*. For the purposes of this chapter the most important ones seems to concern the ongoing revision of the Data Retention Directive; the re-negotiation of transatlantic agreements on the sharing and processing of PNR data, as well as the proposed introduction of a similar EU-wide scheme; and the "diplomatic negotiation" of a EU-US agreement over data protection and data processing.

Finally, particular attention should be deserved to the adoption, in November 2010, of the Recommendation of the Committee of Ministers of the Council of Europe on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

The following sections present a short overview of the above-mentioned discussions and evolutions, underlining the elements that directly, and to some extends indirectly could be important for smart surveillance practices.

[581] See also Open Society Justice Initiative, *Ethnic Profiling in the European Union: Pervasive, Ineffective, and Discriminatory*, New York, May 2009.

3.3.1 The revision of the Data Protection Directive

As discussed in the first part of this chapter, the Data Protection Directive is generally considered the most important piece of legislation when it comes to privacy and data protection. However, in the last few years a certain consensus on the need to revise this instrument has emerged, arguing, in the words of the Commission, that while "[its] objective is still valid and the principles enshrined in the Directive remain sound […] rapid technological developments and globalisation have profoundly changed the world around us, and brought new challenges for the protection of personal data".[582] The aim of this section is not to re-assess the need for a revision, or the grounds and reasons for such an exercise, but rather to understand the "place" of smart surveillance in the context of some potential changes to the current legislative framework, and how potential modifications could affect smart surveillance practices.

The Future of Privacy

One of the key contributions to the ongoing process of revising the EU's privacy and data protection architecture was the joint reaction of the Article 29 Working Party and the Working Party on Police and Justice to the 2009 Commission Consultation, entitled "The Future of Privacy".[583] The document is particularly relevant for the scope of this chapter because it dedicates an entire chapter to the field of police and law enforcement, as an area of "specific concern".[584] Also, the two institutions point out that the revision process is a "useful" opportunity to "include the fundamental principles of data protection into one comprehensive legal framework, which also applies to police and judicial cooperation in criminal matters".[585]

Indeed, as also noted in the sections below, the intention to extend a comprehensive framework to also cover the previously labeled "third pillar policies" is a recurring concern among institutional actors. This ambition is generally coupled with more or less explicit criticism of the protection offered by the 2008 Framework Decision, which "seems to lack essential elements and tools to effectively deal with the changing working methods in the area of law enforcement".[586] Indeed, in the Future of Privacy document, the "shift of emphasis" in law enforcement practices is seen as the main reason to justify modifications in the data protection framework for police and judicial cooperation.[587] Most notably, the description of the main features of such a shift are all closely related to the Sapient working definition of smart surveillance: use of "preventive policing"; focus on a wider group of persons, including those who are not involved in an investigation; a technologically dense processing of information, with reliance on correlation and profiling tools to "predict future behaviour"; an growing heterogeneity in the nature of the information processed, including information originated in the private sector; use of information behind the legitimate purpose for which it was collected, mainly via "interoperability" and "interconnection of databases having different purposes"; widening of the number of agencies accessing and processing data,

[582] European Commission, "Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A Comprehensive Approach on Personal Data Protection in the European Union," 2.

[583] Article 29 Data Protection Working Party and Working Party on Police and Justice, "The Future of Privacy."

[584] Ibid., 4, and, in extenso, Chapter 8.

[585] Ibid., 2.

[586] Ibid., 25.

[587] Ibid., 25-28.

including "national security services".[588] Furthermore, some of the specific examples provided in the document overlap with the practices analyzed, or mentioned, in the second part of this chapter, as in the case of intelligent CCTV, data mining and risk assessment practices operating on non-suspects.

Finally, another implicit challenge underlined in the document is the proliferation of European measures, which "may easily lead to overlapping or even distortion measures".[589] Against the background of these challenges, the Article 29 working Party and the Working Party on Police and Justice propose specific remedies: ex-ante and ex-post evaluation of introduced measures; transparency on the processing mechanisms, and in the decision-making; a shift in the architecture of stage and exchange systems; stronger attention to the external (extra-EU) dimension of data sharing; special attention for large scale information systems; and strengthening of the role and competences of data protection authorities.[590]

Out of this list, some elements deserve a more attentive analysis, and in particular those revolving, implicitly or explicitly, on the relation between technologies and political debate and decision. Indeed, technology is not perceived as threatening *per se*, but on the contrary, open to what could be defined a "protective use" (in particular in the architectural design of systems, via the adoption of "privacy by design" and the option for non-direct access to stored data). However, even if mostly implicitly, emphasis is put on the fact that even technological choices remain somehow problematic, requiring transparency both at the level of the decision making, and at the very level of "the use of the formation collected and the logic underlying the processing".[591] On the one side, a specific call for the introduction of Privacy impact assessment is advanced, and, on the other side, strong attention to the "technicalities" of the systems proposed in advocated. Thus, in synthesis, the two institutions seem to perceive in the revision process a possibility to tilt the meaning of "smart" surveillance towards forms that are less intrusive, more politically legitimized, and data protection-proof.

Finally, it is interesting, and somehow surprising, to note that the text does not introduce any strong reflection on the possible problematic notion of "personal data", nor it takes into consideration how to handle surveillance practices able to transform trivial data into sensitive ones.

The 2010 Commission Communication on a comprehensive approach on personal data protection

On the basis of the contributions to the Consultation launched in 2009, and relying on the inputs of the experts' studies, the Commission has presented a communication in November 2010 on "a comprehensive approach on personal data protection in the European Union".[592] The Communication summarizes the main challenges to personal data protection emerged since the adoption of the Data Protection Directive in 1995, and concludes that there is a need to "develop a comprehensive and coherent approach guaranteeing that the fundamental right to data protection for individuals is fully respected within the EU and beyond".[593] This

[588] Ibid., 25-26.

[589] Ibid., 26.

[590] Ibid., 27-28.

[591] Ibid., 27.

[592] European Commission, "Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A Comprehensive Approach on Personal Data Protection in the European Union."

[593] Ibid., 4.

"omnibus" approach is already relevant in itself for the scope of this contribution, especially since it pre-supposes an effort to bypass the present gaps in both the Directive (the non-application to security related policies and activities) and the 2008 framework decision. In relation to this latter instrument, the Communication highlights several shortcomings, and in particular four crucial limits. First, its scope is too limited, covering only to "cross-border exchange within the EU and not to domestic processing operations in Member States".[594] Second, the 2008 framework decision provides for a "too wide exception to the purpose limitation principle".[595] Third, there is no provision concerning the labeling of, and differentiation among, different categories of data, which should be distinguished "in accordance with their degree of accuracy and reliability (…) [and] between different categories of data subjects", with a special attention devoted to data of non-suspects.[596] Finally, the Communication underlines the direct effect on the "possibilities for individuals to exercise their data protection rights" originated in the co-existence of the Framework Decision next to other sector-specific legislative instruments, which limits the transparency of data processing processes vis-à-vis data subjects.[597]

To remedy to these shortcomings, the Communication proposes to consider "the extension of the application of the general data protection rules to the areas of police and judicial cooperation in criminal matters" while providing specific and "harmonized limitations to certain data protection rights"; to introduce tailored provisions on the processing of specific data and "distinguish the various categories of data subjects"; and to "align (…) the existing various sector specific rules (…) with the new general data protection framework".[598]

Apart from the adoption of such a comprehensive approach, which will nevertheless preserve practices and limitations specific to law enforcement, other "general" objectives of the Communication are potentially relevant for the handling of smart surveillance. First, it is important to note that the presentation of the key objectives of the new approach starts with some considerations on the concept of "personal data" and the linkage between this notion and specific systems of data processing. Unfortunately, in the Communication no real proposal is made, apart from a generic commitment to "ensure a coherent application of data protection rules, taking into account the impact of new technologies on individuals' rights and freedoms".[599] Thus, the Communication seems to take note of the potential limits implicit in the notion of personal data, which, as discussed above, tend to become evident in the deployment of smart surveillance systems. On the negative side, it does not formally engage in considering the proposal of a legal definition of profiling and data mining.

Other relevant points concern the emphasis on "data minimization" and on the possible extension of the category of "sensitive data" (to include also genetic data), and the harmonization of the conditions of processing.[600] Again, given that no specific propositions are advanced, it is difficult to assess how the possible changes could affect "smart surveillance" practices; even their potential is already evident. Indeed, strengthening the principle of "data minimization" could tilt the meaning of smart in the sense of "data protection-proof", obliging systems to operate on less data and reducing "further processing".

[594] Ibid., 13.

[595] Ibid.

[596] Ibid., 13-14.

[597] Ibid., 14.

[598] Ibid., 14-15.

[599] Ibid., 6.

[600] Ibid., 7-9.

In the case of the extension of the category of "sensitive data", a possible positive outcome could consist of the de-trivialization of the storing and processing of DNA data. Another possible evolution could be the creation of a sort of "dynamic" categories, which could include data not only on the base of their own specific nature, but also on the base of the type of knowledge that is possible to extract from them in the light of technological advances.

Finally, given the transnational nature of many "smart surveillance" systems, which can also be located outside the EU while fed by, and acting upon, EU data subjects, it is important to note that the Communication underlines the need for the clarification and simplification of the rules for international data transfers, "while at the same time ensuring tat personal data are adequately protected when transferred and processed outside the EU and the EEA".[601]

Institutional reactions to the Commission Communication

Apart from the few lines published by the Council, advocating for the guarantee of compliance of "appropriate data protection standards (…) in all areas where personal data are processed",[602] the two most interesting institutional reactions to the 2010 Commission Communication are the opinion of the EDPS and the report of the European Parliament. Again, the main aim of this section is to focus on the elements that can be more significant in the light of smart surveillance, rather than critically discussing the full documents.

The EDPS

As in the case of the "Future of Privacy" document, an entire chapter of the EDPS-opinion is dedicated to the area of police and justice, in which the EDPS strongly welcomes the idea of extending the comprehensive framework to this area. The EDPS supports the idea by mentioning specific advantages linked to this decision, as such as the possibility to apply in a restrictive way the power for Member States to "adopt specific legislation to restrict obligations and rights under the general instrument for specific public interests".[603] However, the EDPS acknowledges the law enforcement and judicial needs for the introduction of "special rules of derogations", as well as the possible need for "sector specific data protection regimes".[604] Nevertheless, on the one side, limitations should respect the criteria of necessity, proportionality and "should not alter the essential elements of the right in itself"; and, on the other side, the "new legal framework should be, as far as possible, clear, simple and consistent".[605]

The Opinion also advances five new elements relating to be included: (i) a "distinction" between different categories of data, on the base of accuracy and reliability; (ii) a "distinction" between "categories of data subjects"; (iii) "mechanisms to ensure periodic verification and rectification"; (iv) specific provisions and guarantees for the processing of biometrics and genetic data (and in general, a limited use of them); (v) rules for the transfer of law enforcement data to non-law enforcement actors (including private parties) and for the

[601] Ibid., 16.

[602] Council of the European Union, "Press Release. 3034th Council Meeting Justice and Home Affairs. Luxembourg, 7-8 October 2010."

[603] European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - 'a Comprehensive Approach on Personal Data Protection in the European Union'," (Brussels: European Data Protection Supervisor, 2011), § 130.

[604] Ibid., §§ 131 & 35.

[605] Ibid., §§ 131 & 36.

"further use by law enforcement authorities of personal data collected by private parties".[606] Quite surprisingly, no specific recommendation is formulated on the introduction of specific provisions concerning profiling and data mining activities.

The fifth recommendation concerns the "blurring" of the "distinction between activities of the private sector and of the law enforcement sector", and it is also presented as one of the main reasons for which the integration of the area of law enforcement within the comprehensive framework is a "*conditio sine qua non*", and "one of the main improvements a new legal framework can bring".[607] Even further, the EDPS stresses that "[i]ncluding police and justice in the general legal instrument would not only offer more guarantees to citizens but also make the task of police authorities easier".[608] Indeed, one of the most interesting elements of the EDPS opinion is the emphasis devoted on the role of data protection within societies and societal activities, and in particular in respect to security and law enforcement and judicial cooperation. In the words of the EDPS, "[d]ata protection was quite often wrongly characterized as an obstacle to fully protecting the physical security of individuals, or at least an unavoidable condition to be respected by law enforcement authorities".[609] Instead, the Opinion states that "[a] strong framework of data protection can sharpen and strengthen security", ensuring, inter alia, accuracy and pertinence of the data, the security of the systems themselves and fostering trust on the work of law enforcement agencies.[610] As in the case of the Artice 29 and the Working Party on Police and Justice, it emerges from the EDPS' opinion that the revision of the data protection Directive could be an occasion to reframe, in general terms, the relation between security (or surveillance) and data protection. In particular, it could (partially) re-orientate current surveillance practices towards a different use and collection of personal data, which is more regulated and more "data protection friendly". Nevertheless, at this stage it is very difficult to understand how such a shift could take place beyond the discursive level, especially since several of the recommendations proposed are based on very limited practical experience.

Finally, the EDPS Opinion highlights the relevance of the international dimension of data exchange and processing, as well as the need for a further strengthening of data subjects' possibilities to enforce their data protection rights.

The European Parliament

The European Parliament resolution on a comprehensive approach on personal data protection was adopted in July 2011.[611] It shares with the EDPS the same, generally favorable, position on the Commission Communication, as well as the strong support for the inclusion of the area of police and justice within the omnibus framework. Indeed, "it considers it imperative to extend the application of the general data protection rules to the areas of police and judicial cooperation, including processing at domestic level, tacking particular account of the questionable trend towards systematic re-use of private-sector personal data for law-enforcement purposes, while also allowing, where strictly necessary and proportionate in a

[606] Ibid., § 133.

[607] Ibid., §§ 34-35.

[608] Ibid., §36.

[609] Ibid., § 22.

[610] Ibid., § 22, & ff.

[611] European Parliament, "European Parliament Resolution of 6 July 2011 on a Comprehensive Approach on Personal Data Protection in the European Union," (Strasbourg: European Parliament, 2011).

democratic society, for narrowly tailored and harmonized limitations to certain data protection rights of the individuals".[612]

Furthermore, it is interesting to note that the European Parliament acknowledges explicitly the protection role of data protection and privacy "from possible surveillance and abuse of their data by the state itself, as well as by private entities".[613] In this sense, the resolution puts emphasis on the need to reinforce elements such as transparency, data minimization and purpose limitation.[614] Even more relevant for the purpose of this section, is Parliament's call on the Commission to "include provisions on profiling, while clearly defining the terms 'profile' and profiling'".[615] Regulating, and defining, profiling is thus put back on the agenda in the most explicit way.

Another important element of the Resolution is the request "to make Privacy Impact Assessments mandatory",[616] implicitly echoing the reflections introduced in the "Future of Privacy" document. Indeed, such an attention to mandatory privacy impact assessment highlights the increasing challenge of maintaining the ability to intervene on potentially threatening measures before they are implemented, rather than afterwards, when systems have been already deployed.[617]

3.3.2 The evaluation and revision of the Data Retention Directive

In parallel with the process of revision of the Data Protection Directive, a second important process is taking place in the European Union, focusing on the evaluation of the implementation, and upcoming revision, of the Data Retention Directive. The process was launched in May 2009 with a conference organized by the Commission, which was then followed by the diffusion of a questionnaire drafted by the Commission. Then, a second conference was organized in December 2010, to take stock of the ongoing replies to the questionnaires and re-launch the debates and discussions. Finally, in April 2011, the Commission has released an Evaluation report, providing analysis of the data and assessments received by Member States, and paving the way to the prospective process of revision.[618] As in the pages above, the elements discussed are chosen on the basis of their relevance for the scope of the chapter, and do not pretend to be an exhaustive introduction to such complex debates.

Commission Evaluation report

In accordance with article 14 of the Directive, the Commission presented its long-awaited evaluation report on the implementation of the Directive in April 2011. The biggest advantage of this document is that it presents hard facts on how Member States have implemented the Directive until now. This evaluation makes clear that the aim to harmonize Member States'

[612] Ibid., § 6.

[613] Ibid., § K.

[614] Ibid., § 11.

[615] Ibid., § 18.

[616] On mandatory Privacy Impact Assessment, cf. David Wright, "Should Privacy Impact Assessment Be Mandatory?," *Communications of the ACM* 54, no. 8 (2011).

[617] European Parliament, "European Parliament Resolution of 6 July 2011 on a Comprehensive Approach on Personal Data Protection in the European Union," § 31.

[618] European Commission, "Repot from the Commission to the Council and the European Parliament. Evaluation Report on the Data Retention Directive (Directive 2006/24/Ec)," (Brussels: European Commission, 2011). Hereafter: Commission Evaluation Report.

data retention regulations has failed. Crucial issues like the purpose limitation for data retention, the length of retention, the security of retained data and access to data are very different among the member states. Also the procedure for obtaining access to retained data differs substantially.

Fort the purposes of this chapter it is interesting to note that the evaluation never questions the necessity of the Directive, but instead just states that "data retention is a *valuable* tool for criminal justice systems and for law enforcement in the EU". According to anecdotal stories provided by some member states, data retention is necessary since only retained data enable the construction of trails of evidence leading up to an offence which involves communication over the internet or over the telephone. Further there have been cases for which, in the absence of forensic or eyewitness evidence, "the only way to start a criminal investigation was to consult retained data".[619] Abolishing the Directive is therefore not considered as an option; the Commission expects "Member States who have not yet fully transposed the Directive (…) to do so as soon as possible".[620] The Commission will now introduce amendments to the existing Directive in 2012.

The choice to retain the data retention Directive is interesting since civil society organizations and some MEPs have advocated to replace the data retention Directive by a 'smarter', more limited system of data retention, namely the system of 'data preservation' or 'quick freeze'. This system has been earlier embraced by the EDPS,[621] the Article 29 WP[622] and the rapporteur on the data retention directive for the European Parliament.[623] As Bignami describes: "Under this procedure, when the police have a suspect in mind, yet still do not have evidence that would satisfy the standard for obtaining a court warrant, they can ask communications providers to store that person's communications data. If at a later point the police do have the evidence necessary for a court warrant, they can obtain access to the data."[624] In this scenario, communication providers only have to keep the traffic data which they usually retain themselves, because they need them for billing purposes. A variation of this procedure is called 'quick freeze plus'. In this scenario, certain communication data which are not normally stored, such as location data, internet connection data and dynamic IP addresses for users which have a flat-rate subscription could be accessed as well. According to the Commission however "most Member States disagree that any of the variations of data preservation could adequately replace data retention, arguing that

> "whilst data retention results in the availability of historical data, data preservation does not guarantee the ability to establish evidence trails prior to the preservation order, does not allow investigations where a target is unknown, and does not allow for evidence to be gathered on movements of, for example, victims of or witnesses to a crime".[625]

---

[619] Commission Evaluation Report, p. 24.

[620] Commission Evaluation Report, p. 21.

[621] See Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC, 2005 OJ (C 298) 1, §20.

[622] Article 29 Working Party, Opinion 4/2005, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp113_en.pdf at 6.

[623] European Parliament Committee on Civil Liberties, Justice and Home Affairs, Report on the proposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (COM(2005)0438 – C6-0293, A6-0365/2005, 28 November 2005.

[624] Francesca Bignami, "Privacy and Law Enforcement in the European Union: The Data Retention Directive," *Chicago Journal of International Law* 48(2007): 249.

[625] Commission Evaluation Report, p.5.

Besides from offering more clarity on the exact implementation of the Directive, the 'evaluation' actually does not evaluate the societal effects of the implementation of the Directive. While this aspect of the evaluation is not required by Article 14 of the Directive, it remains a missed opportunity that only 3 out of 43 pages were devoted to a general assessment of the impact of the Directive on fundamental rights.

The EDPS filled this gap by giving his comments on the Commission's evaluation from a privacy and data protection point of view. According to the EDPS, the Data Retention Directive does not meet the requirements imposed by the rights to privacy and data protection because of three main deficiencies. The EDPS is of the opinion that the necessity of data retention has not been sufficiently demonstrated by the Commission. "Interesting examples of its use have been provided, however, there are simply too many shortcomings in the information presented in the report to allow general conclusions on the necessity of the instrument."[626] The EDPS furthermore criticizes the fact that the Commission did not fully consider whether a system of data preservation, or other less privacy-intrusive alternative means, could fully or partly substitute the current data retention scheme.[627] Last but not least, the current Directive lacks 'foreseeability', in particular when read in conjunction with the ePrivacy Directive.[628]

3.3.3 Other EU developments

Apart from the ongoing processes of revision of the Data Protection Directive and the Data Retention Directive, it is important to note that at least three other tracks of legislative developments are currently taking place. One of these tracks (the negotiations for the establishment of a EU-US agreement on data protection) directly concerns the development of the EU data protection framework. The other two tracks concern the evolution of the EU data protection and privacy frameworks in a more implicit way, as we will see in the discussion about the negotiations of transatlantic security or police cooperation agreements, or the EU development of a European PNR system. Both initiatives are relevant for this chapter because they touch upon surveillance-relevant issues, such as new "digital border controls", or aim to integrate ad hoc data protection frameworks or provisions (in the case of EU and transatlantic PNR systems). Given that attention has been already devoted to the case of the PNR systems in Part 2, and that the data protection provisions of new border controls have not yet been presented, the rest of the section will rather focus on the evolution of the EU-US data protection framework.

EU-US data protection framework

The High Level Contact Group (HLCG)
The High Level Contact Group (HLCG) was established by a decision of the EU-US JLS Ministerial Troika on November 2006. The goal was two-fold: to enhance transatlantic cooperation in data- and information-sharing while ensuring data protection and privacy rights. Since the first meeting, the HLCG worked to "identify and define a set of core

[626] European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Evaluation Report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/Ec)," (Brussels: European Data Protection Supervisor, 2011), 9. Available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf

[627] Ibid., 11.

[628] Ibid., 14.

principles on privacy and personal data protection, acceptable as minimum standards when processing personal data for law enforcement purposes".[629] The three most important outcomes of the HCLG activities where synthesized in a final report that was released in 2008. The group identified 12 common principles and five pending questions.[630] Furthermore, they developed "common language" for all the common principles, and, later in the same year, also for three out of five pending issues. Finally, they proposed two policy options, one leading to a "soft law" instrument, or non-binding agreement, and the other to a binding agreement, providing further guarantees and safeguards.

The first political feedback on the report indicated that there was more support for the second option, which explains the decision of the Commission to adopt, and submit to the Council, a draft mandate for negotiating a EU-US data protection agreement.

Before presenting the main points of the draft mandate, some of the open questions left open by the HLCG final report should be kept in mind. First, the HLCG itself was not able to "fix" all the outstanding issues, and even the common language of specific core principles proved difficult to establish. Second, it is also important to note that the resolution of some conflicting interpretations of common principles could be properly done only by the adoption of binding international treaty, and not by a more commonly used executive agreement. Third, while the differences in the definition of "law enforcement" on the two sides of the Atlantic were dismissed as minor by the HLCG, they are crucial because they risk to open the way to "purpose deviation".

Commission Draft Mandate for a EU-US data protection agreement

The Commission draft mandate was presented in May 2010, and it was preceded by a public consultation held in the first months of 2010.[631] According to the draft, the purpose of future transatlantic agreement "shall be to ensure a high level of protection of the fundamental rights and freedoms of individuals when personal data are transferred and processed to and by competent public authorities of the European Union and its Member States and the US".[632] The scope of data transfers is limited to the "purpose of preventing, investigating, detecting or

[629] Council of the European Union, "EU US Summit, 12 June 2008. Final Report by EU-US High Level Contact Group on Information Sharing and Privacy and Personal Data Protection," (Brussels: Council of the European Union, 2008), 3.

[630] The list of common principles includes: (i) Purpose Specification/Purpose Limitation; (ii) Integrity/Data Quality; (iii) Relevant and Necessary/Proportionality; (iv) Information Security; (v) Special Categories of Personal Information (sensitive data); (vi) Accountability; (vii) Independent and Effective Oversight; (viii) Individual Access and Rectification; (ix) Transparency and Notice; (x) Redress; (xi) Automated Individual Decisions; (xii) Restrictions on Onward Transfers to Third Countries. The pending questions were: (i) Consistency in private entities' obligations during data transfers; (ii) Equivalent and reciprocal application of privacy and personal data protection law; (iii) Preventing undue impact on relations with third countries; (iv) Specific agreements regulating information exchanges and privacy and personal data protection; and (v) Issues related to the institutional framework of the European Union and the United States, Ibid. For a critical overview of the works of the HLCG, and in general on EU-US negotiations in privacy and data protection matters, cf. Hiroyuki Tanaka et al., "Transatlantic Information Sharing: At a Crossroads," (Washington: Migration Policy Institute, 2010), 34-38.

[631] European Commission, "Proposition De Recommandation Du Conseil Autorisant L'ouverture De Negociations En Vue D'un Accord Entre L'union Européenne Et Les États-Unis D'amérique Sur La Protection Des Données Personnelles Lors De Leur Transfert Et De Leur Traitement À Des Fins De Prevention, D'investigation, De Detection Ou De Poursuite D'actes Criminels Y Compris Le Terrorisme, Dans Le Cadre De La Cooperation Policiaire Et Judiciaire En Matiere Penale," (Brussels: European Commission, 2010).

[632] §1 of the Negotiating Directives, Ibid.

prosecuting crime, including terrorism".[633] In this respect, the draft mandate limits forms of police and judicial cooperation to what is established in the relevant parts of title V of the Treaty on the Functioning of the European Union. Apart from the basic principles of data protection, the draft mandate provides for very interesting, and partially innovative elements. Firstly, it foresees a wide application of the future agreement, both in relation to actors, EU institutions, bodies, offices and agencies, EU Member States and US public authorities;[634] as well as in relation to other data protection and processing instruments, including all existing EU and Member States transatlantic agreements.[635] In practice, "after a transitional period of three years", PNR, Prüm-like and other agreements should be brought in conformity with the, generally more restrictive, guarantees provided by the overall transatlantic data protection agreement.[636]

Second, while the draft mandate acknowledges the relevance of the HLCG work, it goes beyond that, and clearly calls, *inter alia*, for the protection of all data subjects without discrimination on grounds of nationality; for the introduction of the principle of data minimization and the definition of "appropriate time limits for erasure"; for the obligation of security breaches; for the rights of both administrative and judicial redress; and even for the right to compensation.[637] In this sense, the draft mandate not only takes a strong stance in relation to pending questions highlighted by the HLCG, but even adds further safeguards. This is also the case in relation to independent public authorities, in relation to which the draft mandate not only establishes specific requests in terms of capabilities, but also foresees a "cooperation mechanism (…) with a view to effective Implementation of the Agreement".[638]

The main critical point is the national security exemption foreseen in the text. There, the draft mandate states that the agreements' provision shall not apply to criminal intelligence "concerning essential national security interest and specific intelligence activities in the field of national security".[639] In the same paragraph, the draft mandate also states that the agreement "shall include a narrow definition of national security interests in order not to unduly limit the scope of the agreement".[640] However, both the phrasing of the paragraph and its content are problematic. In fact, on the EU side there is no definition at all of what "national security" is,[641] while on the US side "national security" encompasses a very wide range of activities, including most of the practices of data sharing and processing analyzed in part one. It is therefore not really clear what the effective extension of the exclusionary clause could be.

3.3.4 The CoE Committee of the Ministers on profiling

[633] §1 of the Negotiating Directives, Ibid.

[634] §6 of the Negotiating Directives, Ibid.

[635] §4 of the Negotiating Directives, Ibid.

[636] §4 of the Negotiating Directives, Ibid.

[637] §7 of the Negotiating Directives, Ibid.

[638] §9 of the Negotiating Directives, Ibid.

[639] §11 of the Negotiating Directives, Ibid.

[640] §11 of the Negotiating Directives, Ibid.

[641] The lemma "national security" is mentioned only one time in the full text of the TFEU, in article 73, in reference to cooperation between Member States' departments, but outside the framework of police and judicial cooperation (thus, *de facto*, refers to secret services). It also appears in the Schengen Convention, but also there it refers to Member States internal security, and not to a possible EU-wide form of security.

In November 2010, the Committee of the Ministers of the Council of Europe adopted a Recommendation concerning "the protection of individuals with regard to automatic processing of personal data in the context of profiling".[642] This short, non binding, text is particularly interesting for the scope of chapter because it touches upon one of the most important (and sensitive) features of many smart surveillance practices: profiling. Furthermore, as discussed in Part I, the EU legal framework still lacks a proper legal definition of profiling and an explicit legal instrument tackling it, and the European Parliament has already advanced a request to the Commission to fill the gap.

In the recitals, the Recommendation highlights clearly the explicit dangers and the implicit challenges of profiling. On the one side, it notes how "the lack of transparency, or 'invisibility', of profiling and the lack of accuracy (…) can pose significant risks for the individual's rights and freedoms", and that "the use of profiles, even legitimately, without precautions and specific safeguards, could severely damage human dignity, as well as other fundamental rights and freedoms, including economic and social rights".[643] On the other side, the text makes the peculiarity of this type of process vis-à-vis more classical forms of data processing explicit, thus, implicitly, calling into question the ability of the notion "personal data" to provide effective protection. On the nature of the processing, it states: "through this linking of a large number of individual, even anonymous, observations, the profiling technique is capable of having an impact on the people concerned by placing them in predermined categories"; and that "profiles, when they are attributed to a data subject, make it possible to generate new personal data which are not those which the data subject has communicated to the controller or which she or he can reasonably presume to be known to the controller".[644] However, the Recommendation does not formally put into question the notion of "personal data" when it comes to adopt a definition, which remains mostly inspired by the wording of the COE Convention 108.[645]

The two most relevant sections of the Recommendation are section 3, lying down the criteria for a lawful use of profiling; and section 6, establishing exceptions and limitations. Most of the criteria established for "lawful profiling" are drawn both from "classical" data protection principles, such as purpose limitation, data quality, (limited) data retention and data adequacy; and from the "lawfulness test" established on the basis on art.8(2) ECHR. In particular, section 3.4 states that:

> "Collection and processing of personal data in the context of profiling may only be performed:
> a. if it is provided for by law; or
> b. if it is permitted by law and:
> - the data subject or her or his legal representative has given her or his free, specific and informed consent;
> - is necessary for the performance of a contract to which the data subject is a party or for the implementation of pre-contractual measures taken at the request of the data subject;
> - is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the personal data are disclosed;

[642] CoE Committee of Ministers, "Recommendation Cm/Rec(2010)13 of the Committee of Ministers to Member State Son the Protection of Individuals with Regard to Automatic Processing of Personal Data in the Context of Profiling," (Strasbourg: Council of Europe, 2010).

[643] Ibid.

[644] Ibid.

[645] "'Personal data' means any information relating to an identified or identifiable individual ('data subject'). An individual is not considered 'identifiable' if identification requires unreasonable time or effort", Ibid., § 1(a).

- is necessary for the purposes of the legitimate interests of the controller or the third party or parties to whom the profiles or data are disclosed, except where such interests are overridden by the fundamental rights and freedoms of the data subjects;
- is necessary in the vital interests of the data subject".[646]

It is also important to note that in the same section three other elements are added: first, personal data used in the context of profiling should be anonimized as soon as possible; and, second, information and access to public goods and services should be possible without having to communicate personal data to the goods or services provider. .[647] The third element is a general prohibition on "the distribution and use, without the data subject's knowledge, of software aimed at the observation or the monitoring in the context of profiling of the use being made of a given terminal or electronic communication network", which can be permitted only when "provided by domestic law and accompanied by specific safeguards".[648] The second section is also particularly relevant for the scope of this chapter, because it provides for a wide set of exceptions and restrictions to the criteria mentioned above. Indeed, in section 6, the Recommendation states that "[w]here it is necessary in a democratic society for reasons of state security, public safety, the monetary interests of the state or the prevention and suppression of criminal offences, or protecting the data subject or the rights and freedoms of others, member states need not apply the provisions set out in Sections 3 (…), where this is provided for in law".[649] Such a wording allows for important limitations to the very criteria established in the same document for a really broad range of policies. What is more noteworthy is that even if two important criteria (the necessity and lawfullness test) remain valid, the exceptions are formulated in such a way that most of the added value of the instrument risks to be lost. For example, all the criteria touching upon the technical quality and architecture of surveillance measures are no more clearly defined or ensured, unless the national legislators adopt, de facto, the same guidelines provided in the abrogable sections of the Recommendation.

Also, such a vast case of exceptions conveys do not permit to clarify cases the most "border-line" cases in which the private and the law enforcement spheres tend to overlap, or articulate one on the other.

3.4 CONCLUSIONS: SOME ELEMENTS TO GO BEYOND THE STATE OF THE ART

This chapter has offered a legal analysis, in terms of fundamental rights, of smart surveillance. Its goal was to advance a state of the art to pave the way to further analysis and research. Below, we propose seven elements, or points of reflection, to advance beyond this first move.

(i). Smart surveillance and data minimization?

Calling a measure 'smart' might raises the expectation, from a legal point of view, that a measure will be targeted to a specific individual, thereby reducing adverse effects on others. This meaning of 'smart' also correlates with the principle of data minimization that as little as

[646] Ibid., § 3.3.

[647] Ibid., §§ 3.3 & 3.7.

[648] Ibid., § 3.8.

[649] Ibid., § 6.

possible data should be actually gathered. Hence, data minimization should not only affect smart surveillance at the moment of data collection, but also its core data processing features, which should be able to generate knowledge out of a limited data-set. Such a possible conceptualization of smart surveillance seems particularly promising from a human rights perspective, as it would dramatically reduce its possible negative impact. However, two caveats should be taken into account. The first concerns EU policies trends. While the Commission for instance supports this principle of data minimization in its communication on the reform of the Data Protection Directive, it nevertheless accepts that this 'smart' principle is not entirely appropriate in a law enforcement context. This is nowhere more obvious than in its review of the Data Retention Directive.

The second caveat is based on an analogy with 'smart sanctions'. Smart sanctions (such as the freezing of assets or imposing of travel restrictions) against certain individuals or groups were originally introduced by international actors such as the EU and the UN as a response to the criticism that sanctions against states, for instance through trade restrictions, were a too blunt instrument that affected the humanitarian situation of complete populations.[650] While such smart sanctions indeed stopped the general suffering of these populations, they did not turn out to be a panacea to pressurize repressive regimes into accepting change. Various reports have shown how targeted sanctions have been characterized by severe due process concerns (in the case of terrorist listings for example) or cases of mistaken identity on the basis of wrongly spelled names.[651]

(ii). Scalable data gathering

As discussed in Part II of the present chapter, some surveillance technologies can be transformed in 'smart' ones by the adoption or inclusion of specific features. For example, from a fundamental rights perspective, neither body scanners or smart CCTV cameras for instance store data until the system notices a 'dangerous' object (in the case of body scanners and some smart CCTV systems) or a dangerous 'situation'. As such, these smart surveillance techniques are therefore perceived as a form of tailored surveillance, in which data gathering is somehow scalable: stand-by observation without ongoing retention of data, or, in the case of advanced body scanners, generation of personal data. An operator working at an airport, in a CCTV control-room, or near a body scanner will only be interested in an individual when the system signals that 'something is wrong'. This leads easily into thinking that persons who don't trigger the pre-defined alerts of these smart surveillance systems won't be affected by their use, which, consequently, does not amount to an interference with their rights. Two elements should nevertheless be highlighted. The first concerns the productive effects of data protection on this evolution. For example, in the case of body scanners, it can be argued that the 'smart' technological solutions lately proposed have been a sort of response to data protection institutional and legal mechanisms. The second element concerns the issue of 'mere' data retention: when data are not always subsequently processed. Indeed, the European Court of Human Rights has made clear that the fact that information is only gathered and not always subsequently used in practice, is irrelevant for the application of Article 8 ECHR. Therefore, it represents in itself a form of intrusion in the private life, that should assessed according to the test established in art. 8(2) ECHR.

(iii). Machines operated surveillance: automatic non-discrimination?

[650] See for instance: David Cortright and George A. López, eds., *Smart Sanctions: Targeting Economic Statecraft* (New York: Rowman & Littlefield,2002).

[651] Iain Cameron, Report to the Swedish Foreign Office on Targeted sanctions and legal safeguards, 2002, http://resources.jur.uu.se/repository/5/PDF/staff/sanctions.pdf.

Another advantage seems to be that there is no risk of discrimination in using smart surveillance techniques, since it is the machine that selects persons for further investigation, and not an operator. In the case of body scanners and smart CCTV cameras no decision with a negative effect is taken without further verification by an operator. Smart surveillance technologies only help the operator to focus his attention to persons to whom – according to the machine – might be interesting to look further into. Preamble 20 and Article 3 (5) of the Commission's EU PNR proposal similarly provide that no enforcement action shall be taken by the PIUs and the competent authorities of the member states solely on the basis of the automated processing of PNR data.[652] In other words, smartness is performed by a re-distribution of roles between machines and human operators. Machines should ensure that the first shift is not biased by prejudices, then, the (same) human operators that were initially sidelined, are supposed to guarantee a fair judgment of the 'anomalies' spotted by machines. Such a rationality can foster the idea that surveillance by machines, which have a much greater surveilling capability compared to humans is, by default, less discriminatory, and therefore their use should be further extended in order to compensate human prejudices. This does not mean however that no discrimination concerns arise. The idea that machines per definition enforce "neutral" criteria is misleading. Since their 'nature' can not be presented as a guarantee against discrimination, their operations, and their interactions with other elements, should equally be the object of a series of controls, including ex-post checks, to ensure that discrimination is not taking place. In this sense, human verification is just an instrument, and not the definitive solution. Rather, the use of statistics proposed by the Fundamental Rights Agency in their 2011 EU PNR opinion could become an important step to ensure oversight on the entire surveillance process.

(iv). A comprehensive data protection framework and the private-public surveillance partnerships

The development and use of these smart surveillance technologies coincides with a major reform of Europe's data protection rules. The most important revision is the revision of the Data Protection directive, and some relevant trends in the review process are of particular importance to smart surveillance technologies. The potential adoption of a comprehensive framework (as proposed by the European Commission, the Article 29 WP and the EDPS) that provides the EU with a consistent data protection framework that also sets out the general principles for the former third pillar, would be a welcome development. Such a framework would in particular be helpful for solving the inextricable legal PNR-knot, but it is very relevant for the other smart surveillance techniques discussed in this chapter as well. Not all operators of smart CCTV cameras or body scanners resort under the law enforcement sector in certain member states; a comprehensive legal framework would help to overcome the uncertainty that is a result of blurring activities of the private sector and of the law enforcement sector. Such a comprehensive framework is likely to act as a counter-balance against the current overstretching of the purpose-limitation principle in the former third pillar as well. In this context it remains to be seen whether a comprehensive data protection framework would include a legal definition of profiling and data mining, and how article 7 of the 2008 Framework Decision would fit in such a decision.

(v). The notion of personal data

[652] A comparable provision has been included with regard to the tasks of the competent authorities in Article 4 (6).

The use of smart surveillance technologies shows more and more the limits of the notion of "personal data". Unfortunately, in the Communication of the Commission no real proposal is made, apart from a generic commitment to "ensure a coherent application of data protection rules, taking into account the impact of new technologies on individuals' rights and freedoms".[653] Ideally the new framework sets out the precise measures which a state should deploy to protect the 'legitimate interests' of a person, including by specifying which possibilities exist to lodge a claim for damages if the use of data processing by governmental organizations is in breach of Article 8 ECHR or other human rights.
As discussed above, data protection legislation can have effects on the 'evolution' of surveillance systems, for example by pushing for the use of limited amounts or limited sets of personal data. However, the paradoxical risk of some of these developments is that data protection loses its ability to apprehend them when data are not considered "personal". Therefore, more reflection is needed on how to maintain data protection relevant in front of specific technological developments.

(vi). Effectiveness

The German Constitutional Court ruled in 2006 that the use of a 'preventive' screening method towards a person would only be compatible with the proportionality requirement if it were shown that there was a "concrete danger" to national security or human life, rather than a general threat situation, as it existed since 11 September 2001.[654] If we apply this threshold to the use of body scanners, smart CCTV and PNR, it would be hard to say in general that there is now more need for these technologies. Furthermore, this lack of clarity concerning "concrete dangers" is often mirrored by the inability to assess the effectiveness of specific measures. This is an important issue, as effectiveness is an important element of the proportionality test, and 'blank cheques' are not an option in the field of surveillance. Still, many of these proposed systems are highly dubious in terms of their outputs. Since there are an infinite number of risks and only a limited (if not shrinking) amount of resources to spend priority should be given to those that ensure an added value in terms of effectiveness. It is therefore crucial that any adaption of 'smart surveillance' systems is accompanied by a proper impact assessment that examines not only the societal and fundamental rights impact, but also the economic impact of such a measure.[655]

(vii). Has privacy been left beyond?

It is abundantly clear from the sections above that most of the legislative attention on the European level is devoted to improving rules and legislation regarding data protection. Privacy is often only mentioned *en passant*, and is not explicitly taken into consideration. "Traces" of privacy remain, at least nominally in the relevant documents, in the notions of "privacy by design" and "privacy impact assessment", and in the generalization of the lawfulness test, which builds upon article 8(2) of the ECHR. The rule of thumb seems to be that a new, more coherent, comprehensive and updated data protection framework would ensure, as such, a better protection of the right to privacy. Put more bluntly: an abstract right to privacy functions better if it is substituted or exclusively translated by data protection

[653] European Commission, "Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions. A Comprehensive Approach on Personal Data Protection in the European Union," 6.

[654] Bundesverfassungsgericht (the Federal Constitutional Court) of Germany in decision BVerfG, 1 BvR 518/02, 4 April 2006, available at http://www.bverfg.de/ entscheidungen/rs20060404_1bvr051802.html

[655] Marie-Helen Maras, "The Economic Costs and Consequences of Mass Communications Data Retention: Is the Data Retention Directive a Proportionate Measure?," *European Journal of Law and Economics* (2011).

language. But – as we've seen in Part I – privacy is more than the protection of personal data. This observation is not only interesting for academic purposes, since it raises the issue of how to make full use of two distinct (even if overlapping) rights, and of how to articulate them to offer a better protection. Indeed, even in the case of the full implementation of all the institutional recommendations concerning the revision of the Data Protection Directive for instance, the right to data protection cannot be assumed as the only tool in dealing with smart surveillance practices. It is true that, at least from the point of view of many actors, most of the threats could be avoided via an expansion of data protection, not only in terms of policy areas or reach of rights, but also in terms of scope over the elements of the security assemblages, explicitly including human and non human ones. However, future research needs to put more attention to the evolving role of the right to privacy in a technology-driven 21st century, resisting the temptation to fully conflate it into the right to, and the legislation on, data protection. Such an effort is probably essential in order to assess the legitimacy of smart surveillance technologies, since a re-assessment building upon the right to privacy could render legal smart surveillance tools (from a data protection point of view) illegal in a not so for away future.

4 Citizens' perceptions on surveillance and privacy

Dara Hallinan, Michael Friedewald (Fraunhofer ISI); Paul McCarthy (Trilateral); Silvia Venier, Emilio Mordini (CSSC)

Security in the post 9/11 world has seen a rapid proliferation of surveillance technologies and expansion of surveillance practices in most Western societies. Discourse on these trends often characterises the issues as trade-offs or finding a balance between security, liberty, freedom, intrusions into privacy and the protection of individual and collective rights through data protection. Researchers have investigated public perceptions and attitudes towards surveillance practices and surveillance technologies, and the media have duly reported their findings. Public opinion plays an increasingly role in development and deployment of surveillance technologies and in the policy planning and decision-making process, in the private and public sectors. In the first sections of this report, we consider findings from various studies exploring privacy, data protection and security issues. We see these issues as being interrelated as we move to a consideration of how smart surveillance technologies in the future might be viewed by the public in terms of acceptance or resistance.

Data protection, privacy and security and public attitudes to these are difficult topics to address, theoretically as well as empirically. In the post 9/11 world security, whether justified or not, is often deployed in policy discourse as a trump card over privacy and data protection. These issues can be emotive, controversial, distant (at least from immediate individual concerns), difficult to understand with attitudes as a result difficult to aggregate to a common public position. Academic discourse on these issues, as we detail later, is at times rich and detailed but empirical research, involving public attitudes and perceptions, is beset by methodological difficulties and other limitations which suggest caution in drawing conclusions from results and findings.

Research and academic discourse in relation to data protection is more developed on private sector practices of surveillance and intrusions into the privacy of individuals. We present some findings from various studies exploring these issues in the following sections. In thinking about public sector practices of surveillance, especially where these are framed in a discourse promoting security through surveillance, we find extensive academic discourse but empirical research is arguably less reliable given the framing of research questions. For example, asking whether individuals would accept surveillance if this would prevent a terrorist attack, this would inevitably lead to acceptance of surveillance. Indeed, data protection frameworks in the EU have exemption clauses which Member States can invoke. These clauses come into play when Member States can demonstrate that exemptions to data protection are in the national interest and justified in order to improve public security. The definition of when it is in the national interest, or what is a proportionate response to perceived threats to national security, is generally wanting and open to wide interpretation.[656]

[656] We do however recount an example, the UK's National DNA database, where a Member State interpretation has been successfully challenged on page n.

These political and legal characteristics often as a result restrict public discourse, especially where governments negotiate or interact with other governments. They also restrict members of the public, individuals or collectively, being able to impact policy decisions in the context of surveillance and security. Where surveillance practices and technologies are driven or conducted by state actors, difficulties exist in access to redress mechanisms that might allow individuals to challenge these. One example would be body scanners where legislation enforces a policy of "no scan, no fly" at airports. As such, while the public can react quickly to private sector surveillance by changing service providers, this is not the case in respect of individual citizens and their respective governments. This does not preclude incidences of widespread public resistance, some of which we give as examples in the following sections. The strength or value of public opinion does vary when considering public and private surveillance practices and use of technologies.

Furthermore, one can ask specific methodological questions in how public opinion is measured, and of the most prominent research tool used to measure them, the survey. Public opinion surveys are carried out by different organisations or actors, for different rationales and with different purposes. Some studies make explicit reference to their objectivity while others wear their normative credentials in light of both empirical findings and motivational rationales. Surveys range in size from small to large and are often complemented (or followed up) by other forms of quantitative and qualitative research. Surveys can be relatively straightforward opinion surveys, asking simplistic binary questions to detailed investigations of public attitudes towards surveillance, security, privacy and data protection.

Some argue that quantitative surveys provide "thin" explanations of public attitudes and sentiments whereas in the case of surveillance, "thick" explanations based on qualitative research methods are much more informative. Reasons given to support this argument include reflections on the difficulty of conveying conceptual meanings in short survey formats, the importance of contextualisation for sometimes vaguely understood issues or concepts and the nuances that can be interrogated (through utilising such methods) in terms of appraising individual perceptions, beliefs and attitudes within a framework of exploring these collectively in publics.

We discuss some of these methodological problems in the following section as well as specific results from surveys. Research on the public's acceptance of or resistance to surveillance is extensive and our report is not an exhaustive analysis of all studies or research. However, we do attempt to synthesise some of the key findings and research objectives of different pieces of research that have been conducted.

Based on a review of public opinion surveys and other research and academic discourse, one can make several points about the public's acceptance of surveillance, as follows:

- Public acceptance or rejection of surveillance is rarely a simplistic, binary proposition even though
- Policy discourse often presents choices on surveillance in simplistic, binary terms, e.g., security vs. privacy, liberty vs. safety.
- Surveys sometimes present questions in these terms, and consequently can be criticised as to how valid their findings are.
- Some technologies and practices of surveillance are rejected more than others, and this qualified rejection depends on whether these are seen to target specific categories or groups or are more generally targeted.

- There are definite cultural and social differences between Member States in the EU and between the EU and third countries with regard to the acceptance of surveillance technologies and practices.
- There are also definite differences between different demographic groups.

These represent a snapshot of some of the key issues that empirical research with publics reveals. The rest of this report explores these in detail and notes where surveys and research indicate other important factors determining the public's acceptance or rejection of surveillance practices and technologies.

4.1 ON PUBLIC OPINION SURVEYS IN GENERAL

Public opinion is a notoriously difficult substance to judge. The diverse nature of 'the public', the nuance and subtlety contained within the creation and manifestation of each individual's opinion and the constant shift of the context of judgement make certain of this. This is particularly true in relation to complex, consequential, publicised, value laden and abstract issues such as privacy, data protection, surveillance and new technologies.[657] However, public opinion is a core aspect of democratic policy making. It is thus no surprise that tools offering metrics and scales through which opinion can be summarised and perceived have become increasingly popular with policy makers and those pursuing other political agendas, particularly in relation to politically or socially murky issues.[658] They allow, on the one hand, a comprehension of, and adaptability to, the needs and desires of the public and on the other, as tools themselves, in a highly symbiotic process of opinion creation and communication, they provide those who control them with a degree of influence over public opinion itself.

Public opinion surveys are amongst the most used and influential of these tools but are far from perfect and come with a range of flaws which circumscribe their accuracy and should temper their use in the policy process. As we discuss in our review of academic discourse in relation to surveillance, security, privacy and data protection, the nature and complexity of the "public" in relation to these have seen a number of theoretical developments. These include the promotion of new methodologies, emphasising engagement, on how to conduct research involving the public. Academic debates suggest caution in how we view traditional research on public opinion such as surveys. Where studies seek to generalise from conclusions, which do not stand up to critical scrutiny, their value as revelations of public attitudes and opinions can be questioned.

Actors wishing to use particular surveillance technologies often present issues in polarised ways, especially where security is at stake. When surveys present issues using relatively vague concepts such as security versus liberty, without specifying what is meant by each of these concepts, then public opinion and attitudes towards security are difficult to evaluate in a credible fashion. Also where research is conducted on the part of particular advocacy groups, whether they are in favour of surveillance to ensure security or are against it, then one needs to exercise caution. One needs to pay attention to the particular motivations that frame the rationale and reason for the research.

---

[657] Harper, Jim, and Solveig M. Singleton, "With A Grain of Salt: What Consumer Privacy Surveys Don't Tell Us", 2001. http://ssrn.com/abstract=299930.

[658] Herbst, Susan, *Numbered voices: How opinion polling has shaped American politics*, University of Chicago Press, Chicago, 1993. Burstein, Paul, "Bringing the public back in: Should sociologists consider the impact of public opinion on public policy?", *Social Forces*, Vol. 77, No. 1, 1998, pp. 27-62. Monroe, Alan D., "Public opinion and public policy", *Public Opinion Quarterly*, Vol. 62, No. 1, 1998, pp. 6-28.

4.1.1 Survey Motivation

The first set of issues can be framed as the presence of underlying motivations, the 'who and why', in the final product. This manifests either in the presence of a direct link between the background to the creation/commissioning of the survey and the results it reports or in an indirect link between the motivation of the organisation involved and the refraction of results this causes.

Actors have a variety of motivations for attempts to directly influence policy processes or public opinion. In relation to *corporations*, for example, Etzioni has commented on how investment in the influence over public policy can be more lucrative than investment in product development, whilst for certain organisations involved in the collection and processing of personal information the development of the privacy legislative debate and environment could define the terms of success or survival.[659] In the policy process, as well as in the process of influencing public opinion itself, information can be viewed as a subsidy. As Gandy comments, "by reducing the cost of acquisition, the subsidy giver expects to increase the probability that the target of the subsidy will consume more of the preferred information".[660] In this respect, public opinion surveys can be seen to be informational currency within a wider process and whilst the use of the information contained depends on its perceived accuracy and unbiased nature, the reality of its inception can belie this fact.

Other actors have their own broader goals and motivations that may lead to result corruption in a more indirect sense. The *media*, for example, has a key role to play in the public opinion process and as such has taken an increasingly large role in the production of, and comment upon, surveys on a variety of issues including privacy. As Haggerty and Gazso comment, not only do methodological considerations and limitations "make poor copy", but the logic of media reporting which "prioritizes deviance, action and individualized dramatic narrative" may lead neither to objective reporting of survey results, nor, in the sense that a media commissioned survey blurs the line between reporting and making the news, to a focus on objectivity in the original purpose for the survey.[661]

Finally, the *organisations entrusted with carrying out surveys* have their own interests at stake. These organisations have their own internal political economy to consider when conducting surveys which may "necessitate that they produce quick results from the smallest possible sample size".[662] Whilst this is not always the case, the implications of this for the reliability of the data may be significant. The issue is amplified as the pollsters who conduct the surveys may themselves provide extrapolation on the resultant information. This presents issues not only in terms of obscuring data deficiencies, but also potentially adds an observational bias to the data themselves, which may itself be influenced by the original motivation for the survey.

---

[659] Etzioni, Amitai, *The Moral Dimension*, The Free Press, New York, 1988.

[660] Gandy, Oscar H., "Public Opinion Surveys and the Formation of Privacy Policy", *Journal of Social Issues*, Vol. 59, No. 2, 2003, pp. 283-299.

[661] Haggerty, Kevin D., and Amber Gazso, "The Public Politics of Opinion Research on Surveillance and Privacy", *Surveillance & Society*, Vol. 3, No. 2/3, 2005, pp. 173-180.

[662] Ibid.

4.1.2 Methodology

Response rates and survey bias may be significant in the consideration of surveys relating to privacy and surveillance but are not always mentioned or considered broadly enough to reflect or correct for the potentially significant non-random element of non-response and consequently the significant methodological limitations this may represent. Within the specifics of each survey process are features which will build disproportionate bias against one or more groups of the population targeted into the final results of the survey.[663] Working from the observation that surveys are themselves a form of surveillance, the argument then runs that when the survey concerns privacy or surveillance this non-random non-response bias gains special significance. Individuals concerned about privacy issues may preference behaviours that are not conducive to their inclusion in surveys, for example by having unlisted numbers, by screening phone calls or by not engaging in behaviour (for example swapping information for reward online) that would result in their appearance on sample framing databases. This in turn makes extrapolations of data supposedly reflecting 'public opinion' potentially incorrect and non-representative, presumably biased against privacy interests.[664]

The blunt nature of the survey process itself also comes fraught with structural and methodological issues. This is particularly true in relation to complex and abstract issues such as privacy. In the creation of surveys, it is often the case that the questions, or even the theme, of a poll are inaccurately or misleadingly formulated. For example, Harper and Singleton point out "many different concepts are often grouped together under the heading of "privacy," including security, identity fraud, spam...Polls often compare not only apples and oranges, but toss in pears, mangoes and persimmons as well".[665] As a consequence it is not always certain that the questions have been interpreted in a uniform, or even the intended, way. Any consequent analysis may then be built on a set of assumptions uncertain or invalid for the respondent answers.

In addition, surveillance practices and technologies are often conflated, while one is often linked to the other in debates. Evidence from some research suggests that the public has a more nuanced view. In other words, the public can accept the general notion of surveillance but not how it is achieved through the deployment of particular technologies.[666] However, these findings vary from country to country and from technology to technology as well from practice to practice. Lyon, for example, has found support for national ID cards varying from 43.7% in France strongly agreeing with the introduction of an ID card to only 19.2% strongly agreeing in the USA.[667] Lyon also reports that in countries where citizens already use ID cards, this level jumps significantly with 77% in Hungary strongly agreeing. In a question asking how effective respondents thought governmental actors would be a protecting a national database (which might complement an ID card), Lyon notes that answers even in

[663] Groves, Robert M., Robert B. Cialdini, and Mick P. Couper, "Understanding the Decision to Participate in a Survey", *Public Opinion Quarterly*, Vol. 56, No. 1992, pp. 475-495.

[664] Haggerty, Kevin D., and Amber Gazso, "The Public Politics of Opinion Research on Surveillance and Privacy", *Surveillance & Society*, Vol. 3, No. 2/3, 2005, pp. 173-180.

[665] Harper, Jim, and Solveig M. Singleton, "With A Grain of Salt: What Consumer Privacy Surveys Don't Tell Us", 2001. http://ssrn.com/abstract=299930.

[666] Katz, James E., and Annette R. Tassone, "Public Opinion Trends: Privacy and Information Technology", *Public Opinion Quarterly*, Vol. 54, No. 1990, pp. 125-143.

[667] Lyons, David, "National ID card systems and social sorting", in Zureik, Elia, Lynda Harling Stalker, Emily Smith et al. (eds.), *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, McGill-Queen's University Press, Montreal, 2010, p. 243

cases of strong acceptance of ID cards show a drop off in support, with only 11% of Hungarians saying protection would be effective.[668]

Research involving surveillance technologies, no matter whether they are well established as is CCTV or new such as smart surveillance technologies, faces an immediate problem of a lack of understanding or knowledge by the public as to the workings, uses and possible impacts of the technology.[669] Some research has approached this problem by employing a deficit model and we discuss this and criticisms of it below in the section on academic discourse. Surveys are an inherently limited research tool in explaining complex issues and in explaining technologies in a way that would render any findings meaningful: they must be refined when approaching topics of security, surveillance, privacy and data protection.[670]

Then, the specifics of survey design, such as the ordering, wording and range of questions can restrict the scope of response or weight the respondents answer in a certain direction.[671] Considering the polled question, "how concerned are you [that]...the company you buy from uses personal information to send you unwanted information?", Harper and Singleton point out that, considering no one wants to be sent unwanted information, it should come as no surprise that 78% of respondents claimed they were "very" or "somewhat" concerned.[672] The logic does not run however, that these people were against unsolicited mail as such, which was the supposed topic of the poll.

Finally, the question format (one which generally lends itself to the eventual extraction of percentage values) does not provide a base form which to judge subtle and nuanced opinions or from which to build pictures of more complicated models of perception.

Following from the above, the interpretation of data collected can be equally problematic. Any given answer (this is particularly true in surveys that ask respondents to rank on a given scale) is taken as part of a greater body of answers comprising the survey. However, considering individuals are often not given objective reference points for scale, nor are perceived reference points often collected or reflected in survey results, the difference between understandings may mean answers, as they were meant, are in fact incomparable despite terms being understood uniformly.

Further, there are a range of contextual factors, such as cultural or linguistic differences, which in themselves skew perceptions and responses. Thus as the survey geographical area, sample size or breadth of topic grow, the comparison of answers may become increasingly flawed.[673] The opposite is also true. The extrapolation of results to areas which were not

---

[668] Ibid, pp. 244-245

[669] Monahan, Torin, (ed.), *Surveillance and security: technological politics and power in everyday life*, Routledge, New York, 2006.

[670] Zuriek, Elia, "Methodological considerations", in Zureik, Elia, Lynda Harling Stalker, Emily Smith et al. (eds.), *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, McGill-Queen's University Press, Montreal, 2010, pp. 5-7

[671] Sheehan, Kim Bartel, "How public opinion polls define and circumscribe online privacy", *First Monday*, Vol. 9, No. 7, 2004, pp. http://firstmonday.org/issues/issue9_7/sheehan/index.html.

[672] Harper, Jim, and Solveig M. Singleton, "With A Grain of Salt: What Consumer Privacy Surveys Don't Tell Us", 2001. http://ssrn.com/abstract=299930.

[673] Zureik, Elia, and L. Lynda Harling Stalker, "The Cross-Cultural Study of Privacy: Problems and Prospects", in Zureik, Elia, L. Lynda Harling Stalker et al. (eds.), *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, McGill-Queen's University Press, Montreal, Kingston, 2010a, pp. 8-30.

included in the original survey may apply a template which does not consider key contextual factors, perhaps rendering the extrapolated results invalid.

Finally, answers may not even reflect genuine opinions or understandings of issues. On the one hand, answers to survey questions may be given dependant on what respondents believe the interviewer wants to hear or what the respondent presumes the correct, or socially acceptable, answer to a question to be. Equally, considering the perceived disposability of the nature of the interaction on the part of the participant, the survey process can elicit a disposable or unconsidered response from a participant. This is particularly true when surveys consider issues to which a respondent may not have given much prior thought or which are of seemingly less direct relevance to the respondent's life. As a consequence answers may suggest opinion (which may consequently appear to suggest preference for one policy option or another) which may contain unconsidered, hidden or potentially contradictory implications or which may simply be inaccurate or based on flawed assumptions.[674]

Finally, the format does not allow a replication of the set of trade offs a respondent may face in real life. As such, and in combination with the above points, public behaviour offer differs starkly from survey results. It is clear that, although the framework of behaviour and that of opinion can differ without contradiction (one can dislike something, but still do it, out of necessity or because it brings greater benefit in a wider calculation), there is a risk in reflecting one without consideration for the causes of its misalignment with the other. For example, whilst an objective study of server traffic found cookies to be disabled only 0.68% of the time, in an Arthur Anderson survey on the same issue 12% of respondents suggested they disabled cookies.[675]

4.1.3 Restriction to Use in the Policy Process

In the European model of democratic society, it is not the job of the policy maker to simply follow the public will, but rather to act as an overseer of a variety or interests and principles of which the public will should not be the absolute factor. In this sense allowing public opinion, even if one assumes its accuracy, to guide political choices is not necessarily good policy making.[676] Against this though, at least in the case of security and surveillance, is the argument that policy-making in this field has been and continues to be somewhat insensitive to public opinion. Instances of widespread public resistance to surveillance practices and technologies which have resulted in concrete policy changes are few and far between. Most involve a level of general public resistance that makes it political suicide for policy-makers to ignore and obscure how particular categories within the public, who suffer disproportionate amounts of surveillance practices, may have little if any impact even if their views and opinions are reported.[677]

In contrast to public sector examples, private sector incidences of resistance to surveillance and "voluntary" changes in policies and practices by actors as a result of this resistance are more common. Examples include the resistance, rejection and retraction of Facebook's Beacon "service". The demise of NebuAd in the US and Phorm in the UK, both engaged in

---

[674] Haggerty, Kevin D., and Amber Gazso, "The Public Politics of Opinion Research on Surveillance and Privacy", *Surveillance & Society*, Vol. 3, No. 2/3, 2005, pp. 173-180.

[675] Harper, Jim, and Solveig M. Singleton, "With A Grain of Salt: What Consumer Privacy Surveys Don't Tell Us", 2001. http://ssrn.com/abstract=299930.

[676] Ibid.

[677] Martin, Brian, "Opposing Surveillance", *IEEE Technology and Society*, Vol. 29, No. 2, 2010, pp. 26-32

behavioural advertising, provide another example of successful public resistance (stoked, of course, by privacy advocacy groups, the media and some politicians). This illustrates that the public has some power as consumers, perhaps more than they do as citizens. Grenville identified 33% of respondents to the survey conducted as part of the Globalisation of Data Project as being "alienated sceptics", arguing they "do not trust the government" and "seem to have largely given up hope of being able to have control over their information".[678] That a large section of the public might have this feeling raises a number of questions about surveys, democratic processes and how policies are formulated in public and private sector settings.

Apart from the limitations on the data itself and the implications this can have for its use in the policy process, it must also be borne in mind that surveys, by design, have a limited context and thus can suggest certain facts only in relation to their own narrow contexts. Thus polls do not include a weighing of issues against broader social or economic concerns or costs, or elucidate the specifics of their definition, context or enactment into policy. Reliance on survey data thus may relegate sensible policy options by presenting an overly simplified or biased view of an issue with far wider reach or consequence.

It can also be argued that surveys are a snapshot of a particular time or moment of when the research is conducted. They are then of interest as an archaeology of public sentiment and attitudes at these times. Surveys only rarely make reference to the events, contexts and time-specific issues that are at play in society at the time the research is carried out. On the other hand, surveillance and security are often emphasised at particular moments in time (e.g., following a terrorist attack). One can question the validity of the findings when surveys are carried out in the wake of a terrorist attack, as the incident might have led to participant bias.

4.1.4 Discussion

Public opinion is an important part of any political or social discussion and surveys can be a useful tool in its measurement. However, as is demonstrated admirably by the range of contradictory survey information supposedly from the same target audience about the same issues, their data is often flawed and should be informed by an awareness of the above methodological and contextual issues it raises.[679]

Ideally, objectively unbiased surveys, with as defined a context and set of questions as possible, when necessary combined with the use of balancing tools such as vignettes[680], should be sought. Surveys data should be informed and used alongside a host of other opinion collection and referencing tools, such as ethnographic research, open and closed interviews and focus groups and complaint monitoring.

---

[678] Grenville, Andrew, "Shunning surveillance or welcoming the Watcher", in Zureik, Elia, Lynda Harling Stalker, Emily Smith et al. (eds.), *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, McGill-Queen's University Press, Montreal, 2010, p. 76

[679] Sheehan, Kim Bartel, "How public opinion polls define and circumscribe online privacy", *First Monday*, Vol. 9, No. 7, 2004, pp. http://firstmonday.org/issues/issue9_7/sheehan/index.html.

[680] See for instance: Alexander, Cheryl S., and Henry Jay Baker, "The Use of Vignettes in Survey Research", *Public Opinion Quarterly*, Vol. 42, No. 1, 1978, pp. 93-104. Hopkins, Daniel J., and Gary King, "Improving Anchoring Vignettes: Designing Surveys to Correct Interpersonal Incomparability", *Public Opinion Quarterly*, Vol. 74, No. 2, 2010, pp. 201–222.

4.2 WHAT DOES THE PUBLIC KNOW ABOUT DATA PROTECTION AND PRIVACY?

Data protection and privacy are highly abstract and fluid concepts whose allocated importance and definition can be highly context dependant. This makes the consideration of public knowledge and opinion very difficult. While generalisable sentiments might be difficult, this does not preclude strong individual understanding and attitudes towards these topics. The relationship between these individual sentiments and how these are averaged out in a larger survey are key to understanding some of the limitations of large quantitative surveys. This is true not only of the topics in this report but also to surveys in general as a research tool.[681]

However there are perspectives which allow the question to be considered in more solid terms. The legal framework provides a solid reference point for the theory and importance of data protection and privacy in contemporary European society. This provides a first perspective; clarifying how (and to what extent) the public are familiar with the structure of protection and the balance and relationships of the rights in relation to the individual, society and other social goals. Using legal frameworks has also been important in some cases of public resistance, as it has been through these avenues that the most success in terms of overturning policy decisions on the implementation of particular surveillance measures has occurred.

The data protection principles and framework relevant for all European countries are set out in a series of international and European documents. The framework builds out generally from the principle of information self-determination whilst attempting to balance this against other legitimate uses of individual data. With its inclusion in Article 8 of the Charter of Fundamental Rights of the European Union[682], its status has been upgraded to that of a unique fundamental right.

Privacy protection manifests predominantly through its status as a fundamental human right, enshrined in both the European Court of Human Rights, ECHR and the Charter of Fundamental Rights and in a rich national and ECtHR case law. Whilst new technologies effect privacy, this piece will focus predominantly on data protection unless otherwise stated. This is as the environments discussed tend toward discussion in terms of data protection. A data protection approach provides a platform and perspective through which pertinent privacy impacts may be considered.

The framework is only operational against a real world background. As a legal instrument its effectiveness is thus restricted to how well it is enforced and how well it fits to, or can adapt to, the constant changes within this background. The second perspective thus considers how the public views the reality of the environment being regulated.

Over the past few years there have been considerable changes in the potential for data use. This has led to increased transfers, storage and replication across all social spheres and indeed even the creation of unique data environments. The background and regulatory environments to the rights will have been considerably changed as a result.

---

[681] Op. cit., Harper and Singleton, 2001

[682] "Charter of Fundamental Rights of 7 December 2000 of the European Union", *Official Journal of the European Communities*, C 364, 18.12.2000, pp. 1-22.

The surveys used in this section represent a variety of different approaches and scales and as such conclusions often represent certain extrapolations from data which vary in compatibility. As the section seeks to explore European attitudes, the key surveys have a Europe wide sample population. This unfortunately narrowed the number of useable surveys. When going further into depth in an issue, it was often necessary to use more local and in depth surveys. This posed further issues in relation to the general extrapolation of general conclusions from essentially local data (see below).

4.2.1 There Is More Then One 'Public'

This piece seeks to identify main trends and create an understanding as to how the European public at large understand and view data protection and privacy issues. However, it must be pointed out that the European public is a diverse body in which an enormous range of views and perspectives are present. There are a range of factors that can have an effect on perceptions and approaches toward data protection and privacy such as social status, political affiliation, income, education, profession and gender. The correlations of these factors to a stance can be very difficult to pick apart and each factor may play a greater or lesser role in relation to each issue.

Particularly significant appear to be nationality (and consequently national culture) and age (or more precisely familiarity with the digital environment). The differences between national results in surveys can be considerable. In Eurobarometer 359[683] for example, knowledge of the national Data Protection Authority varied from 51% in Hungary to just 16% in Spain. An expansion of this even reveals broader regional trends (for example a Scandinavian group perspective can be isolated). In the same survey there is a specific separation and investigation into the specifics of digital natives and initiates (those who were born and raised with, or subsequently became familiar with, digital technology) and other, predominantly older, respondents.[684]

Even when a viewpoint appears to be identifiable, the complexity of the issues involved means this is never monolithic and, considering the fluidity of understanding in relation to the technical and social background to each view, may be subject to qualification or change dependant on context of application or to circumstantial change.

Academic discourse and research are presented in section 2.2 which outlines some of the theoretical work in relation to these trends and publics, socieities and the development of technologies. This work can be placed in the context of the difficulties other areas have faced in assessing public attitudes and opinions.

Surveys exploring the general notion of security and its relationship with surveillance practices and technologies also display this problem. Varied conceptions, understandings of and differentiations between publics as to the meanings of security and surveillance are a

[683] TNS Opinion & Social, "Attitudes on Data Protection and Electronic Identity in the European Union", Special Eurobarometer 359, Brussels, 2011. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

[684] For broad considerations of factors influencing privacy and data protection conceptions see Bellman, Steven, Eric J. Johnson, Stephen J. Kobrin, and Gerald L. Lohse, "International Differences in Information Privacy Concerns: A Global Survey of Consumers", *The Information Society*, Vol. 20, No. 5, 2004, pp. 313–324. Samatas, Minas, "Studying Surveillance in Greece: Methodological and Other Problems Related to an Authoritarian Surveillance Culture", *Surveillance & Society*, Vol. 3, No. 2/3, 2005, pp. 181-197. Zureik, Elia, Lynda Harling Stalker, Emily Smith et al. (eds.), *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, McGill-Queen's University Press, Montreal, 2010b.

recurring theme in research. Different social, cultural and historical contexts influence factors determining the public's acceptance (or not) of surveillance practices and technologies. While there is no one public, one can argue that there is no one society. Although the European Union provides some common bases (such as legal), individual Member States and public responses in each in relation to the notion of security can often greatly diverge and are clearly deeply embedded in social, cultural and historical differences.

Public opinion surveys are of limited value in understanding the actual effects of surveillance on individuals. In research on private sector practices of surveillance, those who have (or percieve themselves as having) surveillance experiences express much stronger views. Also research on state surveillance often reports individuals not seeing survellance as an issue where it is seen only as targetting others who are risks or threats. As such, the limitations of understanding concepts might be extended to a limitation of understanding the ramifications and impacts that surveillance practices and technologies might have on living and participating in a society. Research from the perspectives of these others, and those who experience surveillance may have more validity in offering understandings of surveillance practices and technologies.

While clearly it is nonsensical to suggest that terrorists, for example, might be researched in a survey, other targets of state surveillance could be included in research. These targets include refugees, legal or illegal migrants or even some criminals who may or may not wish to participate in such research. In most cases, and framings in the way in which particular surveys are carried out, these others are deemed outside of normal society in terms of having any rights to avoid surveillance practices and technologies. They are seen as being outside and separate from society and in some cases are subject to even greater surveillance. In Europe, this trend has manifested itself in the increased popularity of right wing movements, which might suggest that policy discourses continually referring to threats have given ammunition to a general disenfranchment amongst some sections of European publics in different countries.[685]

4.2.2 What Does the Public Know About the Current Protection Framework?

With overarching relevance, it is necessary to bear in mind that the philosophical and social justifications of the right to privacy (and data protection) is incredibly difficult to define and is constantly changing with the development of society and law. As Post declares, "privacy is a value so complex, so entangled in competing and contradictory dimensions, so engorged with various and distinct meanings, that I sometimes despair whether it can be usefully addressed at all".[686] Thus even the use of legalislation as a certain manifestation is arguably in principle flawed. These ambiguities in understanding and definition at the most fundamental level influence the clarity of public perception, very likely making uncertain the relevance and operation of the framework generally as well as in relation to an (itself uncertain) quickly developing background, the calculation of its relationship with other rights, with individual action and its relevance in the light of other social goals.

[685] Kossowska, M., M. Trejtowicz, S. de Lemus et al., "Relationships between right-wing authoritarianism, terrorism threat, and attitudes towards restrictions of civil rights: A comparison among four European countries", *British Journal of Psychology*, Vol. 102, No. 2, 2011, pp. 245-259.

[686] Post, Robert C., "Three Concepts of Privacy", *The Georgetown Law Journal*, Vol. 89, No. 2001, pp. 2087-2098.

From the survey results it is clear that the public allocates data protection and privacy significant importance. Indeed in the 'Public Awareness Survey 2008' carried out on behalf of the Irish Data Protection Commissioner the privacy of personal information was ranked 3rd in order of importance (with 84% regarding it as 'very important') in a list of key issues, trailing crime prevention by only 3%.[687]

It is immediately evident that there is confusion (or at least an apparent lack of distinction) between privacy and data protection, although this is not explicitly stated in any individual survey (indeed many surveys appear to use the concepts interchangeably themselves). The privacy protection framework does not feature at all in respondents answers. Practically however, this can probably be explained firstly by considering the subject matter of surveys considered and their bias toward issues of data processing, secondly, in consideration of the symbiotic development and deeper justification for both rights there may be no need for the public to distinguish when considering broader issues and finally, the data protection framework simply has a more tangible set of laws onto which to grasp and references as to its sphere of operation. It is unlikely, for example, that a respondent will be aware of ECtHR case law defining privacy's bounds.

Whilst there seems to be a considerable variation between European countries in relation to their knowledge of protection frameworks and the protections they offer, it is notable that the majority of Europeans appear familiar with the key rights the data protection framework offers. For example, although a citizen's right to access data held by others' was the least known amongst respondents, the EU awareness average still sat at 59%.[688] However, it must also be noted that knowledge levels dropped when respondents were questioned as to the more subtle, abstract or complicated aspects of protection, such as the status of sensitive data or the situation relating to cross-border data flows.

There is not the same level of awareness regarding National Data Protection Authorities (NDPAs). In the same Eurobarometer[689], the EU average awareness of the existence of NDPAs sat at a low, 28%. Amongst those aware of the existence of local NDPAs, there was still considerable uncertainty as to their remit and capability (e.g. whether or not they could impose sanctions etc.). Although this may be partially explicable assuming an individual who has not had cause to complain may not be expected to have found out about a national authority, these figures do not align with knowledge of aspects of protection. This suggests an imbalance in awareness between the letter of protection and its operation in fact. Taken in combination with a lack of awareness regarding certain of the more subtle aspects of protection and with points which will be made later regarding a lack of awareness of the social aspect of data protection, a case can begin to be built for viewing the public's understanding as relatively superficial and limited to the letter of protection itself. It is thus no surprise that other more minor sectoral or supporting legislation made no appearance in any survey, nor were they brought up spontaneously by any lay respondent.

The status of data protection within the contexts of a wider legal order was rarely mentioned or apparently considered. On the one hand this is partially to be expected, not only as its elevation to the status of fundamental right has only been recent and through an instrument

---

687 Landsdowne Market Research, "Public Awareness Survey 2008", Data Protection Commissioner, Portarlington, Ireland, 2008. http://www.dataprotection.ie/documents/press/Survey08.pdf.

688 The Gallup Organization, "Data Protection in the European Union: Citizens' perceptions", Flash Eurobarometer 225, Brussels, 2008. http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

689 Ibid.

and means which may themselves not be so transparent or apparent to the individual citizen but also as the significance and consequences, both theoretically and practically are still uncertain. On the other hand, this is incongruent with an expected public awareness, understanding and familiarity with designated fundamental rights.

The above point brings into question how privacy and data protection within a wider system of law and society are understood and viewed. It is apparent that, although people are aware of the existence of rights they are not immediately aware of why they have manifested as they have, nor do they have appear to have given much thought to their social function. However when longer discussions ensued considering wider erosions of privacy and potential threats to individual data etc. participants began to voice fears based on the social dimensions of the rights, although they often found these difficult to elaborate and articulate. This perhaps demonstrates an imbalance in the public's concepts of privacy and data protection in relation to its dual individual and social function. This resonates with Solove's commentary, "Privacy is often cast as an individual right and balanced against the greater social good, which results in privacy being frequently undervalued".[690] There are factors which perhaps meditate toward making this so. Firstly, it is possibly not high on an individual's list of priorities to consider the social conception of any right, let alone rights as complicated and abstract as data protection and privacy. Secondly, the invisible and unknown environment in which data protection issues play out (this point will be returned to later) may make it difficult for the individual to conceive of social impacts, social importance or trace the consequences of aggregate action in a considered way. Finally, in considering the conception of the issue by the public, it is apparent that a number of reference points, for the conception of data protection, (for example online shopping considered in "the Effect of Online Privacy Information on Purchasing Behavior"[691]) come with a series of easily recognisable individual actions and trade offs, in which acts are seen in terms of isolated instances, as opposed to a reflection or involvement in issues which may have social significance.

4.2.3 Privacy, Data Protection and Security

The above analysis of an imbalanced conception is applicable to the evaluation of privacy and data protection in relation to other social goals and (presented) necessities. The most visible of these contexts is the debate surrounding privacy, data protection and security.
Research in relation to these contexts has been extensive and reflective of vigorous academic and policy debates. As befits the relatively controversial nature of the research area, survey research and conclusions (as well as the motivations to carry them out in the first place) at times diverge significantly. We present a synthesis of various surveys (and other pieces of empirical research) in the following paragraphs.

In 'A Surveillance Society: Qualitative Research Report', participant opinion is split into 3 attitudinal types, Acceptors, Authoritarians and Libertarians. The Libertarians, who formed the minority of the sample were those "who were more outward looking in their concerns, and more likely to think about society and their place in it".[692] Unsurprisingly this group were

[690] Solove, Daniel J., *Understanding privacy*, Harvard University Press, Cambridge, Mass., 2008b.

[691] Tsai, Janice Y., Serge Egelman, Lorrie Cranor, and Alessandro Acquisti, "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study", *Information Systems Research*, Vol. 2, No. 2, 2011, pp. 254-268.

[692] Murphy, Oliver, "A Surveillance Society: Qualitative Research Report", Report prepared for COI on behalf of ICO, Wilmslow, Cheshire, UK, 2007.
http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/surveillance_report_v6_final.pdf.

significantly more concerned about a security privacy trade off and met the issue with a series of principle based democratic and social arguments. However, the other groups, whilst differing in approach, viewed privacy from a predominantly individual point of view, detached from its social significance.

Authoritarians approached privacy strongly as an individual right rather than as a social good. This led directly to a balancing action[693] in which other goals whose social 'importance' was more easily referable (or had at least been more continually referenced) were prioritized. This led to positions such as "national security...and personal safety are of overriding importance: the common good is paramount", "the innocent will not be harmed or inconvenienced", "only the guilty are actively being watched, so I, as an innocent citizen, will not be 'picked out of the crowd' and if I am then I have nothing to hide".[694] In this set of arguments a broader set of consequences to privacy infringement is not present, in the blunt preference for security over privacy, many demonstrate a lop sided balancing process which fails to show a nuanced understanding of privacy's structural importance or the potential effects of increasing data flows and processing.

Acceptors viewed the right to privacy from the narrow, individual perspective, without wider consideration as to its social significance, apparently out of practicality. The complexity of the environment in which the balance was being carries out and the necessity of involvement in day-to-day activities which carried risk, seemed to dull perception of social consequence. This led to positions such as "someone, somewhere, will be looking after our best interests", accordingly "there was an assumption that there 'must be' laws against extreme abuse of data, although respondents tended to be rather vague about who or what this might be", and "the state and security forces are not institutionally malign or corrupt in intent; indeed they are there to protect us, the innocent citizen".[695] Realistically, this approach may be expected from individuals who lead their own lives and may not have considered the issue or the relevant structures in great detail and whilst these views undoubtedly also represent other issues such as the respondents trust for authority this does not obscure the fact that data protection and privacy issues, particularly on a social level were simply a perception black spot. There is concern, but through lack of understanding of structure there is equally a powerlessness to react to it. There were thus necessary presumptions made about the nature of unclear structures that allowed practical functionality without structural clarity (this will be returned to later).

Other surveys exploring these themes give a different perspective to the UK. In terms of a comparative analysis, two Eurobarometer studies provide insight into pan-European concerns as well as the differences and commonalities in public attitudes towards these issues in Member States. We have already mentioned some of the findings of these studies. While data protection was the main focus of both studies, findings relevant to issues related to security can also be found in both reports, specifically in the sections exploring data protection in the context of international terrorism. An important point, noted in the executive summary of the report of the Eurobarometer report on citizen's perceptions on data protection in the European Union, was that the public accepted that international terrorism would be one instance which

[693] 'Balancing' appears to be the predominant concept in many citizens' minds: If we want more security we have to give up privacy. Even if this is highly debated (or even rejected) in the academic community.

[694] Murphy, Oliver, "A Surveillance Society: Qualitative Research Report", Report prepared for COI on behalf of ICO, Wilmslow, Cheshire, UK, 2007.
http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/surveillance_report_v6_final.pdf.

[695] Ibid.

would allow for the suspension or restriction of normal data protection rights. The figures reported here overall saw respondents agreeing that it should be possible to monitor passenger flight details (82%), telephone calls (72%) and Internet and credit card usage (75% and 69%, respectively) when this was for the purpose of fighting terrorism.[696]

However, the survey findings also suggested that citizens viewed with distrust government moves towards relaxing data protection provisions. The findings also reflected the comments made previously about the difference in perceptions when surveillance is seen as something to which ordinary citizens should be subjected. The survery found that around a third "stressed that only suspects should be monitored (27%-35%) and approximately one in five (14%-21%) wanted even stricter safeguards".[697] Expanding on these averages, the survey reported differences between Member States. In response to the question as to whether people should be monitored when they fly in light of international terrorism, those supporting "unconditional monitoring of people's personal data" was highest in Hungary and the UK (53%). It was lowest in the Czech Republic (23%) and Finland (21%). In the Netherlands and Finland, 36% and 40% of respondents respectively stressed that only suspects should be targetted. In the UK and France, only 17% and 18% saw this as being neccessary.[698]

Other surveys confirm that the public often sees surveillance positively when it seems targetted against threats. One interesting example are studies reporting on the views of the US public with regard to various surveillance and security measures. In the aftermath of 9/11, some surveys revealed high levels of support for surveillance measures and technologies but later surveys have revealed tensions between public attitudes and governmental surveillance practices. For example, a 2001 survey by Harris Interactive conducted in the aftermath of 9/11 found 90% of American citizens in favour of three or more new surveillance measures, such as the use of facial recognition and phone and Internet monitoring. Even highly intrusive measures such as cell phone call monitoring was supported by 54% (41% opposed).[699] Compare these findings with a 2006 survey by Zogby International which saw a decline to only 28% supporting routine call monitoring.[700] This latter survey reported that only 38% of respondents believed that Americans had moved beyond a 9/11mentality even though support for surveillance measures had declined. A reason for this could be decreasing levels of trust in the US government.

Trust in government and those controlling surveillance technologies and implementing surveillance practices is a critical feature of surveys. Generally, surveys report low levels of support in most countries. In relation to the US figures above, a recent survey by the Ponemon Institute found that privacy trust in the US government declined from 52% in 2005 to 38%.[701] In the UK, a 2010 study conducted by the Joseph Rowntree Foundation found 65% worried about the UK government holding data on them, an increase from 53% in a 2006 study asking

---

[696] The Gallup Organization, "Data Protection in the European Union: Citizens' perceptions", Flash Eurobarometer 225, Brussels, 2008a. http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf

[697] Ibid, p. 6

[698] Ibid, p. 48

[699] "Overwhelming Public Support for Increasing Surveillance Powers and, Despite Concerns about Potential Abuse, Confidence that the Powers Will be Used Properly", Harris Interactive, Rochester NY, 3rd October, 2001 http://www.harrisinteractive.com/NEWS/allnewsbydate.asp?NewsID=370

[700] "Voters Balance Privacy, Surveillance", Zogby International, Utica, NY, 6th February, 2006, http://www.rogerclarke.com/DV/ZogbySurvey0602.html

[701] Ponemon Institute, *2010 Privacy trust study of the United States government*, Michigan, 30 June 2010, p. 2. http://www.privacylives.com/wp-content/uploads/2010/07/ponemon-2010-privacy-trust-study-of-us-govt-06302010.pdf

the same question.[702] A study by the London School of Economics on national ID cards also found that trust was low for the suggestion that governments would protect and use data responsibly. Using a seven point scale, with 1 being strongly agree and 7 being strongly disagree, it found that the mean of responses was 5.9 for citizens trusting that governments would protect their data.[703] Differences were also reported between European countries with the UK and Ireland being less trusting than respondents from new accession countries.[704]

Further examples of the complicated relationship between surveillance, security, public opinion and attitudes towards surveillance practices and technologies can be seen in research carried out by LogicaCMG in 2006 and Unisys in 2010.[705] These studies revealed public atttitudes and support for some controversial surveillance technologies, namely biometrics and body scanners.[706] In the LogicaCMG study, 92% of respondents from France said they were happy to have a fingerprint or iris scan when travelling abroad contrasted with the Czech Republic, where 67% of consumers would be happy to have their fingerprint or iris checked.[707] The LogicaCMG study however, can be criticised because it did not interrogate how biometric data might be used or shared and focused solely on use of the technology. In the case of body scanners, the Unisys study reported that over 90% of UK respondents would be willing to undergo a scan to ensure a "safe" passage while one in three Belgians and Germans would object. Mexico and Hong Kong were the only two countries in the study where a majority of respondents objected.[708] This study can be criticised because it is not clear what safe passage means and because it was not clear whether respondents saw any chance of being able to resist the technology.

In addition to these general surveys regarding trends in surveillance and security, there are others exploring specific technologies. Here, we begin to see a differentation between general and vague notions in relation to security and surveillance and the impact of certain technologies and how citizen's conceive of the impact of these technologies on them and the way in which they live their lives. Why certain technologies might be problematic is unclear as are the reasons for differences between countries. Zureik argues that cultural traditions reflecting collectivist or individualist traditions may play some role.[709] Zureik also suggests that surveillance technologies often raise concerns about bodily and spatial privacy, which for

---

[702] Joseph Rowntree Foundation, "JRRT State of the Nation opinion poll on Privacy and the Database State - the majority of us are unhappy and fearful", 20 Feb 2010,

http://p10.hostingprod.com/@spyblog.org.uk/blog/2010/02/20/jrrt-state-of-the-nation-opinion-poll-on-privacy-and-the-database-state---we-are-unha.html

[703] Backhouse, James, and Ruth Halperin, *A survey on EU citizen's trust in ID systems and authorities*, London School of Economics and Political Science, London, UK, 1 June 2006.

http://journal.fidis.net/fileadmin/journal/issues/1-2007/Survey_on_Citizen_s_Trust.pdf

[704] Ibid

[705] LogicalCMG, *e-Identity European attitudes towards biometrics*, London, 2006.

http://intra.iam.hva.nl/content/0708/verdieping2/trendanalyse//intro-en-materiaal/LOGICACMG_whitepaper_edentity.pdf. Unisys, *UK public willing to compromise on convenience and privacy for added security*, London, 13 April 2010.

http://www.unisys.com/unisys/countrysite/news/index.jsp?cid=300008&id=1400010

[706] As reported in media stories.

[707] Op. cit., LogicaCMG, 2006, p. 7

[708] Op. cit., Unisys, 2010

[709] Zuriek, Elia, "Cross-cultural study of surveillance and privacy. Theoretical considerations and empirical observations", in Zureik, Elia, Lynda Harling Stalker, Emily Smith et al. (eds.), *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, McGill-Queen's University Press, Montreal, 2010, p. 349

the GPD survey were found to be more important to respondents than informational or communicational privacy.[710] Some surveillance technologies are also ubiquitous, such as CCTV, or used on citizens in a manner restricting any possible resistance such as body scanners. Sentiments expressing the distinction citizens make between themselves and "others" suffering surveillance and levels of support for surveillance as a result warrant further investigation.

Encountering and being subjected to surveillance through exposure to certain technologies might have the effect of increasing support (through familiarity) or increasing rejection (through being seen as disproportionate). To some degree, this is borne out by some empirical research we have reported here and on CCTVs as we discuss later in this report.

4.2.4 Public View of the Regulatory Environment

Actors

Surveys generally distinguished between state actors and private organisations (normally companies). It is interesting to note that 'other individuals', whilst mentioned tangentially in relation to other questions (as regarding ID theft for example), were not seen as a body or entities worthy of specific consideration. This is particularly interesting considering the key role played by the individual in the online environment and the individual nature of many perceived threats. Within this differentiation, state actors tended to be (often considerably) more trusted than private actors. This was broken down further to show that certain state sectors were trusted more than others. For example, in 'Flash Eurobarometer 225'[711] medical services were highly trusted with an 82% positive trust rating, whereas local authorities scored a lower 67%. However, these numbers perhaps obscure a more nuanced understanding of the issue. When the public is further questioned on the issue of trust in state institutions, whilst there seems to be a belief that institutions will try to behave in the right way, there is a far lower belief in their capability to control and safeguard the data they have been given. This could be at least partly as a result of constant media coverage relating to authorities' leakage of personal data.[712]

Within the private sphere there is also considerable trust variation. In the same Eurobarometer survey, banks received a 66% trust rating (although perhaps this would be different now in 2011) whilst mail order companies received a trust rating of only 24 %.[713] However, despite these statistics, when deeper opinion was sought regarding commercial organisations handling of personal data, a distinct undercurrent of distrust emerged. Interestingly, whilst responses predominantly disapproved of sharing between government and private organisations, there was little elaboration as to what the public believed was the model of interaction between organisations, or to public perception of balance or substance to the storage or flow of data between organisations. In essence, there was little elaboration of a model beyond the superficial first instance of data collection.

---

[710] Ibid, p. 350

[711] The Gallup Organization, "Data Protection in the European Union: Citizens' perceptions", Flash Eurobarometer 225, Brussels, 2008. http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

[712] Backhouse, James, and Ruth Halperin, "A Survey on EU Citizen's Trust in ID Systems and Authorities", FIDIS Deliverable 4.4, London School of Economics and Political Science, London, 2007. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.4.survey.pdf . This considers trust in ID authorities' capability to handle data and further dissects citizen, authority trust relationships.

[713] The Gallup Organization, "Data Protection in the European Union: Citizens' perceptions", Flash Eurobarometer 225, Brussels, 2008. http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

In relation to surveillance conducted for the purposes of ensuring security, a clear distinction can be made between levels of trust in actors from the private sector versus those in the public sector. However, some surveys reported the overall level of trust for both was low, yet other surveys demonstrate relatively high levels. For example, the London School of Economics (LSE) conducted a study on ID cards, and reported low levels of trust by respondents. Yet a study by the European Opinion Research Group in 2003 found high and increasing levels of trust by respondents to different actors holding data on them. From 1996-2003, the European Opinion Research Group saw an increase in EU citizens' trust in their national authorities with their personal information. In 1996, 48% indicated trust as opposed to 36% who did not; in 2003, this had increased to 55% trusting and 30% who did not .[714] One explanation for this result could be a general decline in trust in Europe in relation to data and surveillance practices over the last decade as well as pressures on trust due to proliferation of surveillance technologies and greater incidences of losses and problems as a result of how organisations handle personal data.

Responsibility Allocation

Following from this, the public does not seem certain which actors should be responsible for the safe handling of personal data and indeed opinion changes depending on the nature of entity dealt with. When considering social networking sites for example, 49% of respondents stated the individual should be primarily responsible with 33% suggesting the social network should be responsible, whilst in relation to online shopping sites the percentages were 41% and 39% respectively. The difference is interesting not only as it demonstrates uncertainty in responsibility allocation but also as it suggests a difference in perception based on the nature of the specific data processing entity. Taking this logic one step further suggests the public may be basing an approach more on the entity dealt with as opposed to centred around data and the processing of data. Equally interesting is the relatively low response listing public authorities as having primary responsibility (16% and 19% respectively). This allocation is, to some extent in contrast with the relatively harsh penalties (if there is such uncertainty as to who should hold responsibility it seems strange there should be preference for harsh regulation) the public seems to wish on organisations that breach standards. Indeed, in the same Eurobarometer survey, 51% of respondents suggested organisations which misused data should be fined with 40% believing such organisations should be banned from using such data in the future.[715]

On the issue of ensuring security through surveillance measures, some surveys reflected the interesting observation that while some specific measures or surveillance practices were supported trust in those reponsible for regulating these practices was quite low, such as the LSE study on national ID cards. Furthermore, some studies noted public apathy. This was reflected in the public's not having any confidence in the sanctions which their respective regulatory authorities could employ in incidences of misuse whether these occurred in the private or public sector.[716]

---

[714] European Opinion Research Group, "Data Protection", Special Eurobarometer 196, Brussels, 2003. http://ec.europa.eu/public_opinion/archives/ebs/ebs_196_data_protection.pdf

[715] TNS Opinion & Social, "Attitudes on Data Protection and Electronic Identity in the European Union", Special Eurobarometer 359, Brussels, 2011. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

[716] Op. cit, Greenville, 2010

Transborder Data Protection

The public seemed equally uncertain as to how to approach the increasing globalisation of data flows. Whilst there was strong consensus that a harmonised set of data protection guidelines across the EU made sense and consequently that regulation at both national and EU levels was necessary, fewer people seemed aware of the issues arising from extra-territorial transfers or the risks this brought. In fact, even when data controllers were asked about their knowledge of the term 'standard contract clauses' 65% of respondents whose companies transferred data outside the EU were not aware of the term.[717]

In the context of security, the public has not supported transborder data flows as well as other methods of surveillance technologies and practices in order to combat terrorism or criminal activities. While it was often recognised that international terrorirsm and internaitonal criminal activity might neccessisate international cooperation, some surveys reported how the public's lack of trust in national actors and institutions was even more pronounced in terms of trusting foreign governmental and other actors using such surveillance techniques .[718]

Impacts and Fears

In terms of tangible impact, as a consequence of a release of information and the dangers it entailed, the public seemed specifically concerned about ID fraud, which was perceived to be a serious threat.[719] This concern was relevant to both state and commercial organisations. It is curious however, that the number of people who reported actually falling victim to this is tiny in comparison to the apparent concern. There was also undefined concern about other forms of physical or material harm. Particularly in the case of ID Fraud, this may have something to do with the amount and tone of coverage the issue has been given in the media. Murphy points out that concern may be exacerbated by the perception that "it is very easy for people to de-fraud you and that there is very little you can do to stop it, even if you take precautions."[720] The public also demonstrated concern relating to the commercial collection and use of data. Unsurprisingly, the public approached the issue from an individual impact perspective and were concerned and annoyed by the perceived end results of data distribution, namely direct mail, spam, cold calling etc. Related to this, the public showed concern relating to certain data practices linked to this fear (but which also have wider significance), the fear that information would be 'used without knowledge', 'shared with third parties without agreement' and 'that information would be used in different contexts than those in which it was disclosed'.[721]

---

[717] The Gallup Organization, "Data Protection in the European Union: Citizens' perceptions", Flash Eurobarometer 225, Brussels, 2008. http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

[718] See Cockfield, Arthur J., "Legal constraints on transferring personal information across borders: A comparative analysis of PIPEDA and foreign privacy laws", in Zureik, Elia, Lynda Harling Stalker, Emily Smith et al. (eds.), *Surveillance, Privacy, and the Globalization of Personal Information: International Comparisons*, McGill-Queen's University Press, Montreal, 2010

[719] Landsdowne Market Research, "Public Awareness Survey 2008", Data Protection Commissioner, Portarlington, Ireland, 2008. http://www.dataprotection.ie/documents/press/Survey08.pdf.

[720] Murphy, Oliver, "A Surveillance Society: Qualitative Research Report", Report prepared for COI on behalf of ICO, Wilmslow, Cheshire, UK, 2007.
http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/surveillance_report_v6_final.pdf.

[721] TNS Opinion & Social, "Attitudes on Data Protection and Electronic Identity in the European Union", Special Eurobarometer 359, Brussels, 2011. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

Although there were more abstract fears relating to the combination of data and/or databases, the development of a surveillance society and further issues related to assemblages of data etc., in terms of their social basis, these were at best only loosely defined. Murphy states, "some were able to imagine an extreme scenario where these bodies 'join up' the information they hold, thus, to our respondents' eyes, reducing them to pieces of (impartial) data and robbing them of their individuality".[722] However, when listing concerns, a small portion of respondents in Eurobarometer 359 were able to recognise the more solid, individually based, manifestation of these concerns; 12, 11 and 7% respectively recognising the risk of 'reputation damage', 'views and behaviours being misunderstood' and 'the possibility for discrimination in other areas'.[723]

For broader themes of surveillance, particularly where governments promoted surveillance to improve security against threats such as terrorirsm or criminal activity, surveys show a drop in the public's fears about governmental use of their data. For example, Davis and Silver found that, in the case of preventing terrorism in a vague sense, 55% of respondents indicated that civil liberties should be protected. When asked about individuals suspected of being associated with terrorist organisations, then 71% of respondents favoured restricting civil liberties.[724] Most surveys reporting on surveillance in the context of security saw both a justification for the use of data and a recognition that such practices were useful in ensuring the security of the individuals concerned. Differences began to emerge, however, in relation to how much surveillance was necessary in order to balance out and counteract threats and risks faced by individuals. With some surveillance, especially in the name of security, these imbalances of control and power are even more keenly felt. Surveillance measures might disproportionately target those who already suffer social exclusion. Most citizens feel unable to exercise control over public sector surveillance.[725] This feeling of a lack of control explains the low levels of trust in those institutions and actors who are responsible for regulation and control over surveillance practices and technologies.

Justifications and Benefits

Despite the above risk recognition and general uncertainty and the fact that 63% state that disclosing personal information is a big issue for them, individuals seem to accept the need to divulge increasing amounts of information.[726] The overarching reason for this acceptance is the rather deterministic viewpoint that it is 'simply part of modern life'. On the one hand, there is the perceived obligation to release more information, both legally, as required by authorities increased collection practices, and practically as a price for involvement in the information environment. On the other hand the public recognise benefits from the further release of information. These take the form of short term benefits in the form of exchanges for rewards (or service usage) as well as longer term benefits from participation in data

[722] Murphy, Oliver, "A Surveillance Society: Qualitative Research Report", Report prepared for COI on behalf of ICO, Wilmslow, Cheshire, UK, 2007. http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/surveillance_report_v6_final.pdf.

[723] TNS Opinion & Social, "Attitudes on Data Protection and Electronic Identity in the European Union", Special Eurobarometer 359, Brussels, 2011. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

[724] Davies, Darren W. and Brian D. Silver, "Civil liberties vs. security: Public opinion in the context of terrorist attacks in America", *American Journal of Political Science*, Vol. 48 No. 1, January 2004, pp. 28-46

[725] Op. cit. Greenfield, 2010

[726] Ibid.

exchanges and a presence in data environments (social networking for example).[727] When discussing rewards considering (see below) information imbalances and imperfections as well as behavioural aspects (preference for short term over long term considerations etc.) may be explanatory and significant.[728] However, the deterministic approach to obligatory information disclosure can arguably also be seen as a practical coping mechanism for significant power imbalances in the collection process. The processes are operating at a scale over which the individual feels very little control. Equally, formulating a position in response to increased collection may be difficult as goals and institutions may superficially remain the same, whilst the key mechanisms which drive the process are imperceptible. Trends and effects are detached in perception from the decisions and mechanisms driving them creating the impression of inevitability.

There is strong evidence to support the argument that surveillance measures and technologies disproprotionately target those who already suffer from social and other forms of exclusion.[729] Furthermore, surveys show general public opinion favouring more controls and more surveillance targetted at these groups, or a general lack of concern about measures targetting socially excluded groups.[730] However, if the public perceives the technology or practice targetting them and not just these groups, then one can detect more widespread concern and resistance to the technology or surveillance practice. One example of how this trend has played out is in the case of the National DNA database in the UK, which a semi-private company, Forensic Science Services Ltd, has maintained on behalf of law enforcement. Widely reported as the database with the highest proportion of the populace, politicians and law enforcement authorities have promoted it as one of the key tools enabling police to investigate and solve criminal cases.[731] Its utility was seen not only in dealing with existing cases but also in helping to solve some high profile historical cases.[732]

For some years, the database was lauded in policy, media and public discourse as a key, effective tool in crime prevention, solution and investigation.[733] However, cracks in public support for the technology appeared when the media and politicians began to raise concerns and objections to the retention on the database of the DNA of people who were never charged with an offence.[734] Increasingly, the media were reporting incidences where DNA from children was being retained, even very young ones, and the practice of collecting DNA for *any* recordable offence. The police were retaining the DNA of children caught throwing eggs. Gradually, public resistance and disagreement with the collection and maintenance of DNA

---

[727] Brandtzaeg, Petter Bae, and Marika Lüders, "Privacy 2.0: personal and consumer protection in the new media reality", Norwegian Consumer Commission, Oslo, 2009. http://forbrukerportalen.no/filearchive/report_privacy_social_media_1_.pdf.

[728] Acquisti, Alessandro, and Jens Grossklags, "Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting", in Camp, L. Jean, and Stephen Lewis (eds.), *The Economics of Information Security*, Kluwer, Dodrecht, 2004, pp. 165-178. Schütz, Philip, and Michael Friedewald, "Cui bono from giving up or protecting privacy? A basic decision theoretic model", *Journal of Information Assurance and Security*, Vol. 6, No. 5, 2011, pp. 432–442.

[729] Bunyan, Tony, "Just over the horizon- the surveillance society and the state in the EU", *Race and Class*, Vol. 51 No. 3, 2011, pp. 1-13

[730] Op. cit., Davies and Silver, 2004

[731] Lynch, Michael, Simon A. Cole, Ruth McNally and Kathleen Jordan, *Truth Machine: The contentious history of DNA fingerprinting*, University of Chicago Press, Chicago USA, 2011

[732] See, "DNA Database: Key case studies", BBC News, May 7th 2009,

http://news.bbc.co.uk/2/hi/uk_news/8037972.stm

[733] Op. cit. Lynch et al, 2011

[734] Ibid

for those never charged grew.[735] In tandem with these trends in public discourse, challenges to the police and the operators of the database, Forensic Science Services (FSS), were brought to the European Court of Human Rights.[736] Eventually, in a unanimous judgment, the Court decided that the collection and further retention of DNA from indiviuals who either were never charged or were charged but not convicted was not a proportionate policy in public security versus the rights of the individuals who challenged the policy.[737] The Court ordered the UK to amend its policy. The Court cited the Scottish system as an example which could be followed. Unrelated to the judgment, the financial crisis and changes to how police forces made use of forensic scientists resulted in FSS entering liquidation shortly after the coalition government in the UK came to power.

While it was a legal mechanism of redress that led to a change of policy, the judgment of the court (often maligned in the British media) was broadly in line with reported public sentiment concerning the database and the collection and retention of DNA. The arguments of politicians and police forces about the utility of a large database did not hold sway or garner an overall favourable majority of public opinion in the UK. While this case might centred on a controversial area of science, namely genetics, and the use of DNA as a means of identification might engender other public concerns about its use as a surveillance practice and as a means of ensuring security, the public reaction and resistance to the technology and policies regarding use of that technology, despite its visible and widely reported prior successes, is an interesting assemblage of some of the key themes discussed in this report.

Privacy Protection

It is remarkable that, considering the above, individuals do not use privacy enhancing technologies more. In Flash Eurobarometer 225, only 22% of respondents claimed to have use privacy enhancing tools, whilst 56% had never heard of the technology. Amongst the reasons cited were a lack of belief in their effectiveness or that they wouldn't know how to use or install them.[738] The European Commission noted this point in its Communication on privacy enhancing technologies in terms of raising public awareness and increasing consumer use of these technologies.[739] It remains unclear however how far this objective has been achieved or what the impacts have been on rates of use and public knowledge.

However, individuals do claim to use a range of or other technology based techniques including altering browser or usage settings, deleting cookies or reading or ensuring privacy policies before trusting a website. In fact it was only 15% of Eurobarometer 359 respondents who claimed to do nothing to protect their online privacy. It is however, equally informative that when considering the specifics of these methods there was a significant knowledge gap between action, understanding and consequence. For example, when reading privacy

---

[735] See for example Barnett, Antony. "Police DNA database 'is spiralling out of control'". *The Guardian*, London, 16 July 2006. http://observer.guardian.co.uk/uk_news/story/0,,1821676,00.html

[736] S. and Marper v. The United Kingdom, 30562/04, ECHR 1581, 4 December 2008)

URL: http://www.bailii.org/eu/cases/ECHR/2008/1581.html

[737] Ibid

[738] The Gallup Organization, "Data Protection in the European Union: Citizens' perceptions", Flash Eurobarometer 225, Brussels, 2008. http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf London Economics, "Study on the economic benefits of privacy enhancing technologies (PETs)", Final Report to the European Commission DG Justice, Freedom and Security, London, 2010. http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/final_report_pets_16_07_10_en.pdf.

[739] *Communication from the European Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies*, Brussels, May 2nd 2005, COM (228) 2007.

statements there was a considerable lack of comprehension as to what they represented or what they meant when read in full (only a third claimed to understand them fully).[740]

Other strategies were also highlighted, including giving false information, refusing to give information and staying away from situations in which information may have to be given.

(There have been privacy studies which suggest that the responses stating they protect privacy are significant overrepresentations, the above figures may thus be more indicative of what people believe they ought to do rather than what they in fact do).

Uncertainty and Inconsistency

Whilst figures can be put on certain aspects of opinion in individual surveys, there is considerable difference between actual behaviour and opinion, for example with respect to the stated importance of privacy in online environments and behaviour in relation to privacy protection (reading privacy statements for example).

It seems from the above answers that, when considering structural or more abstract issues (transborder data flows for example), the public displays a greater uncertainty than when considering issues with direct individual relevance (spam etc.). This suggests that the model for understanding what happens with data once it is released by the individual, or what this means on an aggregate scale, is rather fluid and uncertain.

The data environment can be perceived as consisting of two parts; supporting technological infrastructure (and its innate capabilities) and the operation of the network of data connections and flows that constitute its lifeblood. In each consideration of technology, the public showed a significant lack of awareness as to the capabilities, uses and key privacy impacting features present. This is demonstrated well in the U.S. survey, 'Technology, Security and Individual Privacy: New Tools, Threats and New Public Perceptions'[741]. A lack of understanding as to the shape and operation of the data flows themselves is demonstrated in 'Privacy 2.0: Personal and Consumer Protection in the New Media Reality'[742], in which it is pointed out that, even within the confines of a single social network, users are neither aware of (amongst a variety of other issues) the intelligent tracking technologies in operation, the connections to different applications or the dynamism of the networks they are taking part in. From this gap in understanding, it is possible to assume that there are a series of other questions of relevance which, although they are aware of their significance, the public may not yet have the reference points to answer solidly, for example, what the value of their data might be, who might want this data or what the exact social or personal consequences of each release might be.[743]

---

[740] TNS Opinion & Social, "Attitudes on Data Protection and Electronic Identity in the European Union", Special Eurobarometer 359, Brussels, 2011. http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

[741] Strickland, Lee S., and Laura E. Hunt, "Technology, Security, and Individual Privacy: New Tools, New Threats, and New Public Perceptions", *Journal of the American Society for Information Science and Technology*, Vol. 56, No. 3, 2005, pp. 221–234.

[742] Brandtzaeg, Petter Bae, and Marika Lüders, "Privacy 2.0: personal and consumer protection in the new media reality", Norwegian Consumer Commission, Oslo, 2009. http://forbrukerportalen.no/filearchive/report_privacy_social_media_1_.pdf.

[743] Allwinger, Kristin, and Joschi M. A. Schillab, "Vertrauen der ÖsterreicherInnen in den Datenschutz", Oekonsult Communication & Consulting, Baden, Austria, 2008. http://www.oekonsult.eu/datensicherheit2008.pdf.

Acquisti and Grossklags consider the possibility that ""Privacy in theory may mean many different things in practice" and consequently that "the parameters affecting the decision process of the individual are perceived differently at the forecasting (survey) and operative (behavior) phases". They isolate a series of potential limiting factors to the individual decision to balance a transaction with a potential information security impact. The decision making model may be unbalanced by limited information, bounded rationality issues, self-control problems and other behavioural distortions. The lack of understanding of the data environment mentioned above would certainly account for impacts on each of these potential limiting factors and thus significantly reduces the ability for the individual to 'rationally' balance each action.[744] Consequently awareness of issues (and the importance of privacy and data protection) and what can be done etc. on an abstract scale may not translate to the apparently corresponding action in concrete situations.

Thus, whilst not unaware of dangers and the existence of structures through which data processing and protection operate, there is a lack of understanding as to how and why they operate. This provides little basis for practical decision making in an environment in which increasing data collection and dissemination is perceived as a necessity for participation in everyday acts as well as society in general.

The broader consequences of this are, firstly, that the public are unable to formulate considered responses even to identified issues as they only have half of the relevant foundations through which to do this and secondly that the public may be vaguely aware of, but largely unable to consider responses to, a series of other threats. Firstly, the tangible impacts which are not obviously related to original data collection are ignored. Secondly, as the data processing itself is invisible and the processes largely not understood, the increasingly broad impact data processing has on other systems (social, economic etc.) is correspondingly invisible. Finally, a lack of understanding of the processes means the processes themselves develop without a public presence to consider and monitor their potential and direction. The split between the necessity to operate within but the lack of understanding of, the structures of the information society is increasingly making the public feel powerless and confused. This brings to mind Solove's applied reading of Kafka, "In *The Trial*, the problem is not inhibited behavior, but rather a suffocating powerlessness and vulnerability created by the court system's use of personal data and its exclusion of the protagonist from having any knowledge or participation in the process. The harms consist of those created by bureaucracies—indifference, errors, abuses, frustration, and lack of transparency and accountability".[745] The bureaucracy here works as a metaphor for the broader data environment with its own systems and order. Although the dystopic image is certainly diluted by the plurality of actors and their lack of coordination, from an individual perspective however, the effect retains some similarity.

EU Project: PRACTIS

The **PRACTIS** project (*Privacy – Appraising Challenges to Technologies and Ethics*[746] is analyzing results of a survey conducted in schools in six European member states and

[744] Acquisti, Alessandro, and Jens Grossklags, "Privacy Attitudes and Privacy Behavior: Losses, Gains, and Hyperbolic Discounting", in Camp, L. Jean, and Stephen Lewis (eds.), *The Economics of Information Security*, Kluwer, Dodrecht, 2004, pp. 165-178.

[745] Solove, Daniel J., ""I've got nothing to hide" and Other Misunderstandings of Privacy", *St. Diego Law Review*, Vol. 44, No. 2008a, pp. 745-772.

[746] http://www.practis.org

Israel among more than 1000 teenagers, and aims at showing their attitudes towards new and emerging technologies ranging from RFID to CCTVs to social networks. Although the PRACTIS survey is not yet available on the project's website, an article that appeared in the first Newsletter (January 2011)[747], that mainly refers to a comprehensive literature review of empirical studies on privacy perceptions and constitutes the survey's background[748], has been taken into account.

The literature review focused on studies on so-called "digital natives'" attitudes towards Social Networks Sites (SNS), that could be of the highest relevance when trying to analyze key elements of the new surveillance, the so-called "self exposure" trend. The literature review revealed that;

1) the concept of privacy is still important to adolescents but it is transforming to include a more flexible management need
2) many users have little knowledge or misconceptions about visibility and privacy policy
3) there seem to be a connection between privacy settings in SNS and cultural preferences or lifestyle in general
4) SNS users are generally aware of potential risks like privacy intrusions or misuse of personal data, but they are not concerned about it

In the paper's conclusive remarks, it is thus assumed that "awareness raising seems to be one of the most important measures to minimize the existing risk of privacy intrusions"[749], and has to be taken as a serious task not only by parents but also by teachers and data protection authorities. Moreover, the PRACTIS paper once again shows the importance of considering privacy and security as socially embedded concepts rather than universal and abstract terms. Privacy perceptions are shaped not only by individual differences, but also by macro-level factors like national culture.

Most surveys, as we have recounted here, illustrate general support amongst the public for surveillance measures in the name of security with the caveat that some specific measures which seem to target particular groups are viewed negatively and with mistrust.[750] While public sector surveillance measures are viewed with some concern, private sector surveillance of individuals is viewed even more negatively.[751] An interesting observation therefore that can be made is why surveillance practices in the private sector are viewed more negatively yet the public's ability to seek redress (through data protection or changing companies) is much easier but is not known.[752] One conclusion that might be reached is that levels of trust or public awareness of data protection regulation lags behind their knowledge or concerns over private sector collection and misuse of their data. One reason for this might be the nature of media coverage in relation to this topic, emphasising the problem and what happened rather than covering the data protection mechanisms that are in place to prevent these occurrences or provide a method of redress and sanction for members of the public when these events occur.

[747] Bach, Nicolas, "Youth and Privacy: Changed Perceptions or a Matter of Awareness?", *PRACTIS Newsletter*, Vol. No. 1, 2011, pp. http://www.practis.org/UserFiles/File/PRACTIS%20Newsletter%2020.05.2011%20www.pdf.

[748] Ibid., p. 8-9.

[749] Ibid., p. 7.

[750] Op. cit. Greenville, 2006

[751] Antón, Annie I., Julia B. Earp, and Jessica D. Young, "How Internet Users' Privacy Concerns Have Evolved since 2002", *Ieee Security & Privacy*, Vol. 8, No. 1, 2010, pp. 21-27.

[752] Martin, Brian, "Opposing Surveillance", *IEEE Technology and Society*, Vol. 29, No. 2, 2010, pp. 26-32.

4.2.5 Effectiveness of Regulation in Light of Environment

From the above it is clear that there is a certain knowledge shortfall in understanding the framework and the environment it is designed to regulate. The aggregated uncertainty this creates can make it difficult to isolate specific expectations as to how and to what extent protection is expected. As a consequence there is very little survey information on what or how the public feel is wrong with the framework or how it could be improved. This may, in itself, be indicative of a greater issue, as the public should be better able to comprehend their legal protection.

Within this uncertainty however, the elements of protection offered are well known and the relevance of each aspect is understood and generally agreed to be important. Considering these aspects to reflect deeper principles, it is possible to suggest that the public (whilst perhaps not having specifically considered it) do generally support the framework and its principles. A reflection of this is shown in organisations' perceptions of the effect of the DPA on consumer trust, 85% believing it had a positive effect.[753]

Yet, from the available data there is a general feeling that personal data does not receive the protection it should. Demonstrated most obviously by the fact that a large majority feel they have lost control over their data as well as other opinions on protection. For example, in Flash Eurobarometer 225 a majority of respondents believed that national legislation could not cope with the demands currently placed on it.[754] Whilst principles seem not to be disapproved of, protection in reality is not perceived to be of the same quality.

It would therefore be logical to suggest that it is in the enforcement and application to the data environment (and by extension the change and fluidity of this environment) in which problems are perceived to lie. That the public see a problem in enforcement is demonstrated by the desire for relatively harsh measures for organisations which breach norms, whilst the uncertainty of application against the complicated current environment is demonstrated in the discrepancy and uncertainty in defining terms for even relatively basic concepts such as responsibility allocation.

Whilst (possibly due to the complexity of the environment making an appreciation of how the framework should apply very difficult) the question as to how to remedy the situation has been only briefly considered in surveys, there are certain instructive opinion trends which unsurprisingly all move toward clarification of the environment and the operation of the framework in relation to it. Firstly, there is a desire for greater education about the principles and processes of the framework and environment. Secondly, there is a desire to solidify the fluidity of the environment (or at least elements of it), for example, 64% of Europeans believe data would be better protected by organisations if they were obliged to have a specific contact person responsible for the correct handling of data, whilst Austrians often spontaneously (outside the survey questions) suggest the need for a 'one stop national authority' to be set up

[753] Social and Market Strategic Research, "Report on the Findings of the Information Commissioner's Office Annual Track 2010: Organisations", UK Information Commissioner's Office, London, 2010. http://www.ico.gov.uk/~/media/documents/library/Corporate/Research_and_reports/annual_track_2010_organisations.ashx.

[754] The Gallup Organization, "Data Protection in the European Union: Citizens' perceptions", Flash Eurobarometer 225, Brussels, 2008. http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

which could, when asked, research and provide information about the dispersion of citizen information.[755]

When measures were put in more solid terms to Data Controllers, the same concerns were applicable and high proportions promoted more specific measures aimed at removing uncertainty such as 'more harmonized rules on security measures', 'further clarification on the practical application of some of the key definitions and concepts of the European Directive and national data protection laws'.

Surveillance and security public attitudes towards the regulatory environment and actors who are regulatory sources is even more complex. Indeed even in those surveys expressing high levels of support for surveillance practices trust in institutions and actors responsible for conducting this surveillance is generally a mixed bag. In studies we have examined mistrust is more commonly expressed than trust. This is often conceptualised as doubts that actors will fully and properly conduct these activities in a way which respects the legal and regulatory environment. Furthermore some specific surveys demonstrate that publics do not have an adequate level of knowledge concering surveillance practices and technologies and also have a lack of comprehension in relation to the regulatory environment in different countries which governs these practices and these technologies. Trust in all of these elements is reported as quite low. This is the case for both public sector and private sector involvement in surveillance.

4.2.6 Conclusion

Privacy and data protection are highly complex concepts around which public opinion is diverse, fluid and strongly tied into a series of other issues. However, from the above certain trends are evident.

Key amongst these is that the public perceives the right in a somewhat unbalanced way, preferening its individual importance over its social function. This leads to a similarly unbalanced weiging of importance in relation to other social issues. This reasons behind this are elucidated when considering the public perception of the data environment. The complexity and invisibility of this environment lead to the lack of ability to solidly perceive trends and structures. A significant part of of the decision making and conceptualisation puzzle is thus missing. Whilst abstractly aware of issues and dangers (even at the social level), in practical terms this does not translate into a suitable decision making model.

With the awareness of this lack of perception it is no surprise that the public believe their protection is limited, if not in theory then certainly in practise. From this, it is clear that desired improvements in the current framework would centre around a more solid and comprehensible enforcement of legislation as well as a clarification and anchoring of the regulatory background.

Surveys exploring surveillance as a practice and as a technology represent a complex field. While most surveys report levels of support from different publics for surveillance measures to ensure security as a response to threats, those which interrogate this or which explore particular practices or surveillance technologies reveal a more nuanced level of public acceptances. The reasons for this are complex and tentative explanations have been suggested

[755] Allwinger, Kristin, and Joschi M. A. Schillab, "Vertrauen der ÖsterreicherInnen in den Datenschutz", Oekonsult Communication & Consulting, Baden, Austria, 2008. http://www.oekonsult.eu/datensicherheit2008.pdf.

here. As these represent potentially broad general issues related to specific elements of surveillance it would require further investigation to interrogate and investigate these properly. What research has been done in these specific elements does as demonstrated here reveal a number of interesting trends.

4.3 PUBLIC PERCEPTION OF SURVEILLANCE TECHNOLOGIES

There is an increasingly broad range of surveillance technology.[756] This technology is deployed in different scenarios depending on its technological specificity and the development of its use. Increasingly, the privacy impacting effects do not stem from each individual technology; rather the technologies facilitate the collection of different types of information. The impact then arises when specific technologies are combined with information processing capabilities, allowing the combination of previously diverse sources of information, the linkage of collected data with existing pools of data and broader significance extraction capabilities from all sources.

As in the case of data protection and privacy issues generally, information relating to public opinion on new surveillance technologies is firstly difficult to evaluate as there have been few related surveys. Perhaps this is because the issue of surveillance as it currently manifests and the technologies now significant in the field have only recently entered public consciousness, or perhaps it is because surveillance, as a relatively abstract concept (particularly in relation to data assemblages), is not a theme easily associated with public opinion. Equally, many of the surveys that have been conducted have been from the American perspective. This may significantly prejudice the use of their findings when considering the EU public.

This piece will firstly consider the difference between CCTV as an established, and not necessarily "smart" surveillance technology, before considering the factors that shape public opinion on technologies. It will consider the comprehension deficit often present in the conception of technologies and where this may have come from before considering public fears arising from technological deployment and desires for control over, and involvement in, the decisions systems and processes involved.

4.3.1 CCTV and Other Technologies

As the relevant privacy and data protection impacts arising from the use of CCTV and many other new technologies arise partially as a result of the specifics of the technologies themselves and partially due to connections to other forms and networks of information processing, CCTV can increasingly be related to other technologies as parts of a wider whole.

However, there are significant differences which make CCTV (considered as an isolated technology rather than as a part of a broader surveillance and data processing infrastructure) a unique case. Firstly, CCTV has already been present for decades in Europe. Whilst this does not preclude its conception and understanding from constantly changing as contexts evolve, it does mean that there has been time to cultivate a presence and a series of reference points in public imagination which other, more modern or less visible, technologies have not.[757]

---

[756] For an overview see Petersen, Julie K., *Understanding surveillance technologies: Spy devices, privacy, history and applications*, Auerbach Publications, Boca Raton, 2007.

[757] Fussey, Pete, "Control and the Community: The spread of surveillance in the post-industrial city", Paper presented at: Political Studies Association 59th Annual Conference, Manchester, 7-9 April 2009, 2009. http://www.psa.ac.uk/journals/pdf/5/2009/Fussey.pdf

Secondly, when considered in its broader social application, the weighting of function of CCTV is arguably significantly different from that of other modern surveillance technologies. It is not only the data collection aspect of CCTV that is its goal or provides its deployment justification, rather it is a combination of this and the effect it has on the environment in which it operates. Its effect is based as much on the direct alteration of the behaviour of the end user by virtue of its presence as on the (data) knowledge gleaned from its operation.[758] This differs from the mode of operation of most other surveillance technologies. Firstly, whilst their justification is equally based on the alteration (securing) of their environment, this occurs predominantly through the security capabilities offered by data collected (although in certain cases the visible presence of technologies also plays a role). Secondly, the pre-emptive control over the subject/user behaviour is not the target substance of control, rather they seek to isolate and allow reaction to aberrant behaviour through interaction with the subject.

Finally, (whilst not true in all cases), the use of CCTV is generally based on as wide a collection of visual data in one scene as possible. Data is thus often collected regarding multiple attributes of multiple individuals simultaneously. This is comparable to a trend in other significant surveillance technologies (considered apart from the data processing infrastructures which support them) which seek to isolate increasingly specific data from specific individuals.

Empirical research on CCTV

As befits one of the more prevalent and established surveillance technologies in Europe, there are numerous studies exploring the use of CCTV, some of which have investigated public attitudes towards the technology in different Member States. In this section, we present a review of some of this empirical research and identify the main findings and conclusions that they have reached. We have already suggested some specific and common themes in relation to CCTV and the review of studies complements this and explores some of the ramifications of CCTV becoming part of a wider smart surveillance infrastructure.

In reviewing past studies on CCTVs in this report, we are interested in the conclusions drawn in relation to public acceptance or resistance to the technology. In this respect, studies present a varied, complex and multifaceted set of answers pointing to the conclusion that CCTV, technology and practices are embedded in a complex web of social, technical and cultural interactions.

CCTV images are often potent, such as the still images released of the Jamie Bulger killing which some see as a watershed moment for reporting on and perceptions of the technology in the UK.[759]

The components of existing studies of relevance to explaining public acceptance and resistance include the following:

- The characteristics of how, where and by whom CCTVs are used.
- How effective are CCTV deployments in meeting policy objectives?
- What are the privacy implications for individuals?
- What are the privacy implications for spaces?

[758] Koskela, H., "The gaze without eyes': video-surveillance and the changing nature of urban space", *Progress in Human Geography*, Vol. 24, No. 2, 2000, pp. 243-265. Lyon, David (ed.), *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2007. pp 61-62.

[759] Norris, Clive and Michael McCahill, "CCTV: Beyond penal modernism", *British Journal of Criminology*, Vol. 46, 2006, pp. 97-118 [p. 100].

- How technology is driving changes in how CCTV data is used and analysed?

Each of these themes has a bearing on the overall premise of how the public views CCTV and levels of acceptance or rejection of surveillance by these technologies. The rest of this section discusses these issues as they are borne out by the conclusions and findings of the studies reviewed.

Characteristics of CCTV deployments

In the context of European research on the use of CCTV, the studies show differences and commonalities between CCTV deployments in different countries. The European country with the most widespread use of CCTV is the UK.[760] It has a number of CCTVs greater than most other European countries combined and it enjoys a high profile in the media and in public and policy discourse.[761] Determining the exact figure is difficult but some (guess) estimates suggest there are between 1.85 million to 4.2 million[762] CCTV cameras installed throughout the UK. This translates into an individual on average being recorded 70-300 times a day depending on the estimate used.[763] As such, other European studies as well as international research often make reference to the UK as a case for comparisons and contrasting conclusions.

The UK has also been used by policy-makers and various organisations in other countries in the EU and outside as a model to replicate in combating various threats such as criminal and terrorist activity. This is due to the perceived (as well as reported) successes of widespread deployment of CCTVs in the UK.[764] Reports that investigate the use of CCTV technologies and that highlight public concerns in the UK are of particular interest. Where, for example, the assumption of broad historical public support for CCTVs has been interrogated, studies from the UK suggest that this is not the case, at least in the simplistic manner in which it is often recounted in policy discourses.[765] Also studies drawing on UK experiences are of interest due to the fact that CCTV surveillance infrastructures are extensive and expansive, meaning a wider range of spaces investigated in terms of public acceptance or resistance to the technologies.

While the UK is interesting as the paradigmatic CCTV state, most studies point to the fact that CCTVs and public attitudes and reactions to them are culturally and socially divergent. Where in the UK there is support, most studies from Germany illustrate a deep suspicion and

[760] Lippert, Rand,y and Blair Wilkinson, "Capturing crime, criminals and the publics' imagination: Assembling Crime Stoppers and CCTV surveillance", *Crime, Media, Culture*, Vol. 6, No. 2, 2010, pp. 131-152.

[761] Webster, William, "CCTV Policy in the UK: Reconsidering the Evidence Base", *Surveillance and Society*, Vol. 6, No. 1, 2009, pp. 10-22.

[762] McCahill, Michael, and Clive Norris, "Estimating the extent, the sophistication and the legality of CCTV in London" in M.L. Gill, (ed.), *CCTV*, Crime at Work Series, Volume IV, Perpetuity Press, Leicester, 2003.

[763] Original estimates of 4.2 million by McCahill and Norris, op. cit., 2003, have been widely reported. A recent study undertaken by Cheshire police in the UK has suggested halving this figure. See http://www.acpo.police.uk/ThePoliceChiefsBlog/20110303GraemeGerrardsCCTVblog.aspx

[764] Deisman, Wade, Patrick Derby, Aaron Doyle et al., "A Report on Camera Surveillance in Canada - Part One", Surveillance Camera Awareness Network (SCAN), 2009, p. 4.

[765] Gill, Martin, Jane Bryan, and Jena Allen, "Public Perceptions of CCTV in Residential Areas : 'It Is Not As Good As We Thought It Would Be'", *International Criminal Justice Review*, Vol. 17, No. 4, 2007, pp. 304-325.

rejection of CCTVs particularly in public spaces.[766] This means that drawing any general conclusions is difficult despite some similarities being present in some findings in studies.[767]

Past empirical studies highlight a number of recurring characteristics to CCTV deployments in the EU and internationally. These include

- The range of spaces and places where CCTVs are deployed and where they are not
- The scale of CCTV deployments
- The uses which are ascribed to CCTV networks
- The types of actors and organisations that make use/or are authorised to make use of CCTVs
- The divide between sophisticated technological networks and simplistic ones

Most studies point to a situation where the range of places where CCTVs are used is on the increase with an increase also in the number of CCTVs. Studies also make the distinction between CCTVs operated by the private sector and those by public sector organisations. This is nearly always reflected in the different types of spaces where each type of deployment can be found with private sector deployments most often in retail or service sector premises and areas and public sector deployments in areas of interest for security (such as transport hubs) or crime prevention (such as streets, squares).[768] Studies also suggest that while rates of the usage for CCTVs are growing in all of the countries where research is conducted, the UK is still the country with the most CCTVs by some considerable distance.[769]

Most research demonstrates a significant disparity between the stated goals of CCTV deployments and how they are actually used.[770] We return to this point in more detail in reviewing the research on the effectiveness of CCTVs. More often than not, the rationale for the deployment of CCTVs is made in terms of the prevention of crime, such as the prevention of shoplifting in retail premises.[771] In relation to the characteristics of CCTV deployments, most research illustrates a complex set of uses for CCTVs, one which is often embedded in practices of risk management as opposed to threat prevention or detection.[772] This latter discourse is one in which proponents of CCTV deployments often engage but which is not displayed in the field.

Studies also illustrate the wide-ranging nature of actors and organisations that make use of CCTVs and the differences between public perceptions of the technology as a result of this issue of control. While some public perceptions, as well as academic discourse, focuses on the "big brother" idea of massive CCTV networks of surveillance, there is a much more patchwork use of CCTVs by small local actors, or "little brothers".[773] One explanation for this is the relative cheapness of the technology: single unit simple CCTVs can be bought for €30-70. Their low price reflects their relative simplicity, and one can question whether they pose

[766] Hempel, Leon, and Eric Töpfer, "CCTV in Europe - Final Report of the UrbanEye Project", Working Paper 15, Zentrum für Technik und Gesellschaft, Berlin, 2004. http://www.urbaneye.net/results/ue_wp15.pdf

[767] Ibid, p. 9.

[768] Ibid, p. 5.

[769] Ibid, p. 4.

[770] Ibid, p. 14.

[771] Lindblom, Arto, and Sami Kajalo, "The use and effectiveness of formal and informal surveillance in reducing shoplifting: A survey in Sweden, Norway and Finland", *The International Review of Retail Distribution and Consumer Research*, Vol. 21, No. 2, 15 April 2011, pp. 111-128.

[772] Hier, Sean P., "Risky spaces and dangerous faces: Urban surveillance, social disorder and CCTV", *Social & Legal Studies*, Vol. 13 No. 4, 2004, pp. 541-554.

[773] Webster, op. cit., 2009.

any of the same issues or problems as larger networks.[774] In nearly all cases, the largest public sector organisation making use of CCTVs is law enforcement and these often have had the most sophisticated networks and have been at the forefront of introducing new developments and new technologies. CCTVs were often promoted by these actors as a perceived response to public demands for security and safety, whether this was actually demonstrated in empirical research or not.[775] In the private sector, shopping centres were cited as having the most extensive and sophisticated deployments.[776]

A further important characteristic of CCTV deployments is the disjunction between sophisticated technological deployments and simplistic ones. While in some discourses, the images associated with CCTV networks are ones of an all pervading complex web of surveillance, the reality in many deployments is simple cameras with limited recording and monitoring. Indeed, some studies highlight how cameras have often been deployed solely for their deterrent effect and to create feelings of security and safety for individuals especially in shops and other retail premises for example.[777] Arguably, however, continued technological development for even the least costly CCTV systems and the spread of cheap digital systems have the potential to increase the sophistication of these CCTV systems.

The effectiveness of CCTVs

A prominent debate within academic, policy and public discourse on CCTVs is the degree to which they are effective in achieving goals and objectives which have been set for them.[778] This debate is also one which studies have addressed in different ways but which have drawn at times often broadly comparable conclusions.

Some of the main areas studies have explored in this regard are

- Public interrogation of the reasons and rationales given for CCTVs
- Public responses as to the impact and effectiveness of CCTVs
- The degree to which the public are involved in the decisions on the use and deployment of CCTVs in different areas and how this impacts on their effectiveness.
- Public knowledge of and understanding of how CCTVs are used, how data is collected stored and analysed from CCTV deployments and how this impacts on the their effectiveness
- Empirical research reviewing CCTV's impact on criminal and other anti-social activity.

In assessing the effectiveness of CCTVs, one key theme that emerges from the research is the nuanced understanding the public has in relation to the reasons and rationales given in public discourse for their use and deployment.[779] This was often set against the simplistic presentation and discourse of CCTVs in policy and security. This is often framed in terms of

[774] Hempel, Leon, and Eric Töpfer, op. cit., 2004, p. 3.

[775] For a review, see Hempel, Leon, and Eric Töpfer, "The surveillance consensus: Reviewing the politics of CCTV in three European countries", *European Journal of Criminology*, Vol. 6, No. 2, 2009, pp. 157-177.

[776] Hempel and Töpfer, op. cit., 2004, pp. 6-7.

[777] For a review of this and other elements of crime prevention through environmental design (CPED) strategies, see Kajalo, Sami, and Arto Lindblom, "How retail entrepreneurs perceive the link between surveillance, feeling of security, and competitiveness of the retail store? A structural model approach", *Journal of Retailing and Consumer Services*, Vol. 17, Issue 4, July 2010, pp. 300-305.

[778] Fussey, Pete, "Beyond liberty, beyond security: The politics of public surveillance", *British Politics,* Issue 3, 2008, pp. 120-135.

[779] Ibid.

the crime prevention function of CCTV deployment and its effectiveness in performing this function.[780] The studies show that the public is often aware of the discrepancy between the stated purpose and actual use of CCTV deployment. Indeed, considerable literature exists which criticises this framing of CCTV, some of which goes further in criticising the methodologies used which purport to show the positive impacts of CCTV on reducing reported crime statistics.[781]

Linked to these empirical findings is the differentiation between different groups of individuals and their reactions to and perceptions of CCTV surveillance. Public responses to the use of CCTV vary between countries, gender, age and other demographic characteristics such as class or race. Some studies have explored how CCTV is a possible mechanism of social exclusion or inclusion based on how different demographics interacted with the technology.[782] Most studies have drawn the same conclusion in terms of suggesting that it is unclear what effect CCTV has had on behaviours and activities of individuals that CCTV was positioned to prevent, such as crime and other anti-social behaviour.

An underreported aspect of the studies is the degree to which publics were involved in decision-making on CCTV deployment, a fact reflected in the different regulatory approaches adopted in relation to deployment.[783] Whether public involvement in decisions on CCTV has an impact on the effectiveness of the technology as a mechanism of surveillance is difficult to ascertain.[784] A further aspect of the studies is the observation that the public knows little about CCTV in terms of its operation but that as a result of widespread media coverage, interest in the technology is growing. Some have suggested that this lack of understanding and knowledge about the actual impact of CCTV on crime and other anti-social behaviour is a key factor in high levels of support for CCTV amongst some groups.[785]

CCTVs and impacts on individuals, groups and communities

As discussed earlier, one theme of empirical research exploring public attitudes to CCTVs is the possible impact the technology has on shaping and influencing behaviour.[786] In other words, is the knowledge that one is being watched, monitored and possibly recorded a significant factor in shaping how we act in spaces under CCTV surveillance? Different conceptualisations of the impact of CCTV on privacy are apparent in the research.

Some of the main findings in relation to this theme from reviewing studies are

- Public concerns over the impacts on privacy as a result of CCTV surveillance which differ between cultural contexts
- Differences in these concerns dependent on demographic characteristics

[780] Welsh, Brandon C., and David P. Farrington, "Effects of Closed-Circuit Television on Crime", *Annals of the American Academy of Political and Social Science*, Vol. 587, May 2003, pp. 110-135.

[781] Welsh, Brandon C., and David P. Farrington, "Public area CCTV and crime prevention: An updated systematic review and meta-analysis", *Justice Quarterly*, Vol. 26, No. 4, December 2009, pp. 716-745.

[782] For example, in relation to perceptions amongst vulnerable homeless people, see Huey, Laura, "False security or greater social inclusion? Exploring perceptions of CCTV use in public and private spaces accessed by the homeless", *British Journal of Sociology*, Vol. 61, Issue 1, 2010, pp. 63-82.

[783] Lett, Dan, Sean P. Hier, and Kevin Walby, "CCTV surveillance and the civic conversation: A study in public sociology", *Canadian Journal of Sociology*, Vol. 35 No. 3, 2010, pp. 437-462.

[784] Ibid.

[785] Webster, op. cit., 2009.

[786] Wigan, Marcus, and Roger Clarke, "Social Impacts of Transport Surveillance", *Prometheus*, Vol. 24, Issue 4, Dec 2006, pp. 389-403.

Reviewing the studies illustrates public concerns in relation to the privacy impacts associated with CCTV deployments varied by cultural, social and demographic characteristics. One of the most striking differences are between gender and age when the two were combined, e.g., young men were much more apprehensive of CCTV surveillance than older women. For the former, most studies which interrogated these attitudes saw young men (and young people generally) viewing CCTV deployment as particularly targeting them and targeting their activities with associated feelings of resentment towards their use.[787] In the UK, this impact of CCTV on anti-social behaviour was cited as one of the main reasons for public support for CCTV.[788]

A final concern noted in the studies we have reviewed was concerns but a lack of knowledge over how data captured by CCTVs is used. A part of this was attributed in the studies to a lack of clarity and transparency on the part of those operating CCTV surveillance networks. This was true of both private and public operators, including the police, of these CCTV networks. This was also demonstrated in some of the methodological difficulties that some studies encountered in attempting to research and study these surveillance networks. Reasons for this as articulated in the studies were varied, but these included concerns over whether or not deployments were in breach of data protection regulations. It was unclear in most circumstances how data protection was applied in relation to CCTV. Other concerns were over operational integrity or efficiency in relation to research teams being situated within work environments. A further concern that some studies highlighted was an unwillingness to specify uses of data where the concern was that future developments in technologies might allow for expanded uses of CCTV and the data collected.

CCTVs and impacts on spaces, places and areas

The knowledge of being watched in a particular space is like the impacts on privacy shaped by the manner in which people conceptualise how surveillance operates within these spaces. Studies have suggested that CCTV is the modern version of the panopticon as described by Foucault, or that they are the further development of the modern gaze through which nation states manage and govern their populaces. CCTV does point towards a revision of the panopticon thesis.[789] The panopticon as suggested by Bentham and analysed by Foucault involved a central tower around which there is a radial prison block, thereby allowing one guard to watch all prisoners. In contrast, most CCTV deployments as reported in the research are not monitored in real-time, and even in larger deployments there is a lack of immediacy between those watching and the monitoring screens. Even in critical areas such as airports, increased private sector involvement in providing security greatly complicates structures of security and surveillance governance.[790] The impacts of these trends on future public acceptance or rejection of CCTV remain to be assessed.

The common themes from a review of past studies in relation to this point are the following:

---

[787] Taylor, E., "I spy with my little eye: the use of CCTV in schools and the impact on privacy", *Sociological Review*, Vol. 58, No. 3, Aug 2010, pp. 381-405.

[788] Welsh, Brandon C., and David P. Farrington, "*Crime prevention effects of closed circuit television: A systematic review*", Home Office Research, Development and Statistics Directorate, London, UK, August 2002.

[789] See Walby, Kevin, "Open-street camera surveillance and governance in Canada", *Canadian Journal of Criminology and Criminal Justice*, October 2005, pp. 665-683.

[790] As an example see Klauser, Francisco, "Interacting forms of expertise in security governance: The example of CCTV surveillance at Geneva International Airport", *British Journal of Sociology*, Vol. 60, Issue 2, 2009, pp. 279-297.

- Members of the publics manifest different attitudes towards CCTV used in different places which are seen as either public or private spaces;
- Public attitudes towards knowing they are under CCTV surveillance in different areas and places
- How both of these differed for different demographics.

While studies show individuals displaying concerns over privacy in relation to the use of CCTV in certain circumstances, there is also a conceptualisation of the impact of CCTV in public vs. private spaces. Often what counts as a private or public space differs from country to country. From a review of the studies, it is unclear how aware members of the public are of being monitored or whether adequate signage was present highlighting that an area was under surveillance by CCTV.[791] Some studies did make use of observational research techniques, yet all of these had very different and in the end inconclusive findings as to whether any behaviour or set of activities were shaped by the presence of CCTV.

One common theme that emerged, despite these variations, was the identification of certain spaces as being seen to be off-limits to CCTV deployment. Unsurprisingly, these were more often than not those spaces and areas which were seen as being essentially private by citizens. These were washrooms, changing rooms and other areas which could be designated as being intimate spaces for citizens either individually or collectively. Studies which examined this phenomenon showed both differences between countries and a gradual gradient of what was considered to be a private intimate space. An interesting observation in one study was how the signage used in notifying people that they were under surveillance, at least in retail or service spaces, might have had an impact on individual experiences and behaviours in relation to using services or purchasing products.[792]

Linked to the concerns above studies also sought to investigate how publics and different demographics responded to the knowledge that they were under CCTV surveillance in particular places. Here some studies illustrated the negotiations and shifts in values in terms of social control CCTVs represent, such as in their use in schools as an example.[793] In the main as with the other aspects of demographic differences we have noted young male individuals rejected more than most the presence of CCTVs. Some studies for example reported how this category of individuals felt targeted by CCTVs which extended to both their behaviours and the locations that they would more often than not frequent as a part of their social and daily activities.

CCTVs and themes of acceptance and resistance

We have already touched on some of the findings in our review of past studies as to the levels of acceptance and resistance from publics to CCTV surveillance technologies. 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 over the use of and deployment of CCTV. Indeed, there are even fewer commonalities if we are to consider the role of public acceptance and rejection outside of the EU.

---

[791] Neyland, Daniel, "Closed circuits of interaction?", Information, Communication & Society, Vol. 7 Issue 2, June 2004, pp. 252-271.

[792] Tsung, Chi Liu, and Feng Chen Cheng, "Please smile! The CCTV is running", *The Service Industries Journal*, Vol. 31, No. 7, May 2011, pp. 1075-1092.

[793] Hope, Andrew, "CCTV, school surveillance and social control", *British Educational Research Journal*, Vol. 35, No. 6, December 2009, pp. 891-907.

These can be grouped under several headings, as follows:

- CCTVs are perceived as having different qualities in different spaces;
- CCTV has different impacts on different categories of individuals;
- CCTV data can be viewed in multiple ways;
- The effectiveness of CCTVs for some publics is linked to support or resistance of the technologies.

CCTV as a surveillance technology is embedded in a complex web of social relationships and technological interactions.[794] This complexity is highlighted by nearly all studies as a key element of understanding public attitudes towards and acceptance of CCTV.

One recurrent theme of all studies was the differences and variations in how data captured by CCTV was used by those controlling surveillance networks and publics subjected to such surveillance. Some have suggested that CCTV represents a defining quality of modern urban spaces and their governance and management.[795] Here as discussed above in relation to the sophistication or not of different surveillance networks, studies revealed a complexity in how data is treated. One important area related to this was concerns over the gradual shift to digital from analogue recordings and the potential implications of this.[796] In most studies, both publics and the researchers cited this as a concern as data becomes cheaper to retain, easier to analyse and transfer making sharing between different parts of the surveillance system and with others relatively simple. This trend will have implications for public acceptance or resistance to CCTV as the implications for data become more known and understood by publics.

One of the most critical elements in determining public acceptance or rejection of CCTV is the spaces where they are deployed and used. Indeed, this would extend to publics being able to determine and influence those spaces which are seen as being beyond the pale in terms of being subjected to CCTV enabled surveillance. For example, the URBANEYE project reported that some 73.4% of participants saw CCTVs being placed in changing room or washrooms as a bad thing.[797] The project recounted that differences in how public and private spaces are defined continue to be sites of resistance for CCTV deployment. In some European countries, the public views open-street CCTV surveillance as privacy intrusive where city centres are viewed as a collective private space.

The final factor in determining overall levels of public acceptance or rejection of CCTV technologies is related to the actual or perceived success of CCTV in achieving the goals that discourses promoting their use are able to demonstrate. All of the studies which were reviewed sought to highlight this aspect as one which was important for further research to address. Some literature also called for existing methodologies related to linking CCTVs to impacts on crime through reviewing crime statistics needed to be revisited and reformed and their use in policy discourses challenged. Often studies reported how CCTVs were seen in some ways as a panacea for problems associated with modern societies and in particular for modern urban spaces.[798] Most studies agreed in their conclusions that the evidence to support

[794] Fussey, op. cit., 2008.

[795] Wood, David Murakami, David Lyon and Kiyoshi Abe, "Surveillance in urban Japan: A critical introduction", *Urban Studies*, Vol., 4 No. 3, March 2007, pp. 551-568.

[796] Graham, Steven, and David Wood, "Digitizing surveillance: Categorization, space, inequality", *Critical social policy*, Vol. 23, No. 2, 2003, pp. 227-248.

[797] Hempel and Töpfer, op. cit., 2004, p. 43.

[798] For a critique, see Talyor, Emmeline, "Evaluating CCTV: Why the findings are inconsistent, inconclusive and ultimately irrelevant", *Crime Prevention and Community Safety*, Vol. 12, No. 4, 2010, pp. 209-232.

this while holding valid in some circumstances did not in all and that successes could repeatedly be set against failures.

CCTVs and smart surveillance technologies

In addition to being one of the more ubiquitous surveillance technologies in Europe, CCTV is at the vanguard of smart surveillance technological development. CCTV represents an existing extensive network of surveillance technologies in most countries. CCTV is the most prominent technology used in critical spaces such as transport hubs where operators champion of the advantages of smart surveillance technologies.

Technology developers are making cameras smart in several ways. Different projects aiming to achieve this have focused on different mechanisms for making smart CCTV surveillance networks and devices. One typology for understanding the development and evolution of CCTVs is to see them moving beyond simply passive watching and recording of visual images to where they can

- Talk or otherwise interact with environments and individuals;
- Listen or otherwise use other sensory information from monitored environments and individuals;
- Act intelligently and independently or with a mixture of human and machine control.

Talking CCTV can be seen as a relatively simple modification of existing networks. Pioneered in the UK, such systems allow CCTV operators to interact with monitored environments, by giving warnings or issuing instructions to individuals who are being recorded. This is a further evolution of attempting to shape, influence and regulate behaviours in spaces where these CCTVs can be found. Further means of enabling CCTV systems to interact with environments might include their embedding in ambient intelligent environments.

Another development in terms of creating smart CCTVs has been projects exploring means by which CCTV can be trained to listen for noises that deserve or warrant further investigation. Such systems are automated and point to CCTVs being programmed in order to recognise audio and visual cues for suspicious behaviours and activities.[799]Examples of projects researching and promoting these developments include the European funded project SAMURAI.[800]

Knowing how these trends will turn out is difficult but it is undeniable that CCTV in its current form is dramatically changing from simply being passive recording devices to interactive elements of a smart surveillance infrastructure and network. Already some of these developments can be seen in systems which are programmed with automatic recognition, such as recognition of car number plates and facial recognition.

Conclusions

As noted earlier, CCTV is one of the most established forms of surveillance in many countries, in the EU and internationally. A wide range of studies examine CCTV and its impact on society and individuals. As such, there is a large empirical base of evidence to

[799] Coudert, Fanny, "When video cameras watch and screen: Privacy implications of pattern recognition technologies", *Computer Law and Security Review*, Vol. 26, No. 4, 2010, pp. 377-384.

[800] SAMURAI is the acronym for "Suspicious and Abnormal behaviour Monitoring Using a netwoRk of cAmeras for sItuation awareness enhancement". See http://www.samurai-eu.org/

make some conclusions as to these impacts, how members of the public view the technology and the degree to which they accept or reject the technology. Based on this large body of empirical evidence, one can make various observations.

CCTVs are specific from other surveillance technologies, smart and non-smart. They have characteristics not found in other technologies. Future developments in CCTV and the networks of surveillance they represent are trending towards smart surveillance with an immediate impact and visibility for individuals and society. Some of the differences between CCTV and other surveillance technologies are peculiar to the ways in which CCTV is operated as part of surveillance practices. They are often technologically simple, used in diverse settings and are in most countries an established feature of "public" life.[801]

A key difference between CCTV and some other surveillance technologies is the wide variety of actors that make use of them. Often and in most contexts, there is little or no regulation for how the private sector uses CCTV. While there is some compliance issues in terms of data protection, regulatory oversight is not universal and its impacts on slowing the proliferation of CCTV in different places, spaces and for different purposes appears to be minimal. Some studies explore this to some degree, but there is little in the way of a definitive common explanation for why there is such minimal regulatory oversight. As such, like all research, the specific social, cultural and policy contexts impact on the main findings of the studies and the theoretical framing for carrying out the research in the first place. In different ways and in different respects, the conclusion is that public acceptance or not of CCTVs is nuanced and detailed and heavily dependent on cultural, spatial, social and individual demographic characteristics.

Smartphones and surveillance

Another technology which has become pervasive is the smartphone. In the final quarter of 2010, some estimates suggested almost 80 million smartphones had been shipped worldwide, an almost 100% increase on the previous quarter.[802] Their popularity as a consumer device is common across all countries with increasing usage and increasingly bitter conflicts between companies seeking to expand their market share.[803] Smartphones have quickly established themselves as a popular and ubiquitous consumer technology with a recent Gartner report stating that as of 2010, 296 million smartphones had been sold.[804]

Their utility as a tool for surveillance came to light after media stories reported the tracking capabilities of these phones (they are able to provide geo-location data on users). Their ability to locate where individuals are and where they have been makes them a tool for law enforcement authorities in preventing or detecting terrorist related threats and criminal activities. For example, forensic examination of cellphone records, of calls and location data, helped identify those responsible for the 2004 Madrid bombings.[805] Commercial enterprise

[801] With specific variations between some countries as recounted in the section.

[802] Ahonen, Tomi, "Analysis: Record 80 Million Smartphones sold in 3Q 2010", BSN, 22 November 2011.

http://www.brightsideofnews.com/news/2010/11/22/analysis-record-80-million-smartphones-sold-in-3q-2010.aspx

[803] See, for example, Apple and Google's ongoing court battles over IP infringement in relation to Apple's iPhone and Google's Android operating system.

[804] Gartner Newsroom, "Gartner Says Worldwide Mobile Device Sales to End Users Reached 1.6 Billion Units in 2010; Smartphone Sales Grew 72 Percent in 2010", 9 February 2011.

http://www.gartner.com/it/page.jsp?id=1543014

[805] Times Online, "29 charged over Madrid train bombings", *The Times*, 11 April 2006.

also finds these phones of value in recording patterns of behaviour when a customer uses services or buys products.[806] This data can oftentimes be extensive; one recent German user found that his phone provider had recorded his location over 35,000 times over a six-month period.[807]

Public resistance to the surveillance capabilities of smartphones has not been as pronounced as the often strong condemnation of these abilities in the media or by privacy advocacy groups. In some instances, lack of public awareness about the capabilities or practices of surveillance is clearly evident. A recent Canadian survey found that 40% of people did not set either a password for their device or adjust any privacy-related settings.[808] Furthermore, in illustrating this lack of public awareness, the study found that 70% of respondents did not believe their mobile phone stored any personal information.[809] Similar levels of low public awareness have also been found in relation to data being stored on smartphones that can be accessed remotely. A study by Juniper Networks found that, for the majority of respondents (more than half), the biggest concern was loss of the device rather than other network-related threats.[810]

Smartphones continuing popularity and expanded range of uses[811] and the perceived value in how data captured by them can be used in public and private settings suggest that as a smart surveillance device, they will grow more visible in terms of public acceptance or resistance. As of yet, however, there lacks a body of empirical evidence exploring this. Smartphones are an example of how the range of functions devices can perform or enable often lead to unforeseen consequences in terms of surveillance and privacy.

RFID and surveillance

In contrast to smartphones, radio frequency identification devices as an important technological development with uses in the private and public sectors have received widespread attention as to their implications for privacy and surveillance. Their use as a tool for surveillance has also been widely reported and recognised. The potential privacy impacts of RFID prompted the European Commission to issue a Recommendation on RFID which, among other things, called for the development of a data protection impact assessment framework specifically for RFID. Industry groups subsequently develop such a framework which was endorsed by the Article 29 Working Party in February 2011.[812]

---

http://www.timesonline.co.uk/tol/news/world/europe/article704414.ece

[806] See, for example, Richards, Jonathan, "Shops track customers via mobile phone", *The Times*, 16 May 2008. http://technology.timesonline.co.uk/tol/news/tech_and_web/article3945496.ece

[807] Cohen, Noam, "It's Tracking Your Every Move and You May Not Even Know", *The New York Times*, 26 March 2011. http://www.nytimes.com/2011/03/26/business/media/26privacy.html

[808] Abma, Derek, "Do a better job protecting mobile privacy, Canadians told", *The Vancouver Sun*, 26 August 2011.

http://www.vancouversun.com/technology/better+protecting+mobile+privacy+Canadians+told/5311241/story.html

[809] Ibid.

[810] Juniper Networks, "Risky Business: Survey Shows Smartphone Security Concerns Running High; Yet 81 Percent Admit Sneaking Onto Employer Networks Without Permission", 26 October 2010.

http://www.juniper.net/us/en/company/press-center/press-releases/2010/pr_2010_10_26-10_02.html

[811] For example, mobile connection to social networking sites, ability to conduct financial transactions.

[812] See http://ec.europa.eu/information_society/policy/rfid/pia/index_en.htm

While industry, policy and academic research have examined the consequences of RFID in some detail, it is less clear that public concern, awareness or resistance is as widely understood or even investigated. While a protest by a digital rights group was successful in halting the use of RFID tags in a retail space, it was not clear or reported whether the public had the same concerns as those protesting. As only 40 people were present at the protest, the issue seems not to be prominent in the minds of customers, although the company did not inform its customers that it was using RFID.[813]

Public resistance to RFID enabled devices and services may increase, as it has with smartphones, as more uses are found for the data generated by these devices. One report highlights how smartcards with RFID tags provide a means whereby individuals can investigate partners who they suspect of infidelities by being able to reveal their location and spending habits.[814] As with smartphones, further empirical research is needed to accurately assess public attitudes and possible resistance to surveillance by RFID-enabled devices and services.

Smart surveillance technologies in the workplace

One interesting example of an activity which traditionally has been the site of surveillance and which is seeing further developments in smart surveillance practices and technologies is work and the work-place. Organisations justify surveillance in this context principally by

- Behavioural monitoring to measure efficiency and performance
- Monitoring to ensure employee or customer safety
- Monitoring to ensure employee compliance with employer conditions.

While the workplace is not a "public" space, surveillance in the workplace is extensive, pervasive and offers some revealing insights into how it is experienced, resisted or accepted. The workplace is the site for many deployments of smart surveillance technologies, as well as extensive use of traditional surveillance technologies. Public resistance to surveillance in the workplace is limited due to the perception that these spaces are private.[815]

Surveillance technologies used in the workplace are varied. They include biometric ID cards, especially in workplaces where demands for security are prominent such as airports. Computer-based monitoring of performance (keystroke and visual recording) are also used. Extensive CCTV can also be a feature of some modern workplaces. Future trends and developments include the proposed use of soft biometric surveillance devices, for monitoring the physiological condition of employees, of use in the transport industry, to detect when drivers need to rest and sleep or detect when physiological conditions pose a danger to the individual or others.[816] More routine practices of surveillance include monitoring office computers and office e-mail, where studies have found that a majority of individuals may be unaware of organisational surveillance.[817]

---

[813] Libbenga, Jan, "German revolt against RFID", The Register, Mobile, 1 March 2004.

[814] Bloomfield, Steve, "How an Oyster card could ruin your marriage", *The Independent on Sunday*, 19 February 2006.

http://www.independent.co.uk/news/uk/home-news/how-an-oyster-card-could-ruin-your-marriage-467077.html

[815] Also the fact that employers in most countries have leeway in establishing what the conditions of employment are.

[816] For an example of EU-funded research in this area, see http://www.actibio.eu:8080/actibio

[817] Dillon, Thomas W., and Daphyne S. Thomas, "Knowledge of Privacy, Personal Use, and Administrative Oversight of Office Computers and E-mail in the Workplace", *Information Technology, Learning and Performance Journal,* Vol. 24, No. 2, 2006. http://www.osra.org/itlpj/dillonthomasfall2006.pdf

A study conducted by the Hong Kong Privacy Commissioner found that more than 80% of companies routinely used one or more surveillance technologies, that 64% considered these surveillance practices to be privacy intrusive but did not impact employee relations and that, overall, 41% saw it as being beneficial for company procedures and operations.[818] As with other instances or surveillance discussed here, the relative inability of employees to resist surveillance may be a factor in its routine use by companies. As with other technologies, the specific use of surveillance technologies in the workplace and public attitudes to these are relatively under–researched.

4.3.2 Factors Affecting Public Opinion

For a variety of reasons, there is no single 'public opinion' on new technologies. Due to their varying contexts, capabilities, visibility, effect and comprehension, opinion can vary greatly. However it is possible to isolate certain more general factors which appear key to the shaping of opinion. These come together (balanced differently dependant on context) to chart a background to each perception.

A range of demographic qualities play a role (age and gender demand mention). Amongst these, nationality and national culture are specifically important. As Samatas clarifies in the Greek context, the history and cultural background of a state has specific relevance in relation to the consideration of surveillance.[819] This defines a series of further issues and consequently defines the borders within which the further specifics of a technology will be received. As examples of this it is possible to consider the lack of the tradition of ID cards in the UK[820] and the significant resistance their introduction has encountered, or how survey participants in Northern Ireland differed to those in the UK when considering CCTV (considering its historical and authoritarian connotations in public use and its perceived lack of necessity in private use).[821] This was also the finding in the PRISE project, where debates over the deployment of new security technologies were deeply linked to debates over national public morals.[822]

Connected to the above point will be the effect of the individual's current (and past) stance on matters perceived to be relevant to a given technology. For example, should an individual feel particularly strongly about the issue of data protection, it is unlikely they will greet the broad introduction of biometric ID cards favourably. Related to this will be an individual's broader social tendencies. For example, as Murphy points out, public perception of the privacy vs.

---

[818] Office of the Privacy Commissioner, Hong Kong, "*Survey on Monitoring and Personal Data Privacy in the Workplace*", October 2004, p. 12.

http://www.pcpd.org.hk/english/publications/files/Workplace_report.pdf

[819] Samatas, Minas, "Studying Surveillance in Greece: Methodological and Other Problems Related to an Authoritarian Surveillance Culture", *Surveillance & Society*, Vol. 3, No. 2/3, 2005, pp. 181-197.

[820] Backhouse, James, and Ruth Halperin, "A Survey on EU Citizen's Trust in ID Systems and Authorities", FIDIS Deliverable 4.4, London School of Economics and Political Science, London, 2007. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.4.survey.pdf

[821] Murphy, Oliver, "A Surveillance Society: Qualitative Research Report", Report prepared for COI on behalf of ICO, Wilmslow, Cheshire, UK, 2007.

http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/surveillance_report_v6_final.pdf.

[822] Jacobi, Anders, and Mikkel Holst, "Synthesis Report - Interview Meetings on Security Technology and Privacy", PRISE Deliverable 5.8, 2008. http://www.prise.oeaw.ac.at/docs/PRISE_D_5.8_Synthesis_report.pdf.

security debate can be broken into three groups who share similar characteristics. In the more authoritarian group for example, respect and trust for authority and the prioritisation of security over other social goals is a key feature. As a result of this it is possible to assume that members of this group would respond more favourably to deployed surveillance technologies than those of another group in which these traits were less prevalent.[823]

As the complexity and novelty of much new technology leaves a scarcity of solid points from which to formulate a position, a significant body of information regarding the use and operation of this technology will be second hand. In this respect it is enlightening to consider the amount of real encounters with new security technologies. Whilst specific evidence is scarce (an ORC survey from the American context from 2002 suggests that only 5% of respondents actually provided biometric characteristics that year), a picture begins to be built when considering the more in depth interview answers in the PRISE project, for instance, where opinions on technologies became increasingly theoretical and anecdotal as the novelty of the technology increased. It would seem logical to suggest that the prevalence of personal damage felt as perceived result of the use of these technologies may also be relatively small. Thus, sources such as the media and other public sources will play a significant role in the building of conceptions of technology, its operation and the tone of opinion. Many of these sources have their own internal logic and founding positions and as such the consideration of the consequences, problems and operation of a technology will rarely be presented objectively and presentation will often be situated within other, broader, debates. Indeed, significant and relevant knowledge, awareness and factual understanding can often be obscured by this merging of debates and the hidden, or background, logic of the sources involved in creating the opinion discourse.[824] For example, the striking, easily identifiable term, "naked scanner" comes with a series of background connotations and its use immediately conveys a series of emotions which can immediately damage the public view on the technology.

Each technology also conjures up images based on its presented operation. Certain of these images may provoke more immediate reactions of unease than others. For example, retinal and iris scanning may be received differently from other forms of biometric partially as they are seen to be focussed on a particularly fragile and vital area of the body while the obvious impact of the body scanner, or 'naked machine' immediately conjures negative images of blunt tangible bodily privacy invasion. The PRISE project specifically points out a high resistance to 'physically intimate technologies'.[825] Secondly, each technology is referenced to preceding technologies. When there are a greater number of reference points for the operation and effect of a technology, its reception will be predicated on these references. For example, fingerprinting as a biometric perhaps receives different attention to other biometrics as the concept of fingerprinting has a significant history of use as a unique identifier.[826] It may thus

---

[823] Murphy, Oliver, "A Surveillance Society: Qualitative Research Report", Report prepared for COI on behalf of ICO, Wilmslow, Cheshire, UK, 2007.

http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/surveillance_report_v6_final.pdf.

[824] Strickland, Lee S., and Laura E. Hunt, "Technology, Security, and Individual Privacy: New Tools, New Threats, and New Public Perceptions", *Journal of the American Society for Information Science and Technology*, Vol. 56, No. 3, 2005, pp. 221–234.

[825] Jacobi, Anders, and Mikkel Holst, "Synthesis Report - Interview Meetings on Security Technology and Privacy", PRISE Deliverable 5.8, 2008. http://www.prise.oeaw.ac.at/docs/PRISE_D_5.8_Synthesis_report.pdf.. p.20.

[826] ORC International, "Public Attitudes Toward the Uses of Biometric Identification Technologies by Government and the Private Sector", Summary of Survey Findings for SEARCH, 2002. http://www.search.org/files/pdf/Biometricsurveyfindings.pdf .

be that the public feel a certain capability in evaluating the technology which they may not with others (whether this evaluation is correct or not is another question). The same is true of the location, logic and action of use. The more the public can associate with, and establish precedent for use in a context, the more solid opinion formation will be.

EU Project: PRISE

In section 1 of PRISE deliverable 5.8, citizens' perceptions and acceptance of specific security technologies are considered. The selected technologies include biometrics, CCTV, scanning technologies, locating technologies, eavesdropping, data retention and privacy enhancing technologies. The report emphasizes that biometrics are "more likely to be generally accepted in border control applications"[827], (to whit a considerable group accepted being pre-registered) and that the more serious concerns related to biometric technologies are function creep and identity theft. The acceptance of scanning technologies is also strictly connected to the site of use ("widely accepted in airports"[828]), while for locating technologies and for eavesdropping "a large majority of the participants would only accept the use of these technologies based on a court order"[829]. Finally, data retention and data mining techniques are only accepted when used for investigation of crime and terror.[830]

Within this evaluation, the sphere of use, namely whether the proposed technology occupies an economic, social or other space, will also define the mode and factors of acceptance. Backhouse comments on the acceptance of technologies used by the state as being based not only on systemic reference points, but also public feeling as to the 'trustworthiness' of the operating institutions. Significant factors in this regard are the levels of competence, benevolence and integrity each institution and structure is seen to have. In the economic context, while the same factors are taken into account in relation to the levels of trust and 'trustworthiness' of an industry or organisation, these are accompanied by a further series of considerations equating to a cost benefit analysis of the use and acceptance of the new technology – the 'privacy calculus'.[831] In this calculus the public will consider whether a technology embodies expectations of procedural and distributional fairness in operation.

4.3.3 Public Opinion Generally Lacks Solid Understanding or a Factual Base On Technologies Themselves

The range of new surveillance technologies and the difference in their operation makes it difficult to pinpoint universal attitudes. However, certain trends and factors in current opinion can be isolated. Perhaps the most significant of these is that the public has little solid understanding of many new technologies or their operation. Public understanding of a technology comes about through a series of reference creations which build a body of comprehension, placing the technology more solidly within broader conceptions. The novelty of technology (at least in the public mind) and the complexity of its operation and effects

[827] Jacobi, Anders, and Mikkel Holst, "Synthesis Report - Interview Meetings on Security Technology and Privacy", PRISE Deliverable 5.8, 2008. http://www.prise.oeaw.ac.at/docs/PRISE_D_5.8_Synthesis_report.pdf.. p. 16

[828] Ibid.

[829] Ibid., page 17

[830] Ibid., page 18.

[831] Culnan, Mary. J., and Pamela K. Armstrong, "Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation", *Organization Science*, Vol. 10, No. 1, 1999, pp. 104-115.

often means this process is currently in a state of flux. In essence the public still lacks the templates through which to view these technologies. As a result of this the critical features and impacts at each social level are subject to a series of uncertainties which, refracted through the above features influencing perception, may paint a significantly distorted picture.

Firstly, the technological understanding of new surveillance technologies such as RFID or biometrics is not always within reach of the general public. This is not to say its comprehension is impossible (at least comprehension of the relevant activity even if not of the technical specifics), simply that this information is often not presented.[832] As a consequence, a comprehension of the function, capability and the inherent danger in each technology is assumed from other references (or sometimes not at all). In public perception, for example, the terminology is often significantly confused; terms for families of technologies are sometimes presented and viewed as one technology and vice-versa. Judging from uncertainty in other aspects of perception, it seems reasonable to assume that the public thus is not always aware of exactly aware of what is being discussed.[833] For example, the term biometrics does not describe one single technology but rather is an overarching description for a series of identification technologies, including second generation behavioural identifiers. Each of these differs significantly from the others in use, capability, privacy impact and technology with significant practical consequences depending on context.

Secondly, the consequences and important impacts of many new technologies comes not in their isolated use (although in isolated consideration some technologies such as body scanners have a more visceral and obvious privacy impact) but in their combination with other technologies or systems. For example, there is a significantly reduced privacy risk in 1:1 systems than with 1:N systems connected to central, or even multiple, databases ("a system capable of performing 1:N searches can be considered more susceptible to privacy-related abuse than a 1:1 system. A 1:N biometric system would be necessary for use in any indiscriminate large-scale searches" [834] whilst a 1:1 system would be used for simpler verification purposes). It is often the consequent data processing operations, which are not part of the technologies themselves, which create the critical privacy impacts. The same problem then presents as considered above in relation to the public conception of data protection and privacy generally, namely that the environment in which the risks manifest is incredibly complicated and largely invisible to the individual. Thus when risks are presented on any level, from the individual to the social, there is a lack of clarity as to how they relate to any specific technology.[835]

This leads to somewhat of a paradox. It is technology, its deployment and combination (as well as its combination with data processing capabilities) that provides the foundation for the development of surveillance in modern society. However, the lack of clarity in

[832] Strickland, Lee S., and Laura E. Hunt, "Technology, Security, and Individual Privacy: New Tools, New Threats, and New Public Perceptions", *Journal of the American Society for Information Science and Technology*, Vol. 56, No. 3, 2005, pp. 221–234.

[833] For an example of the interchange between discussing unique technologies and references to the overarching family. ORC International, "Public Attitudes Toward the Uses of Biometric Identification Technologies by Government and the Private Sector", Summary of Survey Findings for SEARCH, 2002. http://www.search.org/files/pdf/Biometricsurveyfindings.pdf .

[834] International Biometrics Group LLC, "The BioPrivacy Application Impact Framework", IBG Bioprivacy Initiative, 2010. http://www.bioprivacy.org/bioprivacy_text.htm.

[835] Strickland, Lee S., and Laura E. Hunt, "Technology, Security, and Individual Privacy: New Tools, New Threats, and New Public Perceptions", *Journal of the American Society for Information Science and Technology*, Vol. 56, No. 3, 2005, pp. 221–234.

comprehension or perception of technology means the public is often left making presumptions about the significance and capability of its operation (both as it stands alone and as part of a wider infrastructure). This provides a poor basis for the formation of a picture either of the nature of technology within surveillance, surveillance infrastructures or either against or within a wider social background.

EU Project: BITE

From the 15th March to the 15th June 2006, the **BITE** project (*Biometric Identification Technologies Ethics*)[836] carried out an online public consultation on **"**ethical and social implications of biometric identification technologies" that had over 5300 respondents from Europe and other countries. The respondents were stakeholders coming from universities, large enterprises or SMEs, and governmental bodies directly involved in biometrics. According to the BITE consultation final report, the vast majority of respondents (77.61%) thinks that covert biometrics is expected to be widely used and an important portion of respondents (20.9%) thinks that is already widely used. A large majority of respondents also believes that covert and remote biometrics presents critical ethical issues that should be publicly addressed. Biometrics are expected to be used in surveillance applications in conjunction with other technologies such as CCTVs and RFID. The vast majority of respondents also thinks that the risk of function creep in biometrics applications for surveillance purposes are high (44.7%) or very high (34.7%). However, when asked about citizens' acceptability rates for biometrics for surveillance purposes, respondents seem to be quite uncertain and their answers range between significantly distant poles.

4.3.4 Fears

Whilst there is an awareness of the potential and usefulness of surveillance in certain situations[837] (particularly in recognised security hotspots), a recurring point in each survey is the uneasiness with which new surveillance technologies are considered and greeted even as they purport to answer supposedly critical and desired social needs such as the fight against terrorism. This is partly due to the lack of technological understanding but it is also due to the awareness that the proliferation and perceived deterministic use of technologies may be creating something more sinister and potentially threatening to fundamental social principles (indeed a certain PRISE minority stated they would not accept biometrics under any circumstances).[838]

Firstly, there is further uncertainty about the reasoning and targeting behind much surveillance technology and the logic according to which it is alleged to achieve its stated ends (70% of respondents did not believe the technology was effective against terrorism but that it was deployed to create the appearance of action).[839] The logic of technology at the expense of other potential solutions (such as tackling the causes) is questioned as are certain other assumptions of deployment such as that a violation of privacy without significant proof of intent is justified (this is not always a present assumption, but in certain surveillance

[836] http://www.biteproject.org

[837] Jacobi, Anders, and Mikkel Holst, "Synthesis Report - Interview Meetings on Security Technology and Privacy", PRISE Deliverable 5.8, 2008. http://www.prise.oeaw.ac.at/docs/PRISE_D_5.8_Synthesis_report.pdf. p 23.

[838] Ibid., p. 16.

[839] Ibid., p. 22.

technologies there is a necessary relinquishment of privacy without the necessity for any intent to be demonstrated). Uncertainty arises partially due to the complexity and breadth of the related social issues and the difficulty in tracing a path of causation debates social debates and technological deployment and partially as the technologies are seen to have widespread potential outside their designated deployment purposes (function creep). Following this, there is a perception that leads people to be wary about taking surveillance technology related steps, as they feel that once a technology is deployed it will be very difficult (even impossible) to ever remove it while the strength of limitation on function is often difficult to discern. The perception of the non-transparent development of a surveillance infrastructure is present in public imagination.

The consequences of this are perceived equally subtly. In a broad sense it appears that the public perceive surveillance technologies as technologies of power relations. Indeed it is not the technologies themselves that are directly disapproved of, it is the feeling of being 'under suspicion' that they engender on the part of the observed which appears to be of key concern. Perhaps considering the confusion in the logic of deployment and networks of relations, it is a common theme that the lack of identification and clarity as to the 'who and why' of the controllers is seen as a significant concern (the reality and proximity of this fear is closely tied to levels of trust). There is thus an abstract appreciation for the ability of these technologies to reshape key relationships and concepts within society; however, the theoretical awareness of possibility does not seem to stretch to a more elaborated perception as to how this might happen.

At an individual level general data processing fears are transferred onto the background of each new technology, with respondents listing concerns such as the occurrence of ID fraud, function creep, secondary use and misuse.[840] This finding also came through in the PRISE project, as in each of the six countries surveyed there was a strong conviction that security technologies would be abused (function creep, misuse) and create direct personal effects. It is indicative of the apparent gap in understanding of individual technologies as opposed to their presence in wider infrastructures or as part of wider debates, that the precise manifestation of these effects, or fears specifically related to one technology, rarely arose without prompting.

4.3.5 Public Desires

Following from the above there are certain public desires that can be isolated in relation to surveillance technologies of all descriptions. Firstly, the lack of knowledge and certainty about what they are and how they are to be used should be addressed.

Secondly, there is a perception that there is little debate on the theme; why, which and how, to deploy each technology and this should be addressed. It is seen that, as the effects of the technologies could be so significant, there should be a debate including a wider range of possibilities and which should include a wider range of stakeholders in the process.

Before the deployment of each technology, to reduce the potential for function creep and privacy impact, the public believe that the privacy impact should be carefully analysed and considered against potential gains.

---

[840] Backhouse, James, and Ruth Halperin, "A Survey on EU Citizen's Trust in ID Systems and Authorities", FIDIS Deliverable 4.4, London School of Economics and Political Science, London, 2007. http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp4-del4.4.survey.pdf

Finally, there should be further transparency and controls on the operation and use of each technology. This can be seen as a reflection of the perceived need for control over the social impact of the technology, the consequences of its wider deployment and the potential for function creep and misuse. The use of court orders in criminal investigations as manifestations of a balance of power was a popular idea.[841]

4.3.6 Conclusion

When considered alone or as part of wider assemblages it is evident that the technical capabilities of surveillance technologies are not often understood whilst in their presentation, the terminology is mixed and uncertain and the boundaries of discourse around and between technologies are fluid. As a consequence, the public has difficulty in forming images of the technologies themselves or of locating their relevance in wider and equally complex social debates. It is thus very difficult to evaluate what they mean or the wider systems they are part of based on relevant factual starting points. As a result of this, whilst surveillance technology may be accepted in limited spheres, there is general uneasiness around it and what it might mean for the individual and society, and a general perception that more democratic involvement and control is needed.

As a result of this lack of clarity it is other opinion shaping factors that become significant in whether technology is accepted and the role it plays in wider debates (such as how technologies are presented in the media or the immediate reaction they elicit). In this sense it is peculiar that, whilst the technologies and the systems in which they operates are the active features in the privacy impact, it is in fact their references in relation to other debates or perceptions that play the active role in public opinion formation.

4.4 THE ACADEMIC DISCOURSE ON PUBLIC PERCEPTION OF PRIVACY AND SECURITY

There is extensive academic literature on the topic of surveillance reflecting a number of different academic discourses informed by different theoretical frameworks and approaches.[842] There is less discourse on the relatively new topic of smart surveillance but what discourse there is often is built upon the theoretical framings and issues of the topic of surveillance. Furthermore, academic discourse on specific technologies, which are an element of surveillance practices, is at times extensive.[843] An example of this is the considerable research and debates which exist in relation to CCTV across Europe, some of which has already been discussed in this report. Academic reflection on public attitudes is likewise a substantial field as is the already discussed centrality of public opinion in the functioning of democracies and how the public interacts with new technologies. In considering the theoretical framings which underpin academic discourse dealing with surveillance and the public's understanding and acceptance of practices and related technologies, we examine briefly the key theoretical issues upon which such discourses are grounded.

---

[841] Jacobi, Anders, and Mikkel Holst, "Synthesis Report - Interview Meetings on Security Technology and Privacy", PRISE Deliverable 5.8, 2008. http://www.prise.oeaw.ac.at/docs/PRISE_D_5.8_Synthesis_report.pdf. p. 26.

[842] Lyon, David, *Surveillance Society: Monitoring Everyday Life",* Open University Press, Buckingham, 2001.

[843] Ball, Kirstie S,, "Elements of surveillance: A new framework and future directions", *Information, Communication and Society*, Vol. 5, No. 4, 2002, pp. 573–590.

Exploring issues in which academic arguments are grounded provides us with a deeper insight into how these academic discourses on surveillance are framed. Our examination of the academic discourse focuses on theories predominantly found within the social sciences. Here, arguments are made in light of what constitutes the public, their acceptance or rejection of surveillance technologies and the societal structures and institutions and their relationships with publics in the conduct of surveillance activities.[844] Our discussion aims to be informative in identifying some of the major theoretical approaches to an understanding of the public, surveillance practices and technologies and why these are prevalent themes in modern societies, which incorporates state as well non-state actors and their relationships. We focus on what academic discourse has to say about the factors that determine public acceptance or not of surveillance practices and surveillance technologies.

Academic discourse on public acceptance of surveillance incorporates various theoretical viewpoints. Much of the theoretical debate offers interpretations and conclusions that are drawn from the empirical research we discuss in this report. The manner in which results or findings from these empirical findings are interpreted by academic discourse is determined by the particular theoretical lens through which these findings and results are viewed.[845] Indeed, it is impossible in most cases not to have some theoretical framing by which one attempts to make sense of findings drawn from empirical research. It is also impossible to offer an overview of all of the specific elements making up the theoretical backdrops to these academic discourses; hence, we have identified what each of these has to say about the factors influencing public and societal acceptance or resistance to surveillance and related technologies.

In understanding where academic discourse is "coming from" in terms of the construction of theoretical frameworks, we suggest that there are four main thematic areas of relevance which, while not exhaustive of all possible positions, represent the major aspects of most academic discourse in relation to surveillance. These are

- new technologies and theoretical frameworks related to public understanding and public engagement,
- theoretical frameworks on surveillance societies and governance,
- theories of the Information and Risk Society and
- engaging with the social sciences.

Examining each of these forms the remainder of this section. This is, we acknowledge, a relatively brief summation of major theoretical underpinnings in academic discourse in relation to surveillance, society and publics. We believe, though, that it yields insights into some of the debates into the relationships and factors determining public acceptance or not of surveillance technologies.

4.4.1 New technologies: Public understanding and engagement

This report has already noted some aspects of the key theoretical contributions of academic discourse on publics. This has come from work in defining more clearly the term as well as suggesting why public attitudes are central to acceptance or not of particular societal trends and developments. Much of this work on publics of relevance to this report is related to the topics of how publics engage, interact with and view scientific research, innovation and the

[844] See Monahan, Torin, (ed.), *Surveillance and security : technological politics and power in everyday life*, Routledge, New York, 2006.

[845] Pawson, Ray, "Theorizing the Interview", *The British Journal of Sociology*, Vol. 47, No. 2, June 1996, pp. 295-314.

development of new technologies.[846] One of the key contributions has been the observation that in the European (and elsewhere) context, there are a multitude of publics, with divergent views, opinions and attitudes towards science, innovation and new technologies. Theoretical work has been specifically strong in highlighting public attitudes to those technologies that might be considered controversial or with strong implications for citizens and societies.[847] This has focused on areas such as biotechnology, neuroscience, nanotechnology and new developments in information and communication technologies.[848] Increasingly, technologies associated with surveillance (and smart surveillance), such as body scanners, are generating controversy. Academic discourse can help policy-makers understand and engage the public understanding (Why does the public – or some publics – oppose body scanners, but accept CCTV? Why are there national differences in acceptance of or opposition to some technologies?).

We have already identified some cases of public resistance and rejection in relation to some surveillance technologies in this report. Also of importance are issues related to the public understanding of the consequences or meanings of these technologies[849]. As noted earlier, surveillance technologies are often presented in a confusing manner to publics or the societal implications of such technologies are not set out clearly or are understood even by those proposing implementations of these technologies or in the public's mind. As a result, the public understanding of some surveillance technologies at times can be said to be quite limited as a result of failures in communication and engagement between different actors, stakeholders and publics. A common complaint made in the academic discourse in relation to publics and technologies is that paternalistic campaigns serving merely to "educate and inform" the public of the benefits of technologies meet with limited success.[850] This has been a key debate between proponents of public engagement and those researching new technologies and working in science in criticising the deficit model of public understanding of science.

The deficit model (Public understanding of science)

European debates on science and technology over the last 30 years, since in particular the widespread public campaigns in relation to nuclear energy, have increasingly been cognisant of the role of public attitudes in determining societal interactions with technological innovations and scientific development. The traditional view, which much of this academic discourse sought to challenge, was the established deficit model. This saw public rejection or resistance to new scientific and technological developments solely as a result of a lack of understanding or knowledge about these scientific and technological developments and the benefits to society and citizens associated with them. Moving beyond the deficit model saw the introduction and research of conceptions of public engagement.

---

[846] Holliman, Richard, [ed.], *Science communication in the Information Age: Implications for Public Engagement and Popular Media*, Oxford University Press, Oxford, 2009.

[847] Pytlikzillig, Lisa M., and Alan J. Tomkins, "Public engagement for informing science and technology policy: What do we know, what do we need to know, how do we get there?", *Review of Policy Research*, Vol. 28, Issue 2, March 2011, pp. 197-217.

[848] In relation to biotechnology, see Horlick-Jones, Tom, *The GM debate: risk, politics and public engagement*, London, Routledge, 2007.

[849] Marx, Gary T., "A Tack in the Shoe: Neutralizing and Resisting the New Surveillance", *Journal of Social Issues*, Vol. 59, No. 2, 2003, pp. 369-390.

[850] Wilsdon, James, and Rebecca Willis, *See through science: Why public engagement needs to move upstream*, Demos, London, 2004. http://www.demos.co.uk/files/Seethroughsciencefinal.pdf

This work on public engagement has sought to develop mechanisms on how publics can be involved in the research process, especially where strong negative views on certain scientific and technological developments are expressed. This has been an important theoretical and empirical development in how some sciences and technological research has been conducted and governed.[851] It has, for example, been a cornerstone of theoretical and empirical work in European social sciences in relation to new scientific development and technological innovations.[852] So successful has some of this been that in examining European funded research, the call for the public to be engaged or involved with the research and innovation process has been a critical development. This has shaped how European science and technological innovation is conducted and performed through mechanisms of public engagement in science and technology policy.[853] This deliberative and participatory approach has led arguably to a democratising of science and technology policy.

Applying these theoretical developments to surveillance technologies, especially new, controversial technologies, has also taken place, as evidenced by the European projects discussed in this report. One critical difficulty in implementing this approach, however, has been the closed settings in which policy decisions on surveillance take place and as a result what technologies are implemented and deployed. For example, citing decisions as being in the national interest (whether justifiable or not) means opening up such processes to public engagement or involvement difficult to achieve.[854] In detailing some specific examples of public resistance to implementations of new surveillance practices or technologies, our report demonstrates that the same resistance may continue to play out in terms of continued public rejection of and resistance to these developments. In following the arguments of academic discourse related to the public engagement, this resistance will continue unless new models of engagement are pursued. Continuing along a simplistic model of communication which seeks only to educate and inform the public of the benefits will prove as limited in the context of surveillance as it has in other areas of technological development and implementation.

4.4.2 Surveillance societies, theories of modern and post-modern governance

A strong element of some theoretical writing on surveillance is the observation that modern states are surveillance societies.[855] Within this theoretical framework, surveillance often can be conceived in the broadest possible sense and includes practices in the public and private sectors. Surveillance covers low tech solutions as well as emerging high tech solutions, of which smart surveillance technologies is one. In this strand of academic discourse, surveillance is also a potentially positive as well as negative force in modern societies, for example, where surveillance regimes are developed in the context of health-care they are

[851] Kurath, Monika, and Priska Gisler, "Informing, involving or engaging: Science communication in the ages of atom, bio- and nanotechnology", *Public Understanding of Science*, Vol. 18, No. 5, September 2009, pp. 559-573.

[852] Nesserini, Federico, and Massimiano Bucchi, "Which indicators for the new public engagement activities? An exploratory study of European research institutions", *Public Understanding of Science*, Vol. 20, No. 1, January 2011, pp. 64-79.

[853] Wilsdon and Willis, op. cit., 2004.

[854] Davis, Darren W., and Brian D. Silver, "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America", *American Journal of Political Science*, Vol. 48, No. 1, 2004, pp. 28-46.

[855] For an excellent historical discussion on the emergence of surveillance societies, see Higgs, Edward, "The rise of the information state: the development of central state surveillance of the citizen in England, 1500-2000", *The Journal of Historical Sociology*, Vol. 14, No. 2, 2001.

often viewed positively by the public.[856] Surveillance in these academic discourses is explained in relation to how states govern, how states interact with citizens and how state and non-state actors interact with each other and with citizens.[857] Public acceptance of surveillance practices and technologies within these discourses are intrinsically and extrinsically related to the factors and elements in how modern, or post-modern, states seek to govern their citizens and non-citizens.

Surveillance and governance

Lyon argues that all modern societies are surveillance societies, that indeed one is not possible without the other.[858] Furthermore, Lyon and others who follow this theoretical argument suggest that citizens are both used to and reliant on surveillance practices in order to participate and avail themselves of services in modern societies.[859] For example, access to welfare is dependent on information being held by the state on citizens and, more than this, the ability of the state to effectively and fairly administer welfare services is dependent on its ability to gather and use this information. One conclusion from this line of reasoning is that most citizens are used to and may even expect a certain level of surveillance in participating in modern society. However, in the modern context, the terrorist attacks of 9/11 are seen as marking a significant shift in the language of security and surveillance and the role of technology in protecting society and the public.[860]

Others, countering the notion that surveillance is a necessity, argue that, while a certain level is expected, the thresholds of what constitutes acceptable levels of surveillance are either breached by different actors or not explicitly defined for actors and institutions to follow.[861] Academic discourse in this regard is often shaped and informed by considering privacy and how trade-offs between it and, for example, security are debated in policy settings. Linked to the notion of surveillance practices being integral to the operations of modern states are academic theoretical frameworks that see surveillance as a means by which social control and social sorting are achieved.[862] While this is often a function of how surveillance is a governance mechanism for modern states, it is also a strong source for identifying how particular citizens or non-citizens disproportionately bear the burden of increased surveillance and increased interactions with technologies of surveillance compared to those who control these technologies.[863] This strand of thinking seeks to explain findings indicating that citizens may accept technologies and surveillance where it is clear, or promoted, that the technologies or surveillance practices are not targeting them, but are directed towards "threatening" others.

---

[856] Barrett, Geraldine, Jackie A. Cassell, Janet L. Peacock and Michel P. Coleman, "National survey of British public's views on use of identifiable medical data by the National Cancer Registry", *BMJ: British Medical Journal*, Vol. 332, Issue 7549, 5 June 2006, pp. 1068-1070.

[857] Wright, Barry, "Quiescent Leviathan? Citizenship and National Security Measures in Late Modernity", *Journal of Law and Society*, Vol. 25, No. 2, June 1998, pp. 213-236.

[858] Lyon, David, *Surveillance Society: Monitoring Everyday Life,* Open University Press, Buckingham, 2001.

[859] Ibid., pp. 1-5.

[860] Lyon, David, "Technology vs 'Terrorism': Circuits of City Surveillance since September 11th", *International Journal of Urban & Regional Research*, Vol. 27, No. 3, 2003, pp. 666-678.

[861] Levi, Michael, and David S. Wall, "Technologies, Security, and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society*, Vol. 31, No. 2, 2004, pp. 194-220.

[862] Lyon, David, (ed.), *Surveillance as Social Sorting*, Routledge, New York, 2003.

[863] Bunyan, Tony, "Just over the horizon – the surveillance society and the state in the EU", *Race and Class*, Vol. 51 No. 3, 2011, pp. 1-13. –

A key feature of academic discourse drawing on this theoretical framework is the notion that particular groups of individuals suffer disproportionately from surveillance practices and the use of technologies.[864] In this sense, traditional social patterns of inequality become overlaid with technological surveillance interventions and regimes. While some theoretical frameworks are somewhat ambivalent as to the negative aspects and implications of an expanded surveillance within modern states, there is a considerable body of academic literature that sees this trend in modern states as an essentially problematic and negative development associated with trends and specific events in the 20th and 21st centuries.[865] Agamben, for example, argues that the "war on terror" has essentially created a constant state of emergency where rights, freedoms and democratic principles are continually being sacrificed in order to protect citizens and achieve victory, a worrisome position given the difficulties in achieving victory in a war where the enemy is so vaguely defined.[866] In terms of addressing factors determining public acceptance of surveillance, academic discourse reflecting this viewpoint sees the continual creation and reinforcement of a climate of fear and risk as one driving force in securing the support of European publics.

Another aspect of the academic discourse reflecting this theoretical framework is the notion that surveillance has emerged as one component of policies and strategies for how modern societies deal with the problems associated with modernity as well as being a requirement for some aspects of modernity such as commercial operations.[867] A further element to the theoretical underpinnings of academic discourse reflecting these arguments is that the balance of interests in terms of protecting democracy and citizens has shifted too far in the direction of security as opposed to liberty. Furthermore, policy discourse in some settings actively seeks to restrict liberties by promoting security over and above any other values in society.[868] In thinking about factors determining the public acceptance of surveillance, some of the arguments within these academic discourses provide rationales justifying surveillance.

4.4.3 Theories on the Information and Risk Society

While surveillance is an aspect of some theoretical understandings of the notion of the Information Society, the Information Society has a more relevant body of literature in terms of framings of the meanings of "smart". Academic discourse in relation to the Information Society centres on the profound changes in modern societies as a result of technological developments for the most part associated with ICTs.[869] The divides within theories is often as to whether the Information Society represents a "new" type of society or is merely a continuation of the Industrial Society. Its relevance to the topic of this report lies in the attitudes towards technological development and the experiences of novel technological developments and implementations.

---

[864] O'Donnell, Aisling T., Jolanda Jetten and Michelle K. Ryan, "Who is watching over you? The role of shared identity in perceptions of surveillance", *European Journal of Social Psychology*, Vol. 40, Issue 1, Feb 2010, pp. 135-147.

[865] See, for example, Samatas, Minas, "Studying Surveillance in Greece: Methodological and Other Problems Related to an Authoritarian Surveillance Culture", *Surveillance & Society*, Vol. 3, No. 2/3, 2005, pp. 181-197.

[866] Agamben, Giorgio, *State of Exception*, University of Chicago Press, Chicago, 2005.

[867] Zwick, D., and J. Knott, "Manufacturing customers: the database as a new means of production", *Journal of Consumer Culture*, Vol. 9, No. 2, pp. 221-247.

[868] Kossowska, M., M. Trejtowicz, S. de Lemus et al., "Relationships between right-wing authoritarianism, terrorism threat, and attitudes towards restrictions of civil rights: A comparison among four European countries", *British Journal of Psychology*, Vol. 102, No. 2, 2011, pp. 245-259.

[869] For an excellent overview of different theoretical frameworks on the Information Society, see Webster, Frank, *Theories of the Information Society*, Routledge, London, 1995.

A key feature of academic discourse in relation to the emergence of the Information Society is the notion that time and space are increasingly compressed, leading to a 24/7/365 society and one where the local is global and vice versa.[870] The infrastructure allowing this to happen is, of course, ICTs and as the networks and our societies become ever more complex, the reliance on technology to enable this grows. Continued developments in ICTs, or at least one potential trajectory mapped out for future developments by the SAPIENT project, is the development of increasingly smart devices and possibly autonomous machines, devices and networks. The potential surveillance aspects of these technologies are pervasive, problematic and, as of yet, little understood in terms of the potential implications for society. Their close association with other aspects of a digital life has led some to conclude that their uptake will be greater with individuals paying less concern to the negative aspects such as how these impact on privacy.[871]

Developed in the main in the writings of Ulrich Beck, the notion of the risk society offers a different perspective on the role of surveillance and (post-) modern national states.[872] Being able to manage risks is a critical function of the post-modern state, and for Beck and others reflexive modernity dominates political thinking in the sense that post-modern societies are often preoccupied with dealing with the problems which modernity has caused.
As with our discussion on the notion of surveillance as social sorting, those following the arguments made by Beck argue, as he does, that post-modern nation states are characterised by an unequal distribution of risks.[873] The management of some of these risks through surveillance is an important mechanism of governance, one which also shapes public debates on policy.

Furthermore, the observation that these technologies themselves create risks for society, for example, through restrictions on liberty and other freedoms, is endemic of reflexive modernity. In relation to factors determining the public acceptance of surveillance, this discourse offers a number of insights. A key one would be the perception of risk and how this influences public acceptance. For example, in the UK, crime and related surveys continue to show a mismatch between the perception of crime and the actual probability of being a victim of crime.

4.4.4 Engaging the social sciences

Seeking to engage and involve the public in science and technology discourse has been one strand of a potential democratising of science and technology policy. Another element of this process has been the involvement and engagement between science and technology discourse within disciplines of the social sciences such as law and ethics. Ethical academic discourse has extensively discussed the societal implications of different technological developments (bioethics for the life sciences, neuro-ethics, nano-ethics). Various authors have written about the ethical implications of new and current technologies of surveillance as well as the practice of surveillance itself.[874] Ethical, legal and social aspects or implications (ELSA/ELSI) studies

[870] Castells, Manuel, *The Rise of the Network Society*, Blackwell, Oxford, 1996/2000.

[871] Levi, Michael, and David S. Wall, "Technologies, Security, and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society*, Vol. 31, No. 2, 2004, pp. 194-220.

[872] Beck, Ulirch, *Risk Society: Towards a new modernity*, Sage, London, 1992.

[873] With the caveat that some risks, such as environmental ones, can at times ignore traditional class divisions associated with, for example, Marxist analyses of society.

[874] For a synopsis, see Williams, R., M. Barr and E. Haimes, "The bioethics of security" [editorial, Special Issue], *Bioethics*, Vol. 22, Issue 9, November 2008, pp. ii-iii.

have become synonymous with some approaches aiming to examine the implications of new scientific research and new technologies. These approaches have already been applied as well to some surveillance technologies and projects such as the EU-funded BITE project discussed in this report. With origins in performing this task in the life sciences, such studies have quickly expanded in terms of usage in other areas and for other technologies. This form of research is often incorporated into scientific and innovative research processes to provide oversight and deal with concerns that are highlighted as being potentially problematic ones for society. The classic and first large-scale undertaking reflecting this trend was the incorporation and funding of ELSA research during the Human Genome Project.[875]

The spread of ELSA beyond the concerns expressed in relation to biotechnology can be seen at Member State level and within European funded research as well as internationally as a way of addressing public and policy concerns. The institutionalised approaches to ELSA has attracted some criticism[876] within research funded solely as social science and within science research with a funded component dedicated to examining the ELSA issues. One criticism of the ELSA approach has been that ethical and legal aspects have predominated in the research and findings of studies. Reasons for this are complex and multifaceted, but one argument made by other social scientific disciplines is that ethics and law have been central to ELSA research becoming institutionalised in the decision-making and policy process.[877] Reasons given for this include the notion that ethics and legal approaches are perceived as giving easy answers which policy makers can utilise (i.e., ethical or not, legal or not). That this is a simplistic perception and one which damages and does disservice to ethical and legal research was and is recognised by ELSA advocates and critics. One result of attempting to engage with social aspects has been a trend towards incorporating stakeholders (publics) into the ELSA research process – giving stakeholders an opportunity to express their views. As publics have been redefined, so have their possible inclusion and engagement with research and innovation decisions.

One recent development in terms of theoretical understandings of relevance to citizens, societies, technologies and related trends has been the emergence of the design turn in ethics and technological innovation and development. Simply put, the design turn in ethics and technology captures recent trends and developments whereby ethical, legal, social or cultural norms are embedded within technologies in terms of being systems, devices, networks or infrastructural networks. One example of this would be privacy enhancing technologies and other systems which seek to embed privacy and data protection concerns within systems, devices and so on.[878] Arguments that can be derived from this are also important in how surveillance technologies are promoted, in the sense that new threats spur the development of new technologies to deal with these threats. In the private sector, these threats are often seen as a result of the previous introduction of new technologies. One can see Google's new social network (Google+) in this light – it has much better privacy controls than the oft-criticised Facebook.

---

[875] Juengst, E.T., "Self-critical federal science? The ethics experiment within the US Human Genome Project", *Social Philosophy and Policy*, Vol. 3, No.2, July 1996.

[876] Yesley, Michael, "What's ELSI got to do with it? Bioethics and the Human Genome Project", *New Genetics and Society*, Vol. 27, No. 1, March 2008, pp. 1-6.

[877] Hedgecoe, A., "Bioethics and the reinforcement of socio-technical expectations", *Social Studies of Science*, Vol. 40, No. 2, April 2010, pp. 163-171

[878] Philips, David J., "Privacy policy and PETs: The influence of policy regimes on the development and social implications of privacy enhancing technologies", *New Media and Society*, Vol. 6, No. 6, December 2004, pp. 691-706.

Privacy and data protection

Academic discourse on the subject of privacy and data protection in the European and US contexts is a particularly strong normative theoretical framework with a bearing on public acceptance or not of smart surveillance and associated technologies and practices. As discussed above, a key theoretical debate within academic discourse exploring issues of privacy and data protection is a consideration of the balance of interests between surveillance, security, privacy and data protection for citizens. Of particular importance in the European context has been the framing of privacy as a fundamental right.

4.4.5 Theoretical insights dealing with public acceptance

The main points that emerge as being of relevance to an understanding of public acceptance from a consideration of these theoretical positions in the academic discourse are

- the relationship between publics and surveillance, in terms of both technologies that are used and institutions or structures implementing and controlling surveillance;
- the relationship between surveillance and modern societies;
- the relationship between citizens, publics and modern societies;
- the risks and threats facing modern societies and citizens and responses to these.

At times, there is some overlap between how certain theoretical viewpoints deal with these themes. Each of the theoretical frameworks sees interactions between these elements and themes as critical to understanding public acceptance (or lack thereof) of surveillance, as a practice and as individual technologies.

The four key academic discourses highlighted here reflect different theoretical positions with a wide range of explanations or arguments concerning the relationship between surveillance, societies and citizens in Europe. Some of these theoretical viewpoints have directly informed a substantial amount of empirical research, or have drawn on empirical research to justify particular theoretical claims.

With such a divergent range of viewpoints and claims in relation to surveillance, citizens and societies, it is unsurprising that some of the theoretical frameworks presented here disagree with one another on key points and claims vis-à-vis these issues. This report has already illustrated the difficulty in making any definitive claims about public acceptance or not of surveillance technologies. It is similarly difficult to draw definitive conclusions as to which theoretical framings and which elements of academic discourse present the best explanation as to the findings of surveys or the deeper reasons for these findings as a result of how citizens engage with surveillance practices and technologies.

Bearing these viewpoints and theoretical positions in mind is nevertheless helpful in identifying robust analytical and explanatory frameworks for examining the key issues that emerge in surveys and research exploring public acceptance of smart surveillance technologies. Understanding these theoretical framings is critical and vital in fully understanding how research is shaped by theoretical preconceptions or considerations. This allows a much more nuanced appraisal of empirical research such as the opinion surveys examined in this report.

5 Discourses and politics of security and surveillance, privacy and data protection

Julien Jeandesboz, Didier Bigo, Mervyn Frost (KCL)

5.1 INTRODUCTION

This chapter supplements the research efforts presented so far by providing elements for a sociological analysis of smart surveillance. Our purpose here is twofold. It is, firstly, to examine how smart surveillance has become a pertinent item in the EU's security policies. Insofar as the "object" of smart surveillance is sustained by references to the importance of advanced or sophisticated technologies, we take EU efforts in supporting research and development for technologies in the field of security as a starting, "local" point of investigation. We focus on the assembling of security and technology, on the different operations of translation that have assembled security technologies as a relevant object for policy, research and scholarship. At stake here is the understanding of the functional narrative that frames "advanced" technology as a natural response to contemporary insecurities. If translation involves displacement, the hypothesis is that the assembling of security and technology does not so much mirror threats as it shifts the way in which specific developments are constituted as threats, as well as prescriptions regarding how these developments should be dealt with.

The purpose is to offer through this investigation some reflections on the relation between smart surveillance, fundamental freedoms and rights. We analyse in this regard how discourses and controversies that constitute smart surveillance as a policy object do not just involve discussions over the technical parameters of technological systems, but also problematise the relationship between security and surveillance, on the one hand, and fundamental rights and freedom, including data protection and privacy, on the other. They articulate, in other words, judgements on the relationship between security and freedom.

The chapter is structured as follows:

- Section 5.2 briefly introduces the empirical focus of the chapter and the analytical framework adopted.
- Section 5.3 examines the assembling of security and technology in the framework of the EU's security research and development programme.
- Section 5.4 builds on this examination to outline the contemporary controversies over security and surveillance unfolding in the European governmental arenas.
- The conclusions of the chapter discuss how these findings inform the reflection on smart surveillance.

5.2 EMPIRICAL AND ANALYTICAL PARAMETERS

This section presents the main parameters of the research undertaken in this chapter, focusing in turn on:

- Empirical focus (5.21.): as introduced previously, the work will concentrate here on the EU's security research and development activities, mainly through the FP7 Security Theme.
- Analytical framework (5.2.2.): as indicated in the introduction to this deliverable as well as in the DoW of the SAPIENT project, the chapter adopts a sociological perspective, drawing more specifically from so-called ANT approaches. The subsection presents the key tenets and methodological requirements of these perspectives.
- Argument (5.2.3.): in this subsection we link the empirical focus and analytical framework to examine the relevance of this chapter to the overall objectives of SAPIENT.

5.2.1 Empirical focus

The main point of entry for the analysis, here, will be EU activities in the field of security and technology, and particularly security research and development activities. There are several reasons for this choice. Firstly, technology is increasingly singled out as a core component of the EU's security policies. This trend has been singled out by a growing number of inquiries (see among other the results of the CHALLENGE and INEX projects). It is also confirmed by a number of recent policy developments, particularly in the context of the EU's area of freedom, security and justice (AFSJ). The Stockholm Programme, adopted in December 2009 considers technological instruments as essential "tools for the job" of protecting European citizens.[879] Information and communication technologies have been an object of special concern in this regard, with the adoption of the EU's Information Management Strategy[880] and the ongoing discussions on the establishment of a European agency for the operational management of large-scale IT systems. The EU's security research programme is a key nexus in the drive towards technology-oriented security policies, and has been used as a support for a number of surveillance projects related to EU security policies, as highlighted in the previous chapter. One example is the European border surveillance system (EUROSUR), which was formally launched with the Commission's 2008 "border package" communications and whose development has been sustained in part by research and development projects funded under the FP7 Security Theme, such as the R&D Demonstration programme on European-wide integrated border control system, the GLOBE, OPERAMAR and SECTRONIC projects among others.

Of relevance for the specific goals of SAPIENT, secondly, is the updating of the data protection framework (DPF) currently under consideration, and the Commission's proposal for "a comprehensive approach on data protection".[881] Should the Commission's position prevail, the DPF would do away with the existing limitations in the EU's data protection regime, and the tensions between the general data protection framework established in Directive 95/46/EC (the Data Protection Directive) and the provisions applicable to so-called

[879] Council of the European Union, "The Stockholm Programme - an Open and Secure Europe Serving and Protecting Citizens," (Brussels: 5731/10, 2010), 65-67.

[880] Council of the European Union, "Draft Council Conclusions on an Information Management Strategy for EU Internal Security," (Brussels: 16637/09, 2009).

[881] European Commission, "A Comprehensive Approach on Personal Data Protection in the European Union," (Brussels: COM(2010) 609, 2010).

third pillar, police and judicial cooperation activities established in Framework Directive 2008/977/JHA.[882] The updating of the DPF takes place in a context defined by a recent opinion of the Article 29 Working Party (WP29) as one of "data deluge" in security-related activities,[883] whereby data processing schemes are multiplying in a seemingly haphazard pattern. The prescriptions contained in current EU strategic documents in the field of internal security suggest that this trend is likely to continue: the recently adopted European Internal Security Strategy, for example, advocates a "European Security Model" that would be based on a "proactive and intelligence-led approach".[884] Focusing on EU security research, here, will provide strong and updated backing to the devising of innovative privacy impact assessment methods by SAPIENT.

5.2.2 Analytical framework

A few words are needed on the approach adopted in the following pages and on the possible differences of tone with the other perspectives adopted so far in the deliverable. What does it mean to study technology from a sociological perspective? The question has generated a dedicated literature, structured since the mid-1980s and the "turn to technology" of a number of scholars interested in the social study of scientific knowledge,[885] into the field of science and technology studies (STS). We cannot do justice to the full extent of this shift and the debates that it has spurred in the space imparted here, though we can detail at some length the particular elements of this scholarship which we call upon. A key feature of these debates has been the treatment of technology as an "object" by tenants of the constructivist variant of STS - sometimes dubbed "SCOT" (social construction of technology).[886] SCOT approaches emphasise that artefacts constitute the support for different interpretations by different social groups of their meaning and function. These interpretations and the groups that hold them should constitute the starting point of the sociology of technology. Socially constructed interpretations, it is argued, generate the identification of differentiated sets of problems and solutions for the design of further technical systems. Over time, and depending on the outcome of controversies and struggles among the different social groups associated with a technology, this open-endedness of technological design comes to a closure: artefacts are "stabilised" in a specific social meaning and function. The analysis thus proceeds by relating "the content of a technological artefact to the wider sociopolitical milieu" within which meanings are constructed and attributed.[887]

The explanatory power attributed to the "wider [sociolpolitical] context" (the macro-social scale) onto specific social formations (the micro-social scale), however, has been met by strong criticisms by a number of scholars advocating for an approach alternatively labelled as

---

[882] Paul De Hert and Vagelis Papakonstantinou, "The Data Protection Decision of 27 November 2008 Regarding Police and Judicial Cooperation in Criminal Matters - a Modest Achievement However Not the Improvement Some Have Hoped For," *Computer Law & Security Review* 25, no. 5 (2009).

[883] Article 29 Working Party, "Opinion on the Principle of Accountablity," (Brussels: 3/2010, 2010).

[884] Council of the European Union, "Draft Internal Security Strategy for the European Union: Towards a European Security Model," (Brussels: 5842/2/10, 2010).

[885] Steve Woolgar, "The Turn to Technology in Social Studies of Science," *Science, Technology & Human Values* 16, no. 1 (1991).

[886] Cf. Wiebe E. Bijker, Thomas P. Hughes, and Trevor J. Pinch, eds., *The Social Construction of Technological Systems* (Cambridge: The MIT Press,1987); Trevor J. Pinch and Wiebe E. Bijker, "The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other," *Social Studies of Science* 14, no. 3 (1984).

[887] Pinch and Bijker, "The Social Construction of Facts and Artefacts: Or How the Sociology of Science and the Sociology of Technology Might Benefit Each Other," 428.

the "sociology of translation", "sociology of associations" or "actor-network theory".[888] Tenants of the "sociology of the social", to borrow from one of the best-known contributors to this strand of research, "have simply confused what they should explain with the explanation. They begin with society or other social aggregates, whereas one should end with them. They believed the social to be made essentially of social ties, whereas associations are made of ties which are themselves non-social […] They believed the social to be always already there at their disposal, whereas the social is not a type of things either visible or to be postulated".[889] The task of sociology is not to posit the existence of the social, but to "reassemble" it, to investigate the ways in which it is formed, without making any assumptions about its boundaries.

Here lies a second point of contention between ANT and other strands of the sociology of technology. The SCOT perspective, for example, takes for granted the technical nature of technology, i.e. the boundary between the technical and the social. Artefacts do not participate in the social, they are an embodiment of the meanings bestowed upon them by different social groups. For ANT approaches, by contrast, the boundary between the technical and the social is not a given, but a question to be investigated. They consider, rather, that "objects are an effect of stable arrays or networks of relations".[890] A famous example of how this approach develops a sociological analysis of technology is the case of the vessels used by the Portuguese in the early expansion of European colonial empires.[891] As a maritime technology, "a vessel can be imagined as a network: hull, spars, sails, ropes, guns, food stores, sleeping quarters and crew. In more details, the navigational system - ephemerides, astrolabe or quadrant, slates for calculation, charts, navigators and stars".[892] Networks are thus composed not only of people, but also of non-human actors ("actant") such as machines, animals, or texts. They are heterogeneous assemblages, where the relations between human agents cannot be assumed to have ontological precedence. Such relations are indeed constantly mediated, shaped by other networks: "[a]t any rate, our communication with one another is mediated by a network of objects - the computer, the paper, the printing press. And it is also mediated by networks of objects-and-people, such as the postal system".[893]

ANT approaches raise a third point of contention, which originates in the initial focus of this scholarship on scientific controversies. The contention involves the relation between the micro- and the macro-social and the issue of power. ANT perspectives are based on three main methodological tenets.[894] Free association, which has been discussed above, establishes that the observer must abandon pre-given distinctions between natural or technical and social or political events. Generalised agnosticism, secondly, requires scientific impartiality towards the arguments used by protagonists in a given controversy: all interpretations are taken into

---

[888] Michel Callon, "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay," in *Power, Action and Belief: A New Sociology of Knowledge?*, ed. John Law (London: Routledge, 1986); Bruno Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory* (Oxford: Oxford University Press2005); John Law, "Notes on the Theory of the Actor-Network: Ordering, Strategy and Heterogeneity," *Systemic Practice and Action Research* 5, no. 4 (1992).

[889] Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory*, 8.

[890] John Law, "Objects and Spaces," *Theory, Culture & Society* 19, no. 5-6 (2002): 91.

[891] John Law, "On the Methods of Long Distance Control: Vessels, Navigation, and the Portuguese Route to India," in *Power, Action and Belief: A New Sociology of Knowledge?*, ed. John Law (London: Routledge, 1986); Law, "Objects and Spaces."

[892] Law, "Objects and Spaces," 93.

[893] Law, "Notes on the Theory of the Actor-Network: Ordering, Strategy and Heterogeneity," 383.

[894] Callon, "Some Elements of a Sociology of Translation: Domestication of the Scallops and the Fishermen of St Brieuc Bay," 196-97.

account, and no standpoint is censored. Generalised symmetry, finally, entails that sociologists should use a single analytical repertoire when considering the technical and the social side of a problem. Agnosticism and symmetry, then, lead to consider how the forming of associations in a specific (local) framework can have effects at different levels of scale. The most salient example provided by the ANT literature is the laboratory, more specifically that of Pasteur.[895] Laboratories are key locations where different entities and materials are associated and where large-scale effects can be generated by means of what ANT approaches term translation, "in which actors (including collectivities) struggle to impose versions of reality on others which define (a) the number of those others, both natural and social, that may be said to exist in the world, (b) their characteristics, (c) the nature of their interrelations, (d) their respective sizes and (e) their positions with respect to the actor attempting the translation. Since there are many such actors and many different versions of reality, this process is invariably uncertain and reversible, even when rewarded with success".[896] The laboratory of Pasteur was for example the location where an association between different methods of scientific investigations, types of equipment and entities (Pasteur and his laboratory employees, the anthrax bacillus) formed and subsequently influenced the network of farmers, public officials, veterinarians and laboratories.

Translation is central in ANT reasoning because it underpins the linkage between different scales of analysis as well as between the social, the natural and or the technical. It also conveys the idea of uncertainty: "Translation does not mean a shift from one vocabulary to another, from one French word to one English word, for instance, as if the two languages existed independently […] I use *translation* to mean displacement, drift, invention, mediation, the creation of a link that did not exist before and that to some degree modifies two elements or agents".[897] One effect of translation, which is of particular interest to us here, is "black-boxing", namely the simplification and closure of an otherwise intricate network - for example, when an assemblage of circuitries and the relations between them becomes a "computer". The outcome of translation, however, is never predetermined (e.g. there is no telling what will be black-boxed) and will depend, among other parameters, on the durability of the associations forged through translation, and of the mobility of the translated elements beyond a given local setting (e.g. the publication of results obtained in a laboratory in a scientific journal, and the use in this publication of tactics and materials such as graphs or mathematical formula to enroll other actors in the association). Two additional specifications are required here. Firstly, translation involves spokepersons who by means of different techniques manage to speak on behalf of other agents. Through laboratory work, Pasteur for instance became the spokeperson of the anthrax bacillus and of specific methods for vaccination and sterilisation. Translation, additionally, can result in effects of social control and power beyond a given local context (long-distance control). ANT approaches consider that these effects are the outcome, rather than the cause, of specific associations . As an amendment, however, one can highlight that such effects are retroactive: they can contribute to the consolidation of an otherwise unsteady association, or support the assembling of new associations.

---

[895] Bruno Latour and Steve Woolgar, *Laboratory Life: The Construction of Scientific Facts* (Princeton: Princeton University Press, [1979] 1986); Bruno Latour, "Give Me a Laboratory and I Will Raise the World," in *Science Observed: Perspectives on the Social Study of Science*, ed. Karin D. Knorr-Cetina and Michael Mulkay (London: Sage, 1983).

[896] John Law, "On Power and Its Tactics: A View from the Sociology of Science," *The Sociological Review* 34, no. 1 (1986): 6.

[897] Bruno Latour, "On Technical Mediation - Philosophy, Sociology, Genealogy," *Common Knowledge* 3, no. 2 (1994): 32.

Concerns with social control and power also provide a useful connection between ANT approaches and other perspectives in the field of sociology which have been mobilised in different research efforts related to the issues examined here.[898] The concept of "actant" and its analytical underpinnings, namely the active involvement of non-human interveners in the assembling of the social, is clearly original with regard to the vast majority of sociological investigations. There are nonetheless strong ties between the emphasis on networks and the focus of Bourdieusian sociology on the notion of fields, for instance, where "actants" are partially brought in (albeit in a much less active outlook) through the study of capitals and habitus. Translation and the appointment of spokespersons, in a similar fashion, recall the attention dedicated by field approaches to the issue of multi-positionality[899] as well as to Bourdieu's propositions on the political field.[900] The importance attached to the notions of heterogeneity and indeterminacy of social processes in ANT approaches also find an echo in the Bourdieusian method of the "reconstruction of the genesis" which, "by bringing back into view the conflicts and confrontations of the early beginnings and therefore all the discarded possibles […] retrieves the possibility that things could have been (and still could be) different […] [a]nd, through a practical utopia, […] questions the "possible" which, among all others, was actualized".[901] The notion of "control at a distance", similarly, has been mobilised by studies drawing on the notion of "governmentality" developed by Michel Foucault.[902]

5.2.3 Argument

How do these considerations relate to SAPIENT's preoccupations? As we will see, current efforts in the security research and development programmes sponsored by the EU are framed in reference to efficiency and enhancement. The stated aim is to improve technology, to make it more efficient in countering purported threats. If we take seriously the proposals of ANT approaches, however, the correlation between technology, improvement and efficiency is only a specific translation resulting from the association of different elements - financial resources, artefacts, researchers and so forth. The notion that certain developments are threatening, in addition, should also be considered in terms of translation. Although there is limited pertinence in developing a full theoretical discussion here, this observation relates ANT approaches to the insights of "critical approaches to security"[903] that have analysed the performativity of security practices, knowledge and techniques for the definition of threats, dangers and risks and studied security as heterogeneous processes of (in)securitisation.[904] At stake here is the understanding of the functional narrative which frames "advanced" technology as a natural response to contemporary insecurities. If translation involves displacement, the hypothesis is that the assembling of security and technology does not so much mirror threats as it shifts the way in which specific developments are constituted as threats, as well as prescriptions regarding how these developments should be dealt with.

---

[898] Refer, again, to the results of the ELISE (FP5), CHALLENGE (FP6) and INEX (FP7) research projects.

[899] Luc Boltanski, "L'espace Positionnel: Multiplicité Des Positions Institutionnelles Et Habitus De Classe," *Revue française de sociologie* 14, no. 1 (1973).

[900] Pierre Bourdieu, *Propos Sur Le Champ Politique* (Lyon: Presses universitaires de Lyon, 2000).

[901] Pierre Bourdieu, "Rethinking the State: Genesis and Structure of the Bureaucratic Field," *Sociological Theory* 12, no. 1 (1994): 4.

[902] See above Section 1.1. Cf. also: Mitchell Dean, *Governmentality: Power and Rule in Modern Society* (London: SAGE1999); Peter Miller, Rose, Nikolas, "Governing Economic Life," *Economy and Society* 19, no. 1 (1990); Nikolas Rose and Peter Miller, "Political Power Beyond the State: Problematics of Government," *The British Journal of Sociology* 43, no. 2 (1992).

[903] c.a.s.e. collective, "Critical Approaches to Security in Europe," *Security dialogue* 37, no. 4 (2007).

[904] Thierry Balzacq et al., "Security Practices," *The International Studies Encyclopedia* (2010); Jef Huysmans, *The Politics of Insecurity: Fear, Migration and Asylum in the EU* (London: Routledge, 2006).

Insofar as translation is an uncertain endeavour, security research and development should also be regarded as a contested operation, which remains open to controversies. This, in turn, aligns the reflection we want to conduct here with the insights of surveillance studies regarding the "Orwellian" logic of surveillance. As an analytical tool, ANT thus enables us to unfold these controversies, to remain "agnostic" towards specific narratives and consider the various attempts at translation that contribute to shape the object of security research rather than privileging a "functional account" according to which technologies are developed in response to threats. As we will show in the following pages, the assembling of security and technology in the EU framework operates as much, if not more, in relation to industrial and commercial preoccupations, as in relation to security considerations.

A second element here involves the "social" dimension of technological discussions. The methodological principles of generalised agnosticism and symmetry have been designed to take into account the social dimension of scientific controversies, i.e. the fact that agents, as "full-blown reflexive and skillful metaphysicians, […] also have their own meta-theory about how agency acts".[905] Agents have theories about the social and operations of translation involve a take upon the social. Controversies about security research and development are not only about the best, most sophisticated and/or most efficient technology: they are also about what makes a specific technology necessary/desirable for society, what its effects should be and ultimately how it should contribute to the shaping of the social (or how the boundary between the technical and the social should be negotiated). ANT thus provides us with the analytical tools to examine the association between discussions about the technical and the sociopolitical dimension of security and surveillance, or about the ethics of developing and relying on, specific technologies.

A third contribution that is probably more diffuse at this stage involves the way in which SAPIENT itself can be considered as a specific operation of translation. "Smart surveillance" is a newcomer in discourses about security and surveillance in EU security policies. Explicit references to "smart" security techniques have only appeared recently in official EU documents. To the best of our knowledge, the roadmaps tabled by DG Home in 2010 concerning the "smart borders initiatives" are the first institutional endorsement of this notion. For a while, other terminologies such as "intelligent surveillance", or in the case of border controls, "intelligent borders" have been favoured both by security agencies, bodies and services, and by companies developing, promoting or selling such technologies. Besides the "smart borders" initiative, "smart surveillance" has in fact been translated into a research issue and a policy concern in the second FP7 Security Call to which the SAPIENT consortium has submitted an application. The enrolment of researchers constitutes, in this regard, one tactic through which "smart surveillance" is sustained as an object of concern for policy and scholarship. This is a significant ethical issue, particularly in relation to the objectives of SAPIENT regarding the development of privacy impact assessments.

5.3 ASSEMBLING SECURITY AND TECHNOLOGY

Research and development in security has become an increasingly high profile domain in EU policies over the past decade. In this section, we examine how the link between security and technology has been formed from previously distinct components and has been sustained over time, as well as the displacements that have taken place in the process. We focus, in other words, on the assembling of security and technology, on the different operations of translation

[905] Latour, *Reassembling the Social: An Introduction to Actor-Network-Theory*, 57.

that have assembled security technologies as a relevant object for policy, research and scholarship. We seek to take some distance with the narratives of scholars and practitioners that present the increasing reliance on technology in EU security policies as a functional outcome of a "new threat environment". The assembling of security and technology, we want to show, is hardly a mechanical response tied to the evaluation of threats. It is, rather, sustained by a multiplicity of operations, most of which as we will show have very little to do with an evaluation of the developments that might be considered as threatening. In particular, we emphasise in the following pages the role played by market and industrial concerns in the assembling of security and technology. The story in itself has been told a number of times, in official documents as well as in policy briefs and studies. What we want to stress here is the heterogeneity and controversiality of this assembling, of translation that have resulted in the "black-boxing" of a certain number of issues, including the actual technologies involved in the pursuit of security.

5.3.1 A starting point: envisaging the next steps in security research in the EU

An apt starting point for our analysis is the Commission's communication on *Security Research: The Next Steps*. The document was tabled in September 2004 by the directorate-general for the information society (DG INFSO). It is presented as a stocktaking exercise of the steps already taken in this area, and as a prospective exercise delineating the contours of future initiatives. It draws, on the one hand, on the conclusions from the report of the "Group of Personalities on Security Research" (GoP report) convened in October 2003 by commissioners Busquin (in charge of DG Research) and Liikanen (in charge of DG Entreprise and DG Information and Society). The GoP report, titled "Research for A Secure Europe" was presented in March 2004 to the President of the Commission, Romano Prodi.

The *Security Research* communication reflects several operations of translation:

- The first operation involves the portage of the GoP Report into the workings of the European governmental arenas. The communication excises the report's conclusions and executive summary and transforms them into annexes, for circulation to the Council and European Parliament. This is a routine bureaucratic operation that can be observed into a variety of policy domains. The outcome of an exercise in gathering experts, making them work together and reporting on their work is simplified, streamlined through the use of writing techniques such as the drafting of executive summaries and recommendations, for the purpose of broader circulation among non-experts. As the distance between the original content of the report (which, in itself, is the result of multiple similar operations of translation) and its summarised elements is increased, complexity is reduced and the process of reflecting upon security research in the EU is made more pliable to imperatives beyond the specific characteristics of the local setting where the report has been drafted.
- The second operation is the consolidation of a specific chronology to security research. The introduction to the communication thus correlates the issue of security research with a number of institutional milestones, including the conclusions of the Cologne European Council on "a competitive and dynamic industrial and defence base", the conclusions of the Lisbon European Council on the realisation of "a competitive knowledge-based society", the Barcelona European Council conclusions on the reinforcing of "research, development and innovative effort in the Union", the conclusions of the Thessaloniki European Council on "concrete steps in the field of defence", the 2003 European Security Strategy (ESS) on " A secure Europe in a better world", and the conclusions of the Brussels European Council (March 2004) which

adopted a "Declaration on Combating Terrorism". Again, here, the operation involved is simplification. Heterogeneous policy processes involving different sets of agents are brought together into a single sequence, and the controversies that opposed them are silenced.

- The third operation is the actual articulation of security and technology. Invoking the example of the March 2004 bombings in Madrid, the communication asserts that "[i]n addressing the new security challenges, technology plays a key role. The European potential to research, develop and deploy a wide range of security technologies exists. However, in facing the diversity of new threats, Europe needs to surmount current structural and functional deficiencies: reducing fragmentation and duplication of effort, increasing cooperation and achieving standardisation and interoperability" (p. 4).

Through these different operations, the communication points out to several "assembly lines" or assembly processes (insofar as assembling is hardly a linear development), which bring together security and technology and problematise this assembling. In the following subsection, we will examine in more details two of them. A number of elements brought up in the communication, firstly, have to do with market organisation (e.g. "fragmentation" and "duplication", "standardisation" or competition). The market is accordingly a key "actant" in the assembling of security and technology, but it is not only brought in as a space to be organised. The second assembly process at work here follows indeed from the reference to industry and the "industrial basis" for technology in the EU. As the communication recalls, the "Personalities" involved in the GoP report come from European governments, the academia but also the industry. The assembling of security and technology also brings into play the security and defence industry which populates the market. A third assembly process, which has already been dealt with at length in the available literature, involves the problematisation of some developments as "security challenges" (or securitisation in terms more familiar to the security and surveillance studies literature) and the increasingly central emphasis placed on technology in the programmatic instruments dealing with the development of the EU's security policies, as well as in the practices of security professionals.

5.3.2 Assembly process #1: reforming and organising the "defence-related" market

The first assembly process associating security and technology involves the figure of the market and its organisation. An analysis of the succession of official documents that led up to the 2004 communication on security research shows that the assembling of security and technology as a relevant policy item originates in attempts from the Commission's internal market and industry services at circumventing the clause initially laid down in Article 296 (initially Article 223) of the Treaty establishing the European Communities (TEC) on military equipments. The clause enabled a Member State to "take such measures as it considers necessary for the protection of the essential interests of its security which are connected with the production of or trade in arms, munitions and war material" (Article 296(2) TEC), effectively removing defence-related products from the obligations concerning the common, and later single, market.

The foreclosure of discussions regarding the extension of common/single market principles to the armaments sector was challenged in the mid-1990s, as reflected in two communications drafted by the Commission's Entreprise and Industry services. The first one, published in January 1996, enumerated the "challenges" faced by European companies in the field of

defence.[906] The second, tabled in November 1997, focused on developing a "European Union strategy on defence-related industry".[907] Both communications bracketed the negotiations on the Amsterdam treaty (signed on 2 October 1997) within the intergovernmental conference (IGC) convened in March 1996. While they made reference to the then-nascent European security and defence policy (ESDP, formally introduced with Amsterdam), both documents ruled out such "political consideration" as a pertinent basis for action. As argued in the 1996 communication, "although a global approach to this subject is clearly important, the establishment of a European security and defence identity is nevertheless a long-term process. On the other hand, the state of health of the defence-related industries is such that unless action is taken in time, there is a danger that whole sectors of the economy involved in defence-related activities could disappear, with further massive job losses, particularly considering the fiercer international competition".[908] The communication thus steered issues related to the armaments market away from "second pillar" considerations of foreign and defence policy, within which the possibilities of action attributed by the Treaties to the Commission's services are limited, to industrial and commercial matters, which fell within the EU's "first pillar". This is also conveyed by the way in which the armaments industry is re-labelled as the "defence-related industry", the underpinning assumption being that EU intervention in this sector would reach beyond the specific issues listed in Article 296 TEC.

The self-proclaimed "economic" perspective through which armaments and defence issues were approached by the Commission in the mid-1990s built on the notion that the key question to address was the "anachronistic fragmentation of the defence markets" between EU Member States, in the words of the 1996 communication. Market fragmentation was deemed to prevent industrial synergies and economies of scale, as well as mergers and joint ventures among companies in the sector. In the process, the communication embraced fully the view of the industry. The 1997 communication, which introduced an action plan for EU involvement, hence argued that "the process of restructuring and consolidating the European defence-related industry, which should be carried out on a European scale, cannot progress satisfactorily unless market barriers are lifted and a clear, reliable, political and institutional frame of reference is provided. The European Union must take the necessary steps to establish this regulatory framework".[909] A central element used to justify these measures, beyond the economic impact of the purported decline of European defence companies, was the perspective of increased transatlantic competition. As a subsequent communication on a defence equipment policy, tabled in March 2003, would argue, "[t]here is a danger that European industry could be reduced to the status of sub-supplier to prime US contractors, while the key know-how is reserved for US firms".[910] This latter concern also transpired in the analyses published in the second half of the 1990s by a number of European foreign policy, defence and security think tanks. Shortly before it was transferred to the EU, for example, the Paris-based Institute for Security Studies (ISS) published a special issue of its lead publication the *Chaillot Papers*, dedicated to the transatlantic defence market.[911] The

[906] European Commission, "The Challenges Facing the European Defence-Related Industry, a Contribution for Action at European Level," (Brussels: COM(96) 10, 1996).

[907] European Commission, "Implementing European Union Strategy on Defence-Related Industries," (Brussels: COM(97) 583 final, 1997).

[908] European Commission, "The Challenges Facing the European Defence-Related Industry, a Contribution for Action at European Level," 3.

[909] European Commission, "Implementing European Union Strategy on Defence-Related Industries," 3.

[910] European Commission, "Towards an EU Defence Equipment Policy," (Brussels: COM(2003) 113 final, 2003), 11.

[911] Burkard Schmitt, ed. *Between Cooperation and Competition: The Transatlantic Defence Market* (Paris: Institute for Security Studies, Chaillot Papers No 44,2001).

volume pictured the EU and the US as two industrial "fortresses", further underlining that the European context involved the confrontation of various national "citadels". It recalled how, following the 1993 "last supper" organised by then US Defence Secretary William Perry, US defence companies had undertaken a process of concentration, resulting in the constitution or reinforcement of three "giants" (Boeing, Lockheed Martin and Raytheon), and paralleled the situation with developments in Europe. In line with previous publications from the ISS on the topic, the European aerospace and electronics industry was identified as the "champions of integration",[912] with ventures such as Airbus, EADS, and to a lesser extent BAE Systems, following this company's 1999 takeover of the defence electronics company Marconi. The special issue concluded that to reinforce European convergence in the field of defence and foster a balanced transatlantic partnership, an EU policy would have to be deployed alongside the CFSP and ESDP, focusing in particular on supporting new research and development programmes.

It is therefore from this preoccupation with industry, market organisation and regulation that the first initiatives to provide EU support to research and development in defence and security, were shaped. The attempt of the Commission's industry and entreprise services to frame the question of armaments as an issue relevant for the internal market, however, encountered significant opposition within the Council's dedicated working structure, the Ad hoc working party on European Armaments Policy (POLARM). The Austrian and German presidencies (second semester of 1998 and first semester of 1999) attempted to push for the adoption of a common position within the ESDP framework on the matter, with the support of the French representative in POLARM, but several Member State delegations (Belgium, Portugal, Spain, as well as Greece and Denmark to a lesser extent) expressed strong reservations regarding the possibility that the position would include issues of procurement and make reference to the notion of "competition".[913] It is only in March 2003 that the services of the Commission returned to the issue, with a communication jointly drafted by the unit in charge of the ESDP within DG External Relations (DG Relex) and the unit in charge of aerospace and defence in DG Entreprise. The document reiterated, albeit in less alarmist terms, the notion that both the European militaries and the European defence industries were falling behind the US in terms of capabilities and spending, and emphasised the necessity "to create an environment in which European companies can give better value for money".[914] While the angle adopted was sensibly the same as in the communications of 1996 and 1997 ("to set the questions of arms trade and production in their industrial context"), the most concrete proposal put forward by the Commission was "to offer its expertise for an initiative to promote cooperation on advanced research in the field of global security".[915] It is in this document that the reference to security as such, rather than defence equipments or armaments, is introduced, as a result of the persisting controversies among Member States representatives over the desirability of a Community intervention in issues still conceived of as a national, sovereign prerogative. The degree to which this was an intentional move on the part of the drafters of the communication is unclear: it does, however, reflect the fact that the 2003 communication saw the involvement of officials from DG Relex' CFSP unit, at a time where a number of discussions were taking place over the formulation of a European Security

[912] Burkard Schmitt, *From Cooperation to Integration: Defence and Aerospace Industries in Europe* (Paris: Institute for Security Studies, Chaillot Papers No 40, 2000), 15-58.

[913] Council of the European Union, "Outcome of Proceedings from Ad Hoc Working Party on European Armaments Policy," (Brussels: 7287/99, 1999).

[914] European Commission, "Towards an EU Defence Equipment Policy," 5.

[915] Ibid., 16.

Strategy (ESS) to guide EU activities in external relations and foreign policy.[916] The reference nonetheless supported a displacement of the debates, from defence to an all-encompassing concern with security, which would be embraced by subsequent interventions.

Two techniques were mobilised to sustain the Commission's proposal for a research programme in the field of security. The first one, borrowed from what had been done with the aerospace industry a year before, involved the drafting of a programmatic instrument in the form of a report from a high level advisory group. The establishment of the "Group of Personalities on Security Research" in October 2003 echoed the convening of the "European Advisory Group on Aerospace" (EAGA) in 2001.[917] Both groups featured a similar composition, including several CEOs of major electronics and defence companies (e.g. BAE Systems, EADS, Finmeccanica), high level officials from the European institutions (including Commissioners Busquin responsible for research policy and Liikanen responsible for entreprise policy, as well as High Representative Javier Solana, who participated in both outfits), MEPs (chiefly Karl von Wogau, chairman of the subcommittee on security and defence of the European Parliament in 2004-2009, who participated in both groups), and representatives from Member State ministries of Defence. In addition, the GoP comprised representatives from selected think tanks (François Heisbourg, director of the Paris-based Fondation pour la recherche stratégique, and Burkard Schmitt, assistant-director of the Institute for Security Studies, rapporteur of the group and author/editor of this organisation's abovementioned reports) and research organisations (the Dutch organisation TNO). Entitled *Research for a secure Europe*, the GoP's final report formalises the displacement from defence equipments and armaments to security. The distinction is maintained, but the key notion developed in the report is that of a growing continuum between military and security technologies:

> the technology base for defence, security and civil applications increasingly forms a continuum. Across this continuum, applications in one area can often be transformed into applications in another area. This is particularly the case for defence and security: while the armed forces and the various security services will always have their specific needs, there is an increasing overlap of functions and capabilities required for military and non-military security purposes (such as is found between border police; coast guard and emergency response teams) that often allows the use of the same technology for the development of both security and defence applications.[918]

The argument of the continuum enables the translation between the initial, defence focused initiatives promoted by the European Commission until then, and research in security technologies, which is advocated by the GoP in the form of a European security research programme (ESRP) and which it considers should be launched by 2007.

The second technique mobilised to sustain the proposal for a security research programme involved the launching of a "Preparatory action on the enhancement of the European industrial potential in the field of security research" (PASR). The action was launched in February 2004 as a funding scheme for pilot projects coordinated by companies in the field of

---

[916] Anthony Amicelle et al., *Catalogue of Security and Border Technologies at Use in Europe Today* (Oslo: PRIO INEX Deliverable D.1.2., 2009); Didier Bigo et al., *Security Technologies and Society: A State of the Art on Security, Technology, Borders and Mobility* (Oslo: PRIO INEX Deliverable D.1.1., 2008).

[917] Cf. European Advisory Group on Aerospace, "Star 21 Strategic Aerospace Review for the 21st Century: Creating a Coherent Market and Policy Framework for a Vital European Industry," (Brussels: European Commission Entreprise Publications, 2002).

[918] European Commission, "Research for a Secure Europe: Report of the Group of Personalities in the Field of Security Research," (Luxembourg: Office for Official Publications of the European Communities, 2004), 12.

aerospace, electronics and defence, as well as research organisations and university departments.[919] Between 2004 and 2006, the PASR funded 39 projects for a total Community contribution of €44.5 million. Projects dealt with a wide array of issues ranging from biometrics and identification to maritime detection and surveillance, hardware and software for the exchange, processing and "fusion" of information, critical infrastructure and civil protection.[920] Administratively steered by the European Commission's DG Entreprise through a newly established unit on security research, the PASR retained accordingly the market and industrial focus which had characterised Commission initiatives in the field until then. The communication accompanying the decision establishing the PASR, however, reflected the change in focus from defence and armaments to the more loosely defined domain of "security". The document points out that "Europe needs to invest in a "security culture" that harnesses the combined and relatively untapped strengths of the "security" industry and the research community in order to effectively and innovatively address existing and future security challenges" and further suggests that Preparatory Action [...] constitutes a Commission contribution to the wider EU agenda to address Europe's challenges and threats".[921]

The displacement from the organisation of a European market in the field of defence equipments and armaments to security research for industrial purposes was to be confirmed by the second communication tabled by DG Entreprise in September 2004, the already mentioned document on the *Next Steps* in security research, tabled following the publication of the GoP's final installment. This later communication espoused the framing and terminology used in the GoP report, stressing in particular that

> A coherent security research programme at the level of the European Union can add significant value to the optimal use of a highly competent industry. Such research should be capability-driven, targeted at the development of interoperable systems, products and services useful for the protection of European citizens, territory and critical infrastructures as well as for peacekeeping activities [...] research has an important role to play to guarantee a high level of protection.[922]

The document further confirms the perspective of launching, from 2007 onwards, a European security research programme, along the lines of the proposals developed in the GoP report. More generally, it formalises the assembling of security and technology, by making precious few references to the "past" of the initiative and its connection with concerns related to defence equipments and armaments: it is already dealing with the future, with the "next steps", rather than with what has been done before.

---

[919] European Commission, "Commission Decision of 3 February 2004 on the Implementation of a Preparatory Action on the Enhancement of the European Industrila Potential in the Field of Security Research," (Brussels: 2004/213/EC, 2004).

[920] Bigo et al., *Security Technologies and Society: A State of the Art on Security, Technology, Borders and Mobility*, 11-12; Didier Bigo and Julien Jeandesboz, "Review of Security Measures in the 6th Research Framework Programme and the Preparatory Action for Security Research," (Brussels: European Parliament, PE 393.289, 2008).

[921] European Commission, "Communication on the Implementation of the Preparatory Action on the Enhancement of the European Industrila Potential in the Field of Security Research: Towards a European Programme to Advance European Security through Research and Technology," (Brussels: COM(2004) 72, 2004).

[922] European Commission, "Security Research: The Next Steps," (Brussels: COM(2004) 590, 2004), 4.

5.3.3 Assembly process #2: the industry and the construction of a security market

The second assembly process of security and technology follows from the activities of the defence and security industry itself and the patterns of its involvement in the European governmental arenas. As touched upon in the previous section, the devising of a dedicated security research programme has been strongly influenced by the 2004 report from the GoP and the involvement of representatives from major aerospace, electronics and defence groups. The implication of representatives from major aerospace, electronics and defence groups has subsequently been furthered through the proceedings of two consecutive high profile venues, ESRAB (the *European Security Research Advisory Board*) and ESRIF (the *European Security Research Innovation Forum*). The involvement of industry representatives in the GoP, ESRAB and ESRIF has been saluted in 2007 by the European Commission as a blueprint for the further development of a "public-private-dialogue in security research and innovation".[923] Examining the role played by the industry in the assembling of security and technology requires the combination of two lines of inquiry. The first line involves looking at what is translated under the notion of "the industry". Which actors are comprised and mobilised under this denomination, and which spokespersons can be identified? The second line of inquiry entails examining the patterns of engagement of industrial actors in EU security activities. A preliminary distinction, which will structure the following pages, is between programmatic involvement through such venues as the GoP, ESRAB and ESRIF, and practical involvement, the survey of which will built on the analysis of security research activities within the FP7 Security Theme.

The examination of which entities are included under the denomination of the "industry" can be undertaken in two ways. One can firstly look at the structures engaging with the European institutions. This calls for a brief overview of how the presence of aerospace, defence and electronics companies in Brussels has been organised over the past few years. Before the 1990s, there was no representation of the defence industry in Brussels that targeted specifically the European institutions. The main pan-European venue for companies in the defence sector was the European Defence Industry Group (EDIG), which was initially established in 1976 to weight on NATO-led armaments cooperation. In 1990, however, EDIG was established as an ASBLI (*Association sans but lucratif international*) under Belgian law, and opened an office in Brussels. The engagement of the aerospace industry with the European institutions followed a similar pattern. The first pan-European associations, AICMA (*Association internationale des constructeurs de matériel aérospatial*) and EUROSPACE (European association for the space industry) were created in 1950 and 1961 respectively. AICMA became AECMA (*Association européenne des constructeurs de matériel aérospatial*) in 1973, and eventually opened an office in Brussels in 1991. In 2004, AECMA, EDIG and EUROSPACE merged into ASD, the Aerospace and Defence Industries Association of Europe. It appears that those companies involved in both the civilian aerospace and defence sector (e.g. BAE Systms, EADS, Finnemecanica, Thales) have been driving this merger, as they were among the prime defence-related actors from the private sector to be solicited by the European Commission in the context of its first initiatives in the field of the aerospace industry - the establishment of EAGA and the drafting of the STAR 21 report in 2002. In July 2007, another body was formed by the same group of major aerospace and defence companies. The European Organisation for Security (EOS) presents itself as a policy-oriented professional organisation dedicated to "support a consistent and comprehensive

[923] European Commission, "Public-Private Dialogue in Security Research and Innovation," (Brussels: COM(2007) 511, 2007).

implementation of security strategies at national, European and international level" as well as "the development of a European security market". While ASD is exclusively made up of national associations of companies in the field of aerospace and defence, EOS membership comprises both associations, including national outfits and transnational structures such as ASD, and individual companies.

Another way to examine the composition of "the industry" is to look at the membership of the different venues organised for the purpose of involving private sector organisations in EU activities regarding security technologies. Besides the GoP, two other venues established since 2004 stand out: ESRAB and ESRIF. ESRAB was convened by the European Commission in April 2005 as a follow-up to the September 2004 communication on the next steps in security research[924] and delivered its final report in September 2006.[925] It brought together fifty individual participants from the private sector, national governmental agencies with security, defence and research activities, and several think tanks and research organisations. While larger in numbers, ESRAB's membership mirrored that of the GoP in terms of composition. Industry representatives came almost exclusively from the largest companies in their respective domains, such as BAE Systems, Diehl, EADS, Ericsson, Finmeccanica, Sagem, Siemens or Thales.[926] The same observation can be made concerning ESRIF, which was established as a follow-up to ESRAB. ESRIF was launched in September 2007. Unlike the GoP and ESRAB, ESRIF is not formally tied to the European Commission[927]. It is presented by the latter as "a forum for the development of a Public-Private Dialogue in the area of EU security research and innovation" which was "set up in agreement with the Member States and organised by the stakeholders".[928] In the foreword to ESRIF's 2008 intermediate report, Gijs de Vries, the forum's chairman and former EU Counter-terrorism coordinator, introduced it as "an informal and voluntary group of experts coming from the supply and demand side of security technologies and solutions".[929] Despite the notion conveyed by these comments that ESRIF is a more spontaneous venue than the GoP and ESRAB, the forum's constituency features a similar representation from the private sector.

One conclusion that can be drawn from these observations is that "the industry" stands for a fairly limited number of entities, large-scale, multinational companies with ties to the defence equipments and armaments domain, with for some a relatively long-standing involvement in the European governmental arenas. As Figure 5.1 on the following page illustrates, the constituency of the different venues where the issue of security research has taken shape (GoP, ESRAB, ESRIF) has progressively widened over time, but a handful of entities remain

[924] European Commission, "Commission Decision of 22 April 2005 Establishing the European Security Research Advisory Board," (Brussels: 2005/516/EC, 2005).

[925] ESRAB, "Meeting the Challenge: The European Security Research Agenda," (Luxembourg: Office for Official Publications of the European Communities, 2006).

[926] A notable addition to this group, however, is Sagem, which was not represented in the GoP. Besides being involved in defence activities, Sagem, through its Morpho subsidiary which it acquired in the early 1990s, is one of the leading companies in the field of biometric systems. Its inclusion arguably reflects the shift in scope from more strictly defined defence equipments and armaments matters to the looser thematic of security technologies

[927] Although its establishment was announced jointly by German Minister for Education and Research, Annette Schavan, and the two Commission vice-presidents of the first Barroso college, Günter Verheugen (Entreprise) and Franco Frattini (Justice and Home Affairs) at the 2nd European Conference on Security Research in Berlin on 26 March 2007.

[928] European Commission, "The European Security Research and Innovation Forum (Esrif) - Public-Private Dialogue in Security Research," (Brussels: MEMO/07/346, 2007), 2.

[929] ESRIF, "European Security Research and Innovation in Support of European Security Policies: Intermediate Report," (Luxembourg: Office for Official Publications of the European Communities, 2008), 7.

consistently involved, and also stand out in the professional associations that take position for the industry (as ASD's "major companies" and EOS board members). From an analytical point of view, then, the reference to "the industry" in official documents, such as the Commission's 2007 communication, renders the limited scope of the relations between the public and the private sector mobile, and "blackboxes" the actual standing of the "public-private dialogue".[930]

The reflection on the entities composing "the industry" goes hand in hand with the examination of how these entities have contributed to the assembling of security and technology, and problematised the issue. In a presentation of his organisation at a 2010 event in Ankara, EOS CEO Luigi Rebuffi highlighted two rationales for the private sector's involvement with the European institutions: to develop a "harmonised security market across EU countries" and to "create business opportunities for its members" . A running theme in the views expressed by a number of high-level executives from the private sector, indeed, has been the question of the "maturity" of the market for security goods. Speaking at the launch event of EOS in Brussels on 14-15 May 2008, Thales CEO Denis Ranque suggested for example that security accounted for a very small part of his company's turnover, pointing out the need for an intervention from the EU institutions. The degree to which this assessment varies from company to company, of course, should not be underplayed. The market for biometrics, for example, is considered by the main players in the field as well established.[931] This problematisation has resulted in a number of interventions from private sector actors which have contributed to further reinforce and sustain the assembling of security and technologies, through the issuance of a number of programmatic document beyond the participation in venues such as ESRAB and ESRIF. EOS has been an important platform in this regard, with a series of "white papers" covering all the key domains singled out in the ESRAB and ESRIF final reports. Its white paper on "a European approach to border management", for example, advocates for a technology-intensive approach to border control, arguing that "the improved management of passengers, vehicles and goods movements should take full advantage of a rapidly evolving technological landscape".[932] The white paper's recommendations include measures such as the creation of an "EU border checks task force" where EOS would be appointed as the spokesperson of the industry, the creation of an EU fund for the creation of a pan-EU integrated border management system, the enhancement of the standardisation and interoperability of equipments used in border control, as well as the use of so-called "EU reference solutions", to be preferred to the acquisition of equipments from non-EU companies. The report expresses support for all the initiatives that have been launched over the past few years through the European governmental arenas in the field of border control, including the entry/exit system (EES), registered traveller programme (RTP), electronic system of travel authorisation (ESTA) and European Passenger Name Record system (EU-PNR). The scope of the report underlines that "industry" interventions go beyond the mere development of technology: it focuses significantly on market regulation, as well as on the holistic development of "supply chains" and "end-to-end"[933] programmes (one of the references being the GALILEO programme, for instance). The emphasis on "integrated solutions" in the field of border control, furthermore, is a recurrent item in the standpoints

[930] Cf. also Didier Bigo and Julien Jeandesboz, "The EU and the European Security Industry: Questioning the 'Public-Private Dialogue'," (Brussels: CEPS, INEX Policy Briefs, No 5, 2010).

[931] See e.g. the comments of the scientific and business director of Sagem Défense et Sécurité: Bernard Didier, "Biometrics," in *The Security Economy*, ed. OECD (Paris: OECD, 2004).

[932] EOS, "White Paper: A European Approach to Border Management," (Brussels: European Organisation for Security, 2009), 9.

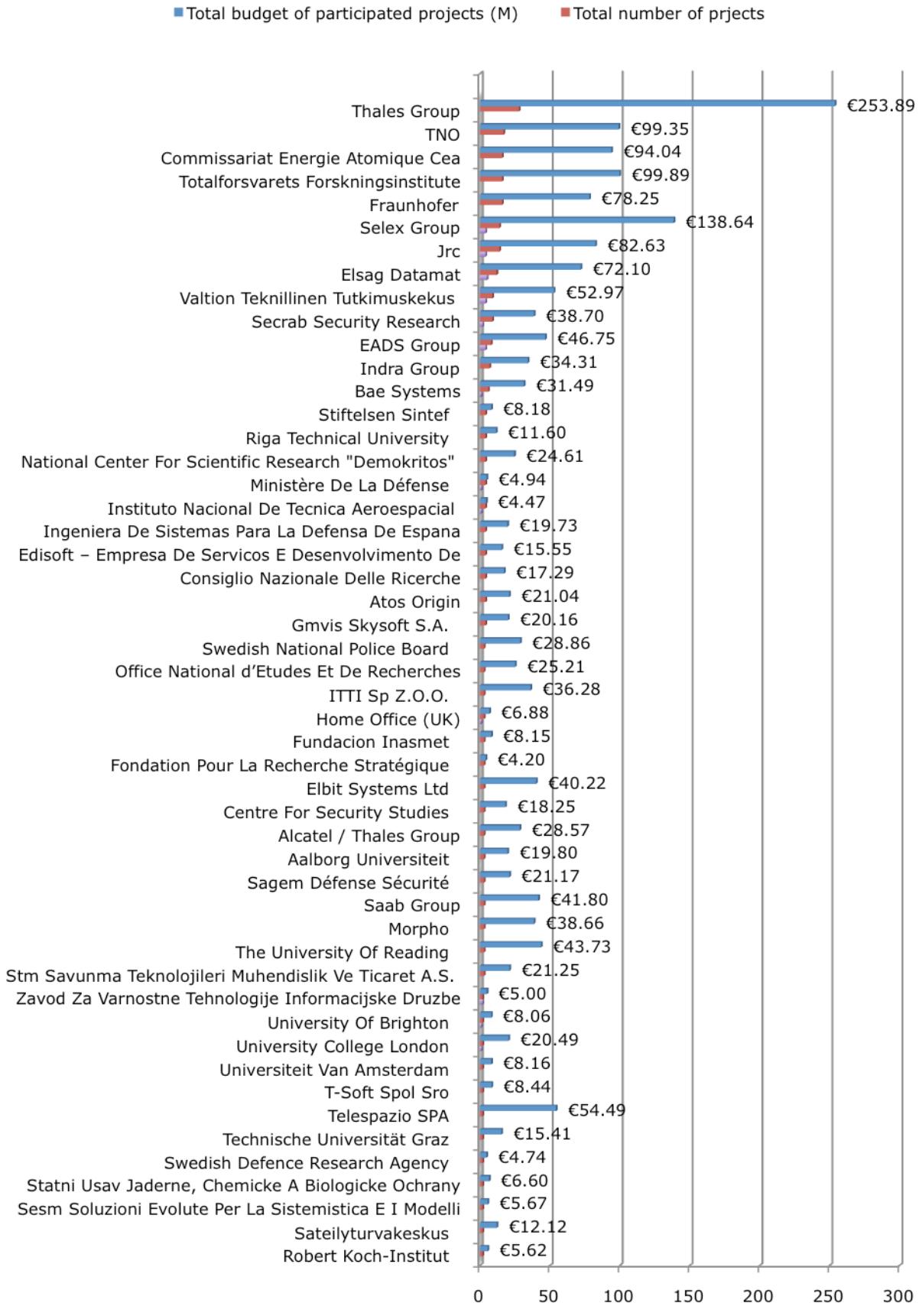
[933] End-to-end programmes correlate the development of a policy/regulatory framework and standards with research and development and pilot projects, the deployment of an actual system, and services to customers.

expressed by the main actors involved in EOS. In the words of EOS CEO Luigi Rebuffi, this entails a "global approach" promoting the correlation between a given system (presumably national), a "system of systems" (presumably EU-wide) and the development of common architectures presumably enabling interoperability.[934]

The programmatic activities of private sector entities have significantly contributed to reinforcing the association forged between security and technology. The assembling of security and technology has been further sustained by the practical involvement of these entities in the development of technological systems, chiefly through the FP7's security research theme. The survey of these activities reflect the same pattern observed above: some of the companies that have become the spokespersons of "the industry" have also prevailed significantly in the conduct of research activities. A study conducted last year for the European Parliament on the FP7 Security Theme (based on projects funded through the first and second calls) has highlighted that both in terms of project coordination and in terms of the aggregated number of participation in EU funded activities, the companies that have been involved in the GoP, ESRAB and ESRIF venues, as well as in ASD and EOS, rank fairly high, as illustrated in the two following figures below:

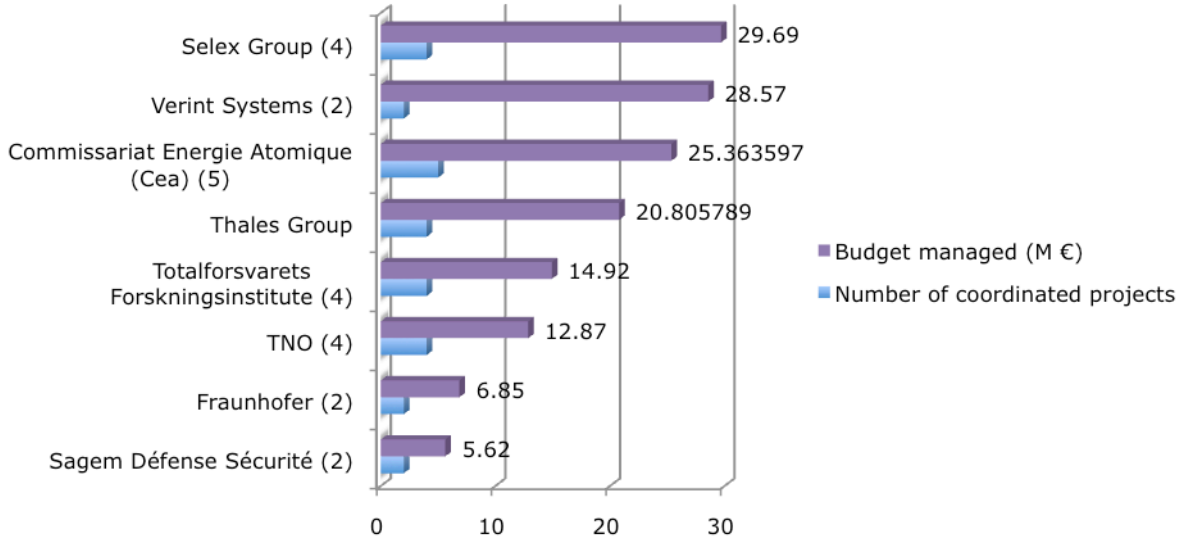
[934] Luigi Rebuffi, "A Description of the European Organisation for Security, Its Roles, Its Actions and Its Recommendations for Building a Common Security Approach," (Ankara, December 20102010).

Figure 5.1: Top 50 of single organisation participation, by project and budget[935]



[935] Source: Ibid., 24.

Figure 5.2: Organisations coordinating more than one project[936]



5.3.4 Assembly process #3: technology and the "internal security market"

The third process involved in the assembling of security and technology follows from the activities of spokepersons from the field of security professionals. Technology has been at the core of discussions involving representatives from various "guilds"[937] of professionals such as criminal police, border guards, the military or intelligence services, as well as representatives from Member State ministries of Interior and Justice, in the European governmental arenas. In policy documents related to EU-sponsored security research, these agents are translated into the "demand side" of security technologies. Just as with the "industry", however, examining the role played by security professionals in the assembling of security and technology requires in the first place an investigation of which actors are actually blackboxed through references to the "demand side", before considering in what terms they frame this assembling. The argument here is twofold. Firstly, the assembly of security and technology has chiefly involved "guilds" whose main professional involvement is in issues labelled as internal security: criminal police officers and officers from specialised branches such as counter-terrorism or immigration police, border guards or gendarmerie-type bodies, and customs officers. Secondly, technology has been framed as a means to sustain better and more efficient internal security policies. This purported belief in technology as efficiency is the entry point for a number of critical assessments of the relation between security and technology, whether by civil liberties organisations[938] or by academics who suggest that technology constitutes a "salvation tool" for security professionals.[939] Prying open this black box, however, enables another view: in the EU context, technology is indeed a "salvation tool", but in the sense that

[936] Source: Julien Jeandesboz and Francesco Ragazzi, "Review of Security Measures in the Research Framework Programme," (Brussels: European Parliament, PE 432.740, 2010), 23.

[937] Didier Bigo, "Delivering Security and Liberty? The Reframing of Freedom When Associated with Security," in *Europe's 21st Century Challenge: Delivering Liberty and Security*, ed. Didier Bigo, et al. (London: Ashgate, 2010), 396.

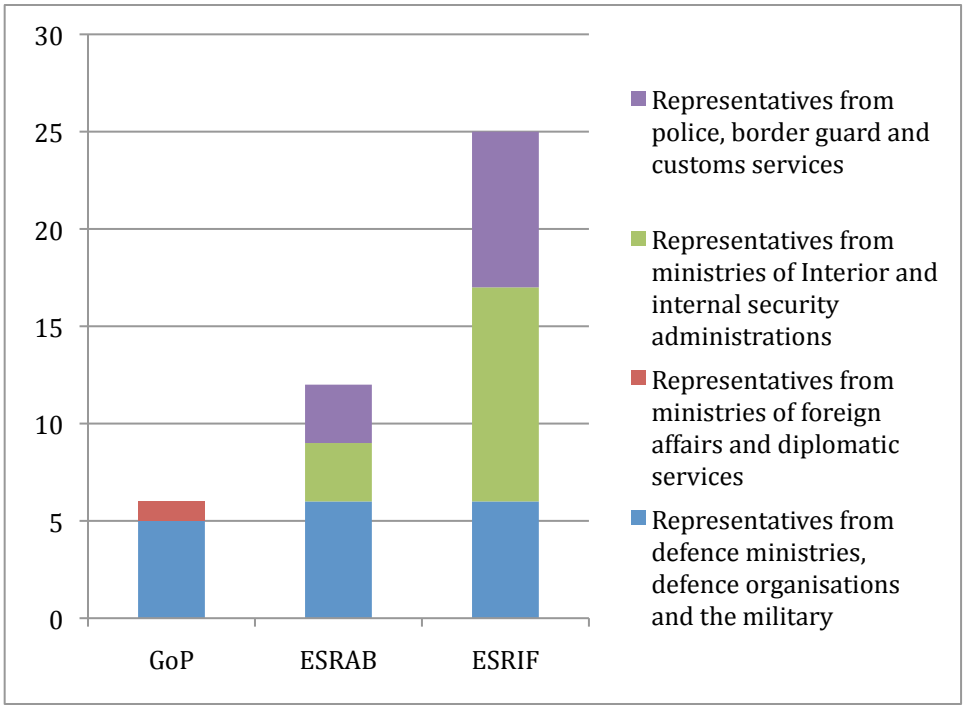
[938] Ben Hayes, "Arming Big Brother: The Eu's Security Research Programme," (Amsterdam and London: TNI and Statewatch, 2006); Ben Hayes, "Neoconopticon: The EU Security-Industrial Complex," (Amsterdam and London: TNI and Statewatch, 2008).

[939] Philippe Bonditti, "From Territorial Spaces to Networks: A Foucaldian Approach to the Implementation of Biometry," *Alternatives : global, local, political* 29, no. 4 (2004).

references to technology and the development of initiatives organised around technologies, particularly systems for the exchange and processing of personal data, appear to have become a condition of possibility for EU internal security policies.

A key insight that can be derived from the analysis of the participants in the three major venues organised around EU security research (GoP, ESRAB, ESRIF) is that a progressive shift has taken place, from defence and military professionals to internal security professionals. This is illustrated in Figure 5.3 below. The GoP predominantly involved participants with a background in defence, military and diplomatic affairs. It comprised representatives from the Belgian and Greek ministries of defence, from organisations tied to the military such as the West European Armaments Group, as well as individuals whose professional standing closely associated them with military and diplomatic affairs (such as MEP Karl von Wogau, at the time chairman of the European Parliament's subcommittee on defence and security, or the EU High representative for CFSP Javier Solana). The setting-up of ESRAB reflected a first shift. While a number of participants in the Board remained professionally tied to defence, military and diplomatic affairs, other delegates originated from ministries of the Interior (the UK Home Office and Italian ministry of Interior), police services (Europol and the German *Bundeskriminalamt*) and border guards (Polish Border Guards). The constituency of ESRIF confirms the trend: forum representatives from internal security agencies, bodies and services (whether EU or national entities) outnumber representatives tied to the military, defence and diplomatic affairs: the latter having all but disappeared, while the numbers of the former remaining steady despite the overall increase in membership between ESRAB and ESRIF.

Figure 5.3: Spokespersons from security agencies, bodies and services in the GoP, ESRAB and ESRIF



What surfaces from this brief analysis is that the assembling of security and technology through EU security research schemes does not concern all security professionals, but involves more specifically the establishment of ties between a number of major companies originating from the defence and armaments sectors, and agencies, bodies and services focused on issues pertaining to internal security. The trend is less a natural outcome of the "needs" of these entities, than the product of the logics of competition among security professionals in relation to the development and use of technology. This transpires, for example, in the statement recently delivered by the EU Counter-Terrorism Coordinator (CTC) Gille de Kerchove at a conference organised by EOS and the think-tank *Security and Defence Agenda* in Brussels in February 2011:

> Unlike ministries of defence which have a culture of planning, programming and are forward looking, ministries of the interior in many, if not in most, member states don't have that culture […] we public authorities should do better to identify and make known our needs in the field of security related research […] If ministries of interior, and by this I mean law-enforcement and all the other players in internal security, like customs, don't express their views and requirements, it's very difficult for academics, researchers and most of all for private industry to invest. That's very important because if we don't do it, the risk is that the political choices will be technology-driven.[940]

The assembling of security and technology, in this perspective, is a stake in the competitions on the definition of priorities in security policies. It is translated in the excerpt above in terms of a comparison between defence ministries and ministries of the Interior. This specific operation of translation has been for some years now a standard view of the CTC and his team. It is formulated, for example, in the CTC's November 2009 discussion paper on the EU's counter-terrorism strategy, which was published shortly before the entry into force of the Lisbon treaty. Noting that "unlike the military, law enforcement does not have a tradition of forward planning for its future requirements from technology", the paper notably introduces the notion of a "market for internal security products in Europe", which is a significantly different entity than the "market for security technologies" examined previously.[941] The CTC, however, is not the only actor relying on this tactic. An initiative worth mentioning, in this regard, concerns the efforts of some governments to establish a "European Network of Internal Security Technology Departments". The proposal was introduced by the French government during the country's turn in holding the Union's Presidency, and also coincided with the organisation of the third European Security Research Conference (SRC) in Paris in September 2008.[942]

This specific translation – from security technology to internal security technology – simultaneously "blackboxes" the relations between actors involved in the field of internal security. The relation between technology and internal security is framed in terms of forward planning and of efficiency – better technologies, in short, for better internal security. This problematisation simplifies considerably the intensity of controversies among internal security actors concerning the priorities and conduct of internal security activities in the EU context. Whereas policy documents translate security into an unproblematic notion, different groups of professionals retain different views of the priorities and outlook that security

[940] EOS & SDA, "A New Partnership for European Security," (Brussels: 10 February, 2011), 12-16.

[941] Council of the European Union, "Note from EU Counter-Terrorism Coordinator to Council/European Council: EU Counter-Terrorism Strategy - Discussion Paper," (Brussels: 15359/1/09, 2009), 9.

[942] Council of the European Union, "French Initiative to Set up a European Network of Police Technology Services," (Brussels: 5629/08, 2008); Council of the European Union, "European Network of Internal Security Technology Departments," (Brussels: 14669/08, 2008).

policies should adopt. This holds true in national arenas, where various agencies and services compete for resources and bureaucratic territory through the definition of what exactly constitutes a threat and how it should be met, and even more so within the European governmental arenas, where the transnational character of the struggles involved adds a layer of complexity to the process.[943] In the EU context, a key stake of these struggles involves the definition of boundaries between what should be considered an internal matter and what should be regarded as an external matter. Which issues should be considered as the exclusive remit of the Member States, and in which matters should one or the other EU agency, body or service in charge of security matters be allowed to intervene? Which questions should be "intergovernmentalised", that is dealt with through the EU but in a configuration where the Commission and the European Parliament are not to interfere, and which questions should be considered as "communautarised", involving the application of the Community method of decision- and policy-making? Which matters should be treated as belonging to international security as defined by the now-defunct second pillar, and which matters should be considered as involving internal security and the third pillar (formally discontinued as well)?

Research conducted on the European field of security professionals within the CHALLENGE project has suggested that these boundary struggles involve two key groupings, termed the "Classics" and the "Moderns", which hold differentiated standpoints on the priorities and strategic outlook of EU security policies.[944] The Classics retain the traditional, sovereign perspective on security as security of the nation-state, encompassed within territorially-defined and fixed borders, with a clear distinction between internal and external security and a mostly reactive attitude, whether in the field of internal security (traditional criminal justice) or external security (the military is seen as a tool for external security to be engaged abroad and used to defend the external borders of the state). The Moderns, on the other hand, support the idea that the post-bipolar period has fundamentally transformed what should be regarded as a security matter and how it should be dealt with. Contemporary threats, Modern narratives contend, are vastly more fluid and unpredictable than during the previous, bipolar period, and no longer tied exclusively to inter-state conflicts. They involve a variety of networked groups operating transnationally, and using the dependence of North American and European economies on free movement of persons, goods, services and capitals to conduct their activities. The activities of these groups, it is argued, establish connections between petty crime and "serious" organised criminality, between organised crime and political violence considered as terrorist, also related to the irregular entry of persons on the territory of European and North American states. This configuration requires a transformation of national, European and international security architectures, fostering more transnational cooperation among more autonomous security agencies and bodies, and the enhancement of capacities to trace persons, particularly travellers, in order to identify members of groups deemed troublesome and prevent them from conducting actions against American and European citizens. This enhancement, in turn, involves increasing the reliance of security agencies, bodies and services on the collect and processing of data, pro-actively and for profiling purposes, and supported the shift towards surveillance-driven EU security policies, in the name of the protection of European citizens.

---

[943] Malcolm Anderson and Monica Den Boer, eds., *Policing across National Boundaries* (London: Pinter,1994); Didier Bigo, *Polices En Réseaux: L'expérience Européenne* (Paris: Presses de Sciences Po, 1996); Didier Bigo, "La Mondialisation De L'(in)Sécurité? Réflexions Sur Le Champ Des Professionnels De La Gestion Des Inquiétudes Et Analytique De La Transnationalisation Des Processus D'(in)Sécurisation," *Cultures & Conflits*, no. 58 (2005); Huysmans, *The Politics of Insecurity: Fear, Migration and Asylum in the EU*.

[944] Didier Bigo, "Globalized (in)Security: The Field and the Banopticon," in *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11*, ed. Didier Bigo and Anastassia Tsoukala (London: Routledge, 2008).

To some extent, it appears the "Moderns" have acquired a predominant position within the European governmental arenas. An increasing number of data processing schemes are being put in place through EU initiatives - the latest count being over twenty-five, including major operations such as the pan-European databases SIS and Eurodac, the upcoming Visa Information System (VIS) and SIS-II, as well as planned schemes such as the upcoming "smart borders" initiative, comprising an EU entry/exit system (EU-EES), registered traveller programme (EU-RTP) or Passenger Name Record (EU-PNR). The trend has been accelerating significantly over the past few years, and is now involving the establishment of data-mining and profiling tools, which would turn some of these data systems into multi-purpose intelligence tools.[945] This trend has also been formalised in strategic EU policy documents. The most striking example here is the *Future of European Home Affairs* report drafted by the eponymous informal High Level Working Group (hereafter Future Group) circulated to the Council in July 2008.[946] The report highlights in particular that:

> In a space where people and goods move freely, information exchange is a key component of European security […] The Group estimates that European information networks should now be developed from a legal as well as from a technical standpoint, with a global and coherent approach taking fully into account operational needs.[947]

The report of the Future Group had a durable influence on the programmatic logic of EU internal security policies. The December 2009 Stockholm programme, the EU's latest multiannual programmatic instrument establishing the priorities for the area of freedom, security and justice, thus considers technology and particular data processing instruments as necessary "tools for the job".[948] The EU's internal security strategy, adopted in February 2010, promotes a "European security model" based on "prevention and anticipation […] on a proactive and intelligence-led approach".[949] The trend is also reflected, beyond programmatic

---

[945] See the discussion in: Evelien Brouwer, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System* (Leiden: Martinus Nijhoff, 2008); Florian Geyer, "Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice," (Brussels: CEPS CHALLENGE Research Papers, No 9, 2008); Elspeth Guild et al., "Review of the Data Protection Legal Framework," (Brussels: European Parliament, Report for the LIBE Committee, forthcoming (September), 2011).

[946] Council of the European Union, "Freedom, Security, Privacy - European Home Affairs in an Open World - Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy ("The Future Group")," (Brussels: 11657/08, 2008). The Future Group was established at an informal meeting of the EU ministers of Interior and Justice in Dresden on 14-16 January 2007. It brought together representatives from the then-upcoming two trios of EU Presidencies, starting with the German presidency who initially proposed the setting-up of the outfit, and including representatives of Portugal (Minister of the Interior Rui Pereira), Slovenia (Minister of the Interior Dragutin Mate), France (Ministers of the Interior Michèle Alliot-Marie and Brice Hortefeux), the Czech Republic (Minister of the Interior Ivan Langer), Sweden (Minister of the Interior Beatrice Ask and Minister for Migration and Asylum Policy Tobias Billström), Spain (Secretary of State for Security Antonio Camacho Vizcaino), Belgium (Minister of the Interior Patrick Dewael) and Hungary (Secretary of State for EU Affairs, Ministry of Justice, Judit Fazekas), as well as the member of the Commission in charge of the justice, liberty and security portfolio (Italian commissioner Franco Frattini until April 2008, French commissioner Jacques Barrot from May 2008). Observers included Baroness Patricia Scotland (Attorney General of the United Kingdom), Chairs of the European Parliament LIBE Committee (Jean-Marie Cavada until January 2008, Gérard Deprez from January 2008), and Director General for Justice and Home Affairs in the Council Secretariat Ivan Bizjak.

[947] Ibid., 14.

[948] European Commission, "The Stockholm Programme - an Open and Secure Europe Serving and Protecting Citizens," 62.

[949] European Commission, "Draft Internal Security Strategy for the European Union: Towards a European Security Model," 11.

documents, in some key nominations, such as the appointment of Rob Wainwright, former director of the United Kingdom's Serious Organised Crime Agency (SOCA), an organisation that has actively promoted intelligence-led policing, at the head of the European police office (Europol) or that of Ilkka Laitinen, the former head of the short-lived EU Risk analysis center in Helsinki, at the head of the EU's external borders agency Frontex. It is also visible in the re-organisation of the Council's working structures in the field of justice and home affairs and the introduction of the Standing Committee on Internal Security (COSI), which has led to the adoption of an "EU policy cycle" in the field of internal security strongly influenced by the prescriptions of intelligence-led policing as it has developed in Belgium, the Netherlands and the UK.[950]

This trend, however, should not be taken to imply that the emphasis on technology-driven initiatives reflects a consensus. As a number of studies have shown, the adoption of proposals regarding new data-processing schemes in the European governmental arenas is usually underpinned by references to multiple purposes.[951] Hence, the SIS II has been framed as a tool for border control, immigration control, counter-terrorism and policies targeting organised crime. The same holds true of the VIS, on which discussions were reinvigorated by counter-terrorism concerns following the events of 11 September 2001 in the United States, but which would, once operational, be considered a tool for the purpose of visa policies, of counter-terrorism policies, and organised crime policies. To some extent, the very proliferation of data-processing schemes in EU internal security policies is a sign that controversies and struggles, rather than consensus, predominates among security professionals. References to security agencies, bodies and services as the "demand side" of an "internal security market", in this regard, are an operation of simplification, which obfuscates the fact that the assembling of security and technology constitutes both a "salvation tool" and a point of contention among security professionals.

The notion that controversies and struggles, rather than consensus and cooperation, fuel the assembling of security and technology, is central to understanding contemporary surveillance practices in the context of the EU's security policies. In previous pages, we have seen how the assembling of security and technology has been enabled by a series of operations of translation, particularly focused on the simplification and "blackboxing" of the complexity of the various entities ("the market", "the industry", the "supply" and "demand" sides, and so forth) involved in this process. As suggested in Section 5.1., translation involves control and effects of power, an argument that puts into question contemporary assumptions about the relation between technology and efficiency, in particular. Of direct concern, here, is the argument of "multi-purpose" systems, which are a direct challenge to a core principle of data protection law, i.e. purpose limitation. This observation, incidentally, also suggests that principles of fundamental rights and freedoms, including the right to data protection and the right to privacy, are opened to contests, controversies and struggles.

[950] Amandine Scherrer et al., "Developing an EU Internal Security Strategy, Fighting Terrorism and Organised Crime," (Brussels: European Parliament, forthcoming study, 2011).

[951] Didier Bigo et al., "Towards a New EU Legal Framework for Data Protection and Privacy: Challenges, Principles and the Role of the European Parliament," (Brussels: Note on behalf of the LIBE Committee of the European Parliament, Manuscript, September 2011, 2011); Brouwer, *Digital Borders and Real Rights: Effective Remedies for Third-Country Nationals in the Schengen Information System*; Joanna Parkin, "The Difficult Road to the Schengen Information System Ii: The Legacy of 'Laboratories' and the Cost for Fundamental Rights and the Rule of Law," (Brussels: CEPS, Liberty and Security in Europe, 2011).

5.4 CONTROVERSIES ABOUT SECURITY, SURVEILLANCE AND TECHNOLOGY

The assembling of security and technology, as suggested above, is far from a univocal process. It has been fuelled, in part, by a number of controversies. Tracing and mapping these controversies is useful to develop a more precise understanding of the contemporary politics of surveillance and the emergence of "smart" surveillance. In the following pages, we outline three sets of controversies:

- The first set involves controversies about security itself. In line with the methodological suggestions developed in Section 5.1., the elements examined above in subsection 5.2.4 as well as with the review of the scholarly literature on surveillance proposed in Section 1.1., it appears central not to "blackbox" security as a consensual matter. Of concern, here, is how the increased emphasis on surveillance, on pro-activity and profiling in EU security policies has played out in the European governmental arenas (5.3.1.)
- The second set involves controversies over ethics (5.3.2.). The discussion of the correlation between security, surveillance and technology in terms of ethics has been "built in" EU-sponsored security research, for example through the formulation of the calls for application of the FP7 Security Theme. Ethics, however, has proved a dynamic notion, open to different operations of translation. As we will see in the following pages, references to ethics have been used, on the one hand, to reduce concerns about the effects of the growing reliance on technology in security policies to narrowly defined issues of trust and acceptability. On the other, references to ethics have also been used to contest the standing of technology as a "salvation tool", as a support both to academic studies and to more activist engagements with security, surveillance and technology.
- The third set of controversies we survey here involve privacy and data protection (5.3.3). It discusses the dichotomy, easily adopted in some of the leading contributions in the field,[952] between privacy and surveillance, between "privacy advocates" and those that should, in this logic, called "surveillance advocates". References to data protection and privacy, it is argued, are much more widespread than should be expected if one follows this dichotomy, including among security professionals as well as producers and promoters of security technologies. We will thus look at how the right to data protection and the right to privacy are differently translated and sustain controversies and struggles about surveillance.

5.4.1 Controversies over security and the shift towards surveillance

The first step to understand contemporary controversies about security, surveillance and technology, as illustrated by developments within the European governmental arenas, is to emphasise that security itself is subject to a variety of contests. The contours of these contests have been outlined in the previous section (5.2.4.). The purpose of the following pages is to start from a more "local" analysis of these controversies as they drive EU security policies towards an increased emphasis on surveillance. This shift, of course, is hardly homogeneous. In line with the discussion on "rhizomatic surveillance" introduced in the state of the art overview of the deliverable's first section, it should be regarded as contingent upon struggles among security professionals. To make this point, we concentrate on one of the so-called

[952] Colin J. Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance* (Cambridge: MIT Press, 2008).

"Justice and Home Affairs agencies" of the EU, the body in charge of the Union's external borders Frontex, and the recent discussions surrounding the updating of its mandate.

The updating of the agency's founding regulation is informed, in a large part, by the reluctance of EU Member States to confer any kind of operational competence to EU bodies in the field of security.[953] None of the EU "JHA Agencies" (Europol, Eurojust, Frontex and Cepol) has currently been given an operational remit. Although a number of discussions have taken place around the establishment of a so-called "European FBI" on the basis of Europol, or of a European border guard through the external borders agencies Frontex, such proposals have been met with staunch opposition by representatives of the Member State ministries of Interior and Justice.[954] This situation has driven the activities of the agencies, most notably Europol and Frontex, to invest in activities of risk assessment and information-sharing, to the detriment of operational activities such as the conduct of criminal investigations (for Europol) or actual border checks, the conduct of which is explicitly outside of the remit of Frontex.[955] The bulk of Europol's activities currently consists in providing and circulating information among the law-enforcement bodies of the Member States, relying in part on its own information system, in coordinating some joint operations, and in providing risk analyses and threat assessment reports, the most notorious being its OCTA (organised crime) and TE-SAT (counter-terrorism) reports. Frontex offers a similar example. While the agency was established in 2004 in response to concern regarding the operational control of the Union's external borders after enlargement, it does not have its own "border guard" units, and has up to now mainly been a channel for planning and staging so-called joint operations. While the operational side of its remit drains most of the agency's resources, Frontex officials place significant emphasis on the risk assessment and intelligence aspect of their participation in EU security activities. The agency, however was initially barred from accessing personal data. Such a competence was not deemed necessary to the fulfilment of its mandate, since it was not expected to conduct actual border checks, which might have required its officials to access the SIS.

This issue spurred a number of controversies, which recently coalesced around the Commission's proposal for a revision of the Council Regulation establishing the agency. The process has recently seen the Council and the European Parliament conclude a political agreement over a final draft. The Commission's proposal, tabled in February 2010, introduces a new Article 11 which specifies that while the agency "shall develop and operate an information system capable of exchanging classified information with the Commission and the Member States […] [t]he exchange of information to be covered by this system shall not include the exchange of personal data". In the explanatory statement accompanying the proposal, the services of DG Home explain that while the processing of personal data by the agency should be considered, the Commission "prefers to return to the question of personal data in the context of the overall strategy for information exchange to be presented later this year".[956]

---

[953] Didier Bigo, ed. *The Field of EU Internal Security Agencies* (Paris: L'Harmattan,2008); Scherrer et al., "Developing an EU Internal Security Strategy, Fighting Terrorism and Organised Crime."

[954] On the case of Frontex, cf. Julien Jeandesboz, "Reinforcing the Surveillance of EU Borders: The Future Development of Frontex and Eurosur," (Brussels: CEPS CHALLENGE Research Papers, No 11, 2008); Andrew W. Neal, "Securitization and Risk at the EU Border: The Origins of Frontex," *Journal of Common Market Studies* 47, no. 2 (2009).

[955] Bigo, ed. *The Field of EU Internal Security Agencies*.

[956] European Commission, "Proposal for a Regulation of the European Parliament and the Council Amending Council Regulation (Ec) No 2007/2004 Establishing a European Agency for the Management of Operational

Claiming access to personal data has however been a staple in the public interventions of the agency's management officials almost since its inception. The director of the agency, former Brigadier General Ilkka Laitinen, has proven a staunch supporter of a preventive, intelligence-driven stance in the control of the Union's external borders. Acting as the "spokeperson" of the integrated border management doctrine promoted in the European governmental arenas, he argued for instance in a 2007 news release aimed at countering some of the criticism that the agency was facing that…

> The raison d'être of Frontex are not emergency operations but the consistent introduction of well planned regular patrols by Member States in order to limit urgent missions and to integrate the management of borders in all its dimensions defined by Member States. Doctors say that the best intensive care unit cannot replace prophylaxis: I would say that it applies also to borders".[957]

Laitinen has continuously emphasised the centrality of risk assessment as a core component of the agency's "prophylaxis" actions: "[a]ll FRONTEX activities are based on risk analyses, the "engine" of FRONTEX activities" was for example how he introduced the question to an interparliamentary meeting between the European Parliament and the Parliament of Finland in October 2006.[958] A key component of his argumentation has been the expression of support for the agency's access to personal data, including in circumstances otherwise unrelated to this particular discussion. A good illustration is provided by Laitinen's final comments at a workshop organised by the European Parliament's LIBE Committee in June 2010 on the issue of access to documents of the EU institutions after the entry into force of the Lisbon Treaty:

> And finally […] I would like to make a very short comment […] on the personal data question. I would just like to make it very clear that now in the new situation when the Lisbon treaty is in force, and we have the internal security strategy in place, where border control can be seen as a multi-purpose instrument and we do have a reason to have more and better targeted operations for different purposes and make sure that all information is used for the most justifiable purposes, I see quite a clear justification for making clear rules to entitle Frontex to process information containing personal data as it refers to the alleged traffickers…[959]

The standpoint illustrates quite strikingly how the correlation between data processing, surveillance and "targeted" interventions plays out, not so much from a theoretical point of view, but in the narratives of the concerned agents themselves. Laitinen's statement should further be understood in view of earlier controversies, particularly on Article 11 of the Frontex regulation, which in its initial formulation opened the possibility the agency to operate exchanges of information, without specifying whether the processing of personal data was included or excluded.[960] The vagueness of this provision has been challenged by a number of civil rights organisations. The UK-based Immigration Lawyers Practitioners'

Cooperation at the External Borders of the Member States of the European Union (Frontex)," (Brussels: COM(2010) 61, 2010), 4.

[957] Ilkka Laitinen, "Frontex - Facts and Myths," 2007.

[958] Ilkka Laitinen, "Introduction Talk," 2006.

[959] European Parliament, "Transcript of the Intervention by the Executive Director of Frontex, Mr Ilkka Laitinen, Titled "Transparency and Accountability of the EU Agencies and Bodies"," (Brussels: Committee on Civil Liberties, Justice and Home Affairs workshop on "Access to EU documents after the Lisbon Treaty", 1 June 2010, 2010).

[960] As the initial formulation of Article 11 goes, "[t]he Agency may take all necessary measures to facilitate the exchange of information relevant for its tasks with the Commission and the Member States.

Association (ILPA), for example, pointed out in a 2008 memoir transmitted to the House of Lords' Committee on European Union during this body's investigation of the agency: "Particular attention should be given to whether the institutional and legal framework ensures accountability of FRONTEX on matters of data protection. There is no Data Protection framework for Frontex. Article 11 of Regulation 2007/2004/EC is very much an enabling provision and does not spell out constraints".[961] It has since appeared that the agency was processing personal data, but in the framework of Article 9 of the Frontex regulation (on return cooperation) rather than in relation to Article 11. The services of the directorate general of the Commission in charge of the Frontex *dossier*, DG Home, openly acknowledged this fact during the recent negotiations on the amendment of the Frontex regulation: during the first reading of the regulation's proposed new Article 9 on return operations by the Council's Working Party on Frontiers on 6 April 2010, the Commission "clarified that when coordinating joint return operations Frontex already processes personal data".[962] The issue initially surfaced in April 2009, when the data protection officer of the agency forwarded to the European Data Protection Supervisor a notification for prior checking on the "Collection of names and certain other relevant data of returnees for joint return operations (JRO)". The stated purpose of the collection of personal data by the agency was in particular to have knowledge of the number and identification of returned persons, provide airline companies with a list of passengers, and ascertain the latter's degree of "risk", health status and age. In its opinion of April 2010 (i.e. while the Working Party on Frontiers was proceeding to the first reading of the Commission's proposal for amending the Frontex regulation), the EDPS found the processing lawful but nonetheless pointed out that Article 9 of the Frontex regulation could only serve as a temporary legal basis and called for the adoption of a more specific provision.[963]

Despite this controversy, debates on data processing in the context of the revision of the Frontex regulation have mostly focused on Article 11. The provision included by the Commission that information exchanged by the agency would not include personal data has featured highly in the discussions within the Council's Frontiers Working Party, in its first reading examination on 8 April 2010:[964]

> [Member State delegation] and [Member State delegation] suggested deleting the third sentence and proposed including a provision that will allow limited rights for FRONTEX to process personal data, which it deems necessary for the Agency to perform its tasks. [Member State delegation] suggested that the possibility for FRONTEX, including its Liaison Officers to deal with "personal data" should be provided in several articles. [The French delegation] also suggested deleting the third sentence. […] [Member State delegation] suggested adding a separate Article providing for the possibility for FRONTEX to handle personal data with clear limitations and for specific functions. [Member State delegation] supported by [Member State

[961] House of Lords, "Frontex: The EU External Borders Agency - Report with Evidence," (London: The Stationery House, 9th Report of Session 2007-08, 2008), 110.

[962] Council of the European Union, "Outcome of Proceedings of Working Party on Frontiers/Mixed Committee on 24 March 2010," (Brussels: 8244/10, 2010), 9.

[963] European Data Protection Supervisor, "Opinion on a Notification for Prior Checking Received from the Data Protection Officer of the European Agency for the Management of Operational Cooperation at the External Borders of the European Union (Frontex) Concerning The "Collection of Names and Certain Other Relevant Data of Returnees for Joint Return Operations (Jro)"," (Brussels: Case 2009-0281, 26 April, 2010).

[964] The cited document is only partially available at this time. As such, references to specific Member States (except as far as the French delegation is concerned) have been edited out. In the following quote, the DELETED mention has been replaced by the mention [Member State delegation] in order to improve legibility.

> delegation] suggested also to make a distinction between the processing of personal data relating to staff and other types of personal data.[965]

The key concern underlying the debate in the Frontiers Working Party on the processing of personal data by the agency is however given away in one of the footnoted comments:

> Following a request by [Member State delegation] to clarify the scope of the proposed system for the exchange of information, Cion [the Commission representative] underlined that this Article does not aim at changing FRONTEX mandate and at creating an alternative system to the Schengen information system and that the collection of personal data is not allowed. The Commission indicated that it will return to this issue in the context of information exchange between JHA Agencies.[966]

In other words, the crux of the discussions among Member States representatives over the reinforcement of the dataveillance capacities of the agency has remained parametered by the question of maintaining the exclusivity enjoyed by national border guard authorities over border checks and its corollary, the exclusive access to the SIS. The episode, in this regard, illustrates the controversies between the "Classic" and "Modern" standpoint on security discussed above, and how it results in struggles over surveillance - here, how concerns with territorial control (border checks at the border) are correlated with exclusive access to dataveillance activities, and how this sovereign view on data is opposed from within the field of security professionals, rather from the outside of the field exclusively.

Two aspects of the controversy surrounding the access of Frontex to personal data have now been presented: eagerness, on the one hand, of the agency's management to have access to personal data, concerns, on the other, over the prerogatives of Member State border guard authorities regarding border control and the correlated access to (personal) data. A third aspect played out in the report drafted by the European Parliament's LIBE committee member Simon Busuttil on the Commission proposal. Allowing the agency access to personal data is one of the main modifications introduced by the report. It foresees a new article 11 which would authorise Frontex to process personal data obtained in the course of joint operations, pilot projects or rapid border intervention missions[967]. The position supported in the report reflects the attitude that a number of MEPs have adopted towards Frontex since the agency's inception, and which has resulted in the Parliament repeatedly increasing the already fast-growing budget of the agency at its own initiative. As the report's author, Simon Busuttil, argued in a hearing in front of the House of Lords' Committee on European Union in 2007, "we have no interest in seeing Frontex walk. We want it to run at great speed, and this explains why we have done this".[968] It is also the byproduct of the relations between the European Parliament and the EDPS on matters of privacy and data protection. The European Parliament's report draws, for this specific provision, on an exchange of letters between the rapporteur and the services of the EDPS, which saw the latter welcome the inclusion of provisions on the possibility for Frontex to process personal data.[969] The fact that an

[965] Council of the European Union, "Outcome of Proceedings of Working Party on Frontiers/Mixed Committee on 8 April 2010," (Brussels: 8466/10, 2010), 3.

[966] Ibid.

[967] The data would concern "persons who are suspected on reasonable grounds of involvement of involvement in cross-border activities, in illegal migration activities or human trafficking activities […], persons who are victims of such activities and whose data may lead to the perpetrators of such illegal activities, as well as persons who are subject to return operations in which the Agency is involved.

[968] House of Lords, "Frontex: The EU External Borders Agency - Report with Evidence," 24.

[969] EDPS, "Letter from Peter Hustinx, Supervisor, to Mr Simon Busuttil Mep," (Brussels: PH/KCG/et/D(2010) 1934 C 2010-0056, 3 December, 2010).

organisation in charge of data protection would welcome additional data processing measures is somewhat counter-intuitive. The exchange, however, echoes the controversy ignited with the EDPS' earlier opinion on the Commission proposal, where it criticised, following its previous Prior Check Opinion, the fact that the processing of personal data had been excluded from the scope of the revision of the Frontex regulation:

> The EDPS has doubts about the approach taken by the Commission in the proposed Regulation with regard the issue of processing of personal data by FRONTEX. [It] […] does not clarify what might be the scope of processing of personal data [which it only envisages in relation to Article 11] in other areas of FRONTEX activities […] To explain this with an example, the EDPS wishes to refer to his Prior Check Opinion regarding the preparation and realisation of the JROs, the activity in the context of which FRONTEX informed the EDPS that some processing of personal data might be necessary for the effective execution of the tasks laid down in Article 9 of the FRONTEX Regulation. […] The Commission's reluctance to specify this in the proposed Regulation or to clearly state the date by when it will do so, instead preferring to postpone the matter pending new legal and political circumstances […] raises serious concerns. In the EDPS's view, this approach could lead to an undesirable legal uncertainty and a significant risk of non-compliance with data protection rules and safeguards.[970]

The concern, here, lies with the lawfulness, regularity and regulation of data processing. The EDPS' position, incidentally, does open a discussion we will lead further on in this section, on how groups and organisations that should programmatically oppose the intensification of dataveillance in the name of privacy and data protection - the "privacy advocates", to refer to an influential contribution in the field[971] - relate in practice to the establishment of dataveillance schemes. The controversies surveyed here show, for example, that reticence towards the processing of personal data can in fact follow from preoccupations with sovereignty and exclusive competence from national border guard authorities and Member State representatives, while concerns with data protection can lead to the formalisation of a data processing scheme, rather than its prohibition, in the name of regulation. The drift towards surveillance, and particularly dataveillance, in EU security policies thus does not unfold univocally, nor in a linear fashion: it is fuelled by controversies that result in diversions, subversions, hijackings and so on. The open-ended effects of controversies, in this regard, is a determinant insight for the study of the domains that are considered at face-value as the locations from which opposition to surveillance should spring: ethics, firstly, and privacy and data protection, secondly.

5.4.2 The implications of surveillance and the question of ethics

The second set of controversies about security, surveillance and technology involves the question of ethics. The theme surfaces very strongly in the context of EU sponsored security research schemes, where it is introduced early on. Ethics is the sole headline under which issues related to civil liberties, fundamental freedoms and rights are investigated in the context of the FP7 Security Theme. In the meantime, it is the least endowed domain of the programme, representing 1.09% of the total EU funding for security research after the two

[970] EDPS, "Opinion on the Proposal for a Reguation of the European Parliament and of the Council Amending Council Decision (Ec) No 2007/2004 Establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union (Frontex)," (Brussels: 17 May, 2010), 4.

[971] Bennett, *The Privacy Advocates: Resisting the Spread of Surveillance*.

first calls for applications.[972] Referring only to the amounts explicitly earmarked for research in ethics, however, are misleading, in the sense that the EU's security research schemes - PASR and FP7-ST - have sustained an intense production of prescriptions on the status of security policies and technologies within contemporary European societies outside of the specific projects dedicated to this question. The main programmatic instruments framing the assembling of security and technology – the abovementioned 2004 GoP report, 2006 ESRAB report and 2009 final ESRIF report - have not just focused on the technical dimension of security research, but have consistently correlated security, technology and surveillance in relation to what has been generally termed "societal issues" by the authors of these documents.

Tracing references to ethics thus raises a question as to the exact meaning that is attributed to this latter notion in the context of the assembling of security and technology. The 2004 report from the Group of Personalities on Security Research, firstly, distinguishes ethics from fundamental freedoms, although it acknowledges their association. "[W]e insist, the report goes, that the respect for civil liberties and ethical principles must govern all European research activities".[973] Ethics and civil liberties are further associated as one of the platters in the "balance" between security and freedom. While security is imperative - "it is particularly important to ensure a consistent level of security throughout the Union", the report goes:[974]

> Europe must defend its commitment to a pluralist, open and liberal society. Striking the right balance between security and freedom will be a permanent challenge while respecting the highest ethical principles. Europe's vision of security must therefore embrace a notion of 'Internal Security' that can include a genuine feeling of well being and safety for its citizens, while respecting its values of human rights, democracy, rule of law and fundamental freedoms.[975]

The figure of the "balance" also permeates the final report of ESRAB. In its section dedicated to border security, for example, it suggests that "Europe is at the same time faced with a strategic challenge of how to balance the new security requirements with those required to facilitate legitimate trade and flow of people".[976] In the section on protection against terrorism and organised crime, the report argues that "the mission's requirement for widespread observation, coupled with the fusion of distributed data and the sharing of information requires that technologies, equipments and systems be developed that are in line with European ethical and privacy values".[977] The introductory paragraph of the report's section on security and society notes that:

> security, whilst very important, is just one of the societal values in Europe which must be balanced against others […] The political challenge is, and will continue to be, striking a socially acceptable balance between these different values which will need to take account of variances between countries, circumstances, and the development of threats and their perceptions.[978]

---

[972] Jeandesboz and Ragazzi, "Review of Security Measures in the Research Framework Programme."

[973] European Commission, "Research for a Secure Europe: Report of the Group of Personalities in the Field of Security Research," 12.

[974] Ibid., 11.

[975] Ibid.

[976] ESRAB, "Meeting the Challenge: The European Security Research Agenda," 24.

[977] Ibid., 32.

[978] Ibid., 55.

The section of the report dedicated to "Ethics and justice", meanwhile, specifies further what is understood by ethics in the context of EU sponsored research on security and technology. It takes note of the fact that "[s]ecurity technologies, and the government policies accompanying them, raise many different ethical and legal concerns amongst the European citizens", the strength of which "directly influences public support and acceptance of both government policies and the security technologies themselves".[979] The distinction introduced in the GoP between civil liberties and ethics is maintained. In the first set, issues related to privacy and data protection feature very highly among other fundamental rights. Ethics involve the issue of "value judgements", particularly in "the process [of] assessing the priority of threats and specific targets to be protected".[980] The report exemplifies this point by proposing that "[a] potential ethical concern is the increasing formation of areas of insecurity within Europe (suburbs, poverty-stricken inner cities) and immediately surrounding the EU's external borders".[981] Leaving aside the issue of privacy and data protection for the moment, it appears important to note the further displacement that these prescriptions operate with regard to ethics: they drift from ethics as the framework of values related to civil liberties, to ethics as the conditions under which security, and security through technology, becomes acceptable.

The same reasoning is found in the final ESRIF report tabled in December 2009. Legal and ethical considerations, at the most general level, are framed as the "legitimacy perimeter" of security policies and technologies. The metaphor of the balance is again present, well summarised by the section dedicated to "situation awareness and the role of space":

> It is important to realise that the needs for high levels of protection of possible targets of antagonistic threats (e.g. subway systems) must be balanced against the needs for integrity, privacy and personal freedom of the European citizen. Achieving such a balance is possible by ensuring that the technological research proposed in this report is integrated with ethical and integrity aspects. New technologies will also enable us to ensure that the personal data acquired in preventive security context can only be accessed under strict and enforceable conditions - e.g. by magistrates - and is destroyed as promptly as possible.[982]

A further displacement is sketched out here. While the ESRAB report still asserted that the "balancing" of security and freedom was a political (i.e. human) decision, the ESRIF report suggests that it could be entrusted to technology. References to ethics enable the authors of the report to capture controversies about dataveillance and the generalisation of surveillance, and alternative proposals such as "privacy-by-design" systems. In the meantime, however, ethics remains problematised in terms of acceptability. The prescriptions issued by ESRIF have been elaborated by this body's working group (WG 11) on the "Human and Societal Dynamics of Security".[983] The correlation between research and development in the field of

---

[979] Ibid., 60.

[980] Ibid.

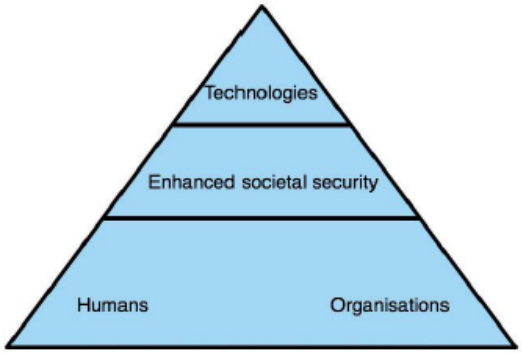
[981] Ibid.

[982] ESRIF, "Esrif Final Report," (Luxembourg: Office for Official Publications of the European Communities, 2009), 155.

[983] Chaired by Liviu Muresan, executive president of the Bucarest- and Brussels-based European Institute for Risk, Security and Communication Management (EURISC Foundation), also executive president of the Euro-Atlantic Council Romania, and former civil servant in various high level offices of the Romanian government (senior adviser to the Prime Minister and the Minister of Interior, High Representative for the Anti-Corruption Initiative of the Stability Pact and Combating Organised Crime Initiative, former Director of the Romanian Agency for the establishment of the SECI Center for Combating Organised Crime). Membership of WG 11 ranges from academia (including the rapporteur, Bengt Sundelius from Uppsala University, sherpa J.Peter Burgess from the Peace Reseach Institute Oslo, Magnus Ranstorp from the Swedish National Defence College, Johann Cas from the Austrian Academy of Science's Institute for Technological Assessment) to international

security and prescriptions on the standing of security policies and technologies in contemporary European societies is explicitly laid out in the group's report, which considers that "[t]echnology can only be part of the effective response to security threats and must be applied in combination with organisational processes and human intervention".[984] In the report, this understanding is translated into the following diagram:

Figure 5.4: Security, technology and society in the ESRIF final report[985]



The main notion knitting together the threads of reflection developed by WG 11, as illustrated in the figure above, is that of "societal security", according to which "[h]uman beings are at the core of security processes".[986] It is premised on the understanding that in the current period "[t]raditional security concerns are combined with revised notions of the consequences of living in Risk Society […] The trans-boundary character of the novel threats of the future will affect both the security challenges faced and our abilities to meet them in effective and legitimate way".[987] References to societal security borrow from both academic sources (Ulrick Beck's *Risk Society*, most prominently)[988] and the "Modern" narrative on (in)security we have already evoked. As a set of prescriptions regarding the implications of security technologies, then, societal security as presented in the ESRIF final report starts from the affirmation of new threats and risks, and considers how responses to such novel developments can be made legitimate. The report of ESRIF's WG 11 formulates a number of considerations associated with the proper functioning of democratic societies, but substantial comments are associated with two areas: the first one is privacy and data protection, and the second ethics. Mirroring the suggestions developed in ESRAB, ethics is framed in terms of trust and particularly of the trust placed by citizens in the technologies and organisations that purport to protect them: "The security of citizens is increasingly dependent upon their own trust in the people and technologies supposed to assure it. As the complexity of technologically based security systems grows and the ability of citizens to understand and control the technologies that surround them weakens, trust in their ordered functioning and the dependability of their operators becomes crucial".[989]

---

organizations (featuring John Holmes, Under-Secretary-General and Emergency Relief Coordinator, UN), and including think tanks (Sadhbh McCarthy, Center for Irish and European Security, Eva-Karin Olsson, CRISMART) and research organisations (Kerstin Castenfors, Norwegian organisation for applied research FOI).

[984] ESRIF, "Esrif Final Report," 229.

[985] Source: Ibid., 230.

[986] Ibid., 243.

[987] Ibid., 229.

[988] A further hypothesis is that the notion also draws from the discussions on societal security in the field of security studies during the 1990s, as well as from the concept of human security with which it bears strong resemblances.

[989] ESRIF, "Esrif Final Report," 242.

The analysis of the programmatic instruments that assemble security and technology enables us to outline some of the key components of the ethics put together in the framework of EU security research. A twofold displacement takes place in the different documents examined above. On the one hand, references to civil liberties are progressively narrowed down to the question of privacy and data protection, which are the only domains that receive fairly substantial attention in the ESRIF final report. On the other, the boundaries of what is understood by ethics are enlarged to encompass all considerations related to the "societal" effects of security technologies. A specific angle is furthermore privileged: taking the assumption of "new threats" as a point of departure, ethics is correlated to the question of the acceptability of security policies and technologies by EU citizens, and to the order of priority to be given to different types of threats. Ethics, then, is framed in terms of securing consent to surveillance measures and technologies, and fostering "trust" among citizens regarding the fact that they are well governed. "Good governance" is one of the key domains examined by ESRIF's WG 11, which defines the notion in terms of order, as "the well ordered flow of information, authority and public resources".[990] Ethics is further associated with allegedly "soft" modes of regulation for security policies and technologies, excluding legal instruments, such as codes of conduct, best practices guidelines and so forth.

Just as in the case of security, however, this framing of ethics has generated a number of controversies. References to ethics, firstly, have been used as a springboard for the two projects funded under the first two calls for application of the FP7-ST (DETECTER and INEX) to develop research on the impact of security technologies beyond the focus on privacy/data protection and ethics as acceptability and trust. DETECTER takes human rights as an explicit starting point for the ethical examination of security technologies. It uses different techniques, including a blog, to monitor this impact and displace the focus to include the "moral implications" of security technologies and the question of democratic oversight. Both DETECTER and INEX displace the "object" of investigation, which is limited in the programmatic instruments of security research to EU citizens, to include third country nationals. DETECTER features for example a work package (WP 05) on the use of technologies for the pre-entry screening of migrants, while INEX takes as its overall focus the shifting boundaries of internal and external security. References to ethics, secondly, have been occasionally used as a means of regulating the practices involved in some security research projects. The best known case, here, involves the INDECT project. It rose to public notoriety due to the circulation on video-sharing platforms of a short movie aimed at demonstrating the capacity of the algorithms developed by the INDECT consortium to identify and track suspects using aggregated data sources, including CCTV. INDECT was the first FP7-ST scheme to be subjected to an ethical audit by the European Commission, supported by researchers from other FP7 consortia, which led among others to the establishment of an Ethics Board supervising the research activities of the project (for further details on the ethical considerations of INDECT project partners.[991]
Controversies have also emerged from outside the security research framework. One example is the attribution of the French Big Brother Awards in the "Novlang" category to the FP6 project HUMABIO (*Human Monitoring and Authentication using Biodynamic Indicators and Behavioural Analysis*) in 2009. The Big Brother Awards are an initiative of the UK branch of the NGO Privacy International, which has been taken up in a dozen of countries since its inception in 1998. The French Big Brother Awards have been attributed since 2000, and featured for two years (2003-2004) a "European Union" category, which distinguished the

[990] Ibid., 230.

[991] Cf. INDECT, "Ethical Issues," (INDECT Consortium: Deliverable D05.1, 17 August, 2010); INDECT, "Ethical Issues," (INDECT Consortium: Deliverable D06, 31 March, 2011).

JHA Council, in 2002 for the measures it had adopted in response to 9/11, and in 2003 for its decision on the biometric passport. The attribution of an award to HUMABIO in 2009 reflects the tactics of "naming and shaming" which are shared by a number of other organisations in controversies on European security research. A good illustration here is also the work undertaken by researchers from the civil liberties organisation Statewatch in relation with the Amsterdam-based Transnational Institute. Statewatch and TNI provided the first documented investigations of the EU's security research efforts.[992] Their reports challenge the assembling of security and technology by drawing on the critique of totalitarianism inspired by some interpretations of George Orwell, on the one hand, and by invoking the figure of the "military-industrial complex", a notion initially coined by American sociologist C. Wright Mills, renamed the "security-industrial complex" after the terminology coined by *Washington Post* journalist and Center for Investigative Reporting associate Robert O'Harrow to qualify the relation between private sector contractors and the Department of Homeland Security in the wake of the Patriot Act.[993]

The effects of these controversies are unclear at this stage. What is notable, however, is the way in which concerns with freedom, translated into concerns with a specific understanding of ethics, have been incorporated into the assembling of security and technology. Going back to a point we made in the introduction to this chapter, for example, the very research conducted within the SAPIENT consortium, although based on preoccupations with issues of privacy and data protection, contributes to reinforcing the "object" of smart surveillance

5.4.3 Privacy advocates versus surveillance advocates? Controversies about privacy and data protection

The last set of controversies to examine involves the right to privacy and the right to data protection. As argued in Chapter 4, the two rights are not synonymous from a legal point of view. They also authorise different operations. A certain number of practices interfering with the autonomy of the person, whether public or private actors enact them, can be prohibited in the name of privacy. Data protection, on the other hand, channels and regulates the processing of personal data. The protection thus conferred can involve other rights, such as freedom of speech or freedom of religion.[994] Chapter 4 has highlighted both the positions of data protection authorities and of various groups involved in contesting surveillance measures by referring to the right to privacy and the right to data protection. To frame these contests in terms of a confrontation between privacy advocates and actors, which for lack of a better term we would have to call surveillance advocates, would result in limiting the scope of the analysis. In line with what we have developed in this chapter and in the deliverable, it appears more interesting to focus on how different practices and understandings of the right to privacy and the right to data protection are brought to bear in different controversies, and variations occur in the scope of principles and rights brought under references to privacy and data protection varies.

The first point to stress, in this respect, is that concerns with the right to privacy and the right to data protection are a recurrent item in EU programmatic documents on security, surveillance and technology. A good example here is the vision of the "future of European

[992] Hayes, "Arming Big Brother: The Eu's Security Research Programme."; Hayes, "Neoconopticon: The EU Security-Industrial Complex."

[993] Robert O'Harrow, *No Place to Hide* (New York: Free Press, 2005).

[994] See for instance the Moon case involving the SIS discussed in Evelien Brouwer, "The Other Side of Moon: The Schengen Information System and Human Rights: A Task for National Courts," (Brussels: CEPS, Working Document No. 288, 2008).

home affairs" outlined by the abovementioned report of the Future Group, composed by representatives of national ministries of Interior and the European Commission's DG JLS. Privacy, together with freedom and security, is one of the three tenets of the framework outlined by the report, which encompasses under privacy "private life as well as data protection".[995] The report's section on "Public security, privacy and technology, furthermore, illustrates this particular group of spokespersons' take on the issue:

> Balancing citizens' expectations of privacy against their expectations of proactive protection is not a new dilemma for public security organisations, but it is taking on an ever more acute form. In the "digital tsunami" environment the traditional measures to protect privacy will become less and less effective unless appropriate technological measures are used as an essential complement to legal means. In order to achieve a sufficient level of protection, "privacy-enhancing technologies" are absolutely essential to guarantee civil and political rights in the age of cyberspace […] Information is the key to protecting the public and in an increasingly connected world in which public security organisations will have access to almost limitless amounts of potentially useful information. This is a challenge as well as an opportunity – public security organisations will need to transform the way they work if they are to master this data tsunami and turn it into intelligence that produces safe, open and resilient communities. The key to effectiveness will be using technology to connect the capabilities of a multitude of stakeholders and ensure the right information gets to the right person in the form they are best able to use.[996]

The report subsequently expands on priorities for Member State security agencies, bodies and services, including investment in "automated data analysis", the building of "converged platforms" (i.e. of computerised networks which are not centralised but communicating with each other) and the establishment of a "European Security Tool Pool" which would enable these agencies, bodies and services to share experience of field tested and functional technologies. Two comments can be made on the excerpt above. On the one hand, the report translates the question of the relation between security, surveillance, technology and fundamental rights into the figure of the "balance" that has already been discussed. On the other, it illustrates the kind of operations that this figure can authorise. Indeed, the issues dealt under the heading of privacy, here, are all related to security, a technique that has been noted in relation to other EU programmatic documents – e.g. the Hague Programme.[997] Concerns with fundamental rights resurface later in the report, as the last requirement related to the development of an EU "Information Management Strategy" (hereafter EU-IMS) with the aim to "facilitate the quick, efficient and cost-effective means for exchanging data",[998] but under the heading of data protection rather than privacy. The facilitation of data exchanges refers to the principle of availability (PoA), formally introduced with the Hague programme, and according to which information related to a specific case or individual available to national security agencies, bodies and services in one Member State should also be made available to agencies, bodies and services with an equivalent remit in another.[999] The Future Group's report highlights that "an adequate normative framework as well as specific provisions on

---

[995] Council of the European Union, "Freedom, Security, Privacy - European Home Affairs in an Open World - Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy ("The Future Group")," 26.

[996] Ibid., 64.

[997] Bigo, "Delivering Security and Liberty? The Reframing of Freedom When Associated with Security."

[998] Council of the European Union, "Freedom, Security, Privacy - European Home Affairs in an Open World - Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy ("The Future Group")," 67.

[999] Didier Bigo, "The Principle of Availability of Information," in *Controlling Security*, ed. Didier Bigo and Anastassia Tsoukala (Paris: L'Harmattan, 2006).

data protection are essential requirements for the implementation of the PoA" but does not make reference to the right to data protection as much as to the need for citizens to understand data processing:

> Ensuring greater public understanding of the benefits of data sharing between Member States should be a priority. The [Information management] strategy should include a commitment to make clear to European Union citizens how information will be processed and protected, on the basis of proportionality and necessity.[1000]

Data protection, here, is framed as a condition for greater acceptability of the relation between data processing and protection against threats, rather than as a modality for protecting fundamental rights. Tellingly, in this regard, EU citizens are the only entity of concern singled out in relation to data protection in the report – whereas the majority of EU measures related to data processing schemes, such as Eurodac, the SIS or the VIS, focus primarily on foreigners.

The EU Information Management Strategy, foreseen by the Future Group's report and adopted by the Council in November 2009, further illustrates the take of EU Ministries of the Interior on the right to privacy and the right to data protection.[1001] The first point to note, here, is that privacy is almost entirely absent from the document. References to the notion do not relate to the right to privacy, but evoke, rather, "citizens' expectations of privacy" (p. 5) and "personal privacy" (p. 10-11). The strategy, on the other hand, features a full subsection on data protection. It specifies that

> [c]ooperation with a view to ensuring the EU internal security places high demands on data protection including data security. Personal privacy as well as business security have to be ensured, while providing for business needs to use and share information.
> A high level of security will protect business interests as well as citizens' private lives, without reducing the availability of information, so that correct information is available to authorised users in a traceable way, when needed and permitted by existing legislation. Adequate use of modern technologies, but also adaptation of business processes and measures to implement data protection, facilitate this. Enhanced trust in these areas between competent authorities is an important step towards an attitude of data-sharing by default.[1002]

The EU-IMS, in this regard, presents the same translation than the report of the Future Group. The focus is on one specific principle of data protection, namely data security. Data protection here is framed literally, as referring to the protection of the data that has been collected, through the devising of secure data processing architectures. Another dimension of this particular problematisation of data protection is the objective of targeted collection:

> …data collection must be well targeted, in order to protect personal privacy as well as to avoid information overflow for the competent authorities and facilitate efficient control over the information.[1003]

[1000] Council of the European Union, "Freedom, Security, Privacy - European Home Affairs in an Open World - Report of the Informal High Level Advisory Group on the Future of European Home Affairs Policy ("The Future Group")," 70.

[1001] Council of the European Union, "Draft Council Conclusions on an Information Management Strategy for EU Internal Security."

[1002] Ibid., 10.

[1003] Ibid.

Data protection, then, is framed both as data security and information control, which are two aspects of data protection law, but not the only ones, as shown in Chapter 3.

This view of the right to privacy and the right to data protection has been at the heart of a number of controversies in the European governmental arenas. In their own forward-looking report, tabled in 2009, the Article 29 Working Party and the Working Party on Police and Justice[1004] highlight a number of problematic trends in data processing practices by EU and Member States security agencies, bodies and services. These include the collection and processing of data from an increasingly large number of persons, the reliance on techniques of profiling, correlation and pattern recognition, the multiplication of data sources, the lack of purpose limitation and the accelerated circulation of personal data between a wider number of agencies, bodies and services through technical measures such as the interoperability of data systems and policy measures such as the application of the principle of availability. Against this background, the position of the data protection authorities for which Article 29 WP and the WPPJ take responsibility as spokespersons is not one of prohibition. Data protection is framed as a set of principles and safeguards to be applied *to* data processing operations, but not against them. This, incidentally, is a key aspect of the view adopted by data protection authorities with regard to data processing, and relates to how legal practice has shaped data protection in relation to privacy. The example of the EDPS' position on the revision of the Frontex Regulation, provided in subsection 5.3.1 above is a clear illustration of this stance. In the "Future of Privacy" report, the Article 29 WP and the WPPJ do not challenge the principle of data processing for security purposes as such, but essentially frame the issue as one of regulation. "The main principles of data protection", they argue, "are still valid despite the new technologies and globalisation", but "[t]he level of data protection in the EU can benefit from a better application of the existing data protection principles in practice" (p. 2). One of the key proposals developed in their report, in this regard, is the generalisation of "privacy-by-design", which aims at incorporating data protection safeguards into the technologies involved in data processing themselves (p. 13-15). According to this principle, information and communication technologies "should not only maintain security [of data] but also should be designed and constructed in a way to avoid or minimize the amount of personal data processed" (p. 13). Privacy-by-design, from an analytical point of view, echoes the framing of data processing in the EU-IMS insofar as it frames the issue of security, surveillance and technology in terms of targeting – to "minimise" (in the words of the "Future of Privacy" report) data processing, on the one hand, and to avoid information overflow, on the other. The controversy emerges, however, from the difference in the treatment of so-called "data-subjects" – as persons (including foreigners) to be empowered, in the view of the Article 29 WP and the WPPJ, or as EU citizens to be reassured and whose acceptance is to be secured, in the view of the EU-IMS.

This brief overview of some controversies on security, surveillance and technology in relation to privacy and data protection is not exhaustive. It does point out, however, to the fact that the right to privacy and the right to data protection are less the basis of a definitive opposition than it could be expected. Controversies on surveillance and fundamental rights in the European governmental arenas, in this regard, are not about the prohibition of data processing. They are parameterised, rather, by the degree of regulation that should be exercised on surveillance practices and the focus of such a regulation – the provision of information to security agencies, bodies and services, on the one hand, the provision of guarantees and safeguards to the persons whose data is being processed, on the other. In both

[1004] See Chapter 3, subsection 3.3.1, for a full analysis.

cases, however, the discussion is on the degree of targeting involved in such dataveillance activities – in other words, on how these activities can be made "smarter".

5.5 CONCLUSIONS: SMART SURVEILLANCE AND ITS IMPLICATIONS FOR FREEDOM

The purpose of this chapter was to examine the processes through which "smart surveillance" has become a relevant "policy object" in EU security policies. We have undertaken an examination of the assembling of security and technology, and highlighted the heterogeneity of this assembling through an analysis of the development of EU-sponsored activities in the field of security research. This has led us to suggest that emerging references to "smart surveillance" should be interpreted in the light of multiple controversies over the relation between security, surveillance and technology which do not only involve technical discussions on cost-efficiency and feasibility, but also involve judgements about which contemporary developments are considered to be threatening, how they should be met, and with which implications.

Some of the key parameters of these controversies include the issue of "multipurpose" technologies which are claimed to offer the possibility of meeting different threats through a single modality, the issue of acceptability of surveillance by the persons placed under surveillance (or rather, by EU citizens since the views of foreigners, particularly those falling under visa requirements, are only considered at the margin), and the question of targeting. It is at the point where these controversies coalesce that the "smart surveillance" systems examined so far in the deliverable come into the picture. The point, here, is that two understandings of "smartness" in surveillance are currently emerging: one which envisages smartness as the technical possibility in a culture of "data-sharing by default" to sift through massive amounts of personal data to detect persons deemed to be a risk, and the other which considers smartness as the technical possibility to "minimise" the impact of surveillance on fundamental freedoms and rights.

To envisage these two directions as polar opposites, however, would be inaccurate: they both involve a discussion on the regulation of the use of personal data. They nonetheless differ on their framing of the subject who is to be watched "smartly". This subject, on the one hand, is the obedient citizen whose acceptance is to be secured and who is to be reassured about the use of its personal data by security agencies, bodies and services. It is, on the other, the pragmatist who tolerates surveillance insofar as guarantees and safeguards exist. These figures, of course, are also translations, whereby specific actors are appointed as spokespersons for the persons who are concerned firsthand by surveillance. In the meantime, it is central to insist upon the data subject, rather than technical systems, as the starting point for the reflection in the next stages of the work of SAPIENT on privacy impact assessment methodologies.