Project acronym:	IRISS
Project title:	Increasing Resilience in Surveillance Societies
Project number:	290492
Programme:	FP7-SSH-2011-2
Objective:	To investigate societal effects of different surveillance practices from a multi-disciplinary social science and legal perspective.
Contract type:	Small or medium-scale focused research project
Start date of project:	01 February 2012
Duration:	36 months

Deliverable D2.2: The Political Perspective

A report presenting a review of the key features raised by the political perspectives of surveillance and democracy

Coordinator:	The University of Edinburgh (UEdin)
Dissemination level:	PU
Deliverable type:	Report
Version:	1
Submission date:	31 January, 2013

	Lead	Contributors
Overview and overall editor	Charles Raab, University of Edinburgh (UEdin)	Richard Jones, University of Edinburgh (UEdin)
The induction of fear by the media	Daniel Fischer, Universität der Bundeswehr München (UNIBW)	Wolfgang Bonss, Universität der Bundeswehr München (UNIBW)
Fears shaping the use of technologies	Daniel Fischer, Universität der Bundeswehr München (UNIBW)	Wolfgang Bonss, Universität der Bundeswehr München (UNIBW)
Societal resilience to terrorist and other threats	Eric Lastic, Comenius University Bratislava (COMENIUS)	
Experiencing surveillance in different democratic contexts, including new democracies and former repressive regimes	Ivan Szekely, Eotvos Karoly Policy Institute (EKINT)	Beatrix Vissy, Eotvos Karoly Policy Institute (EKINT)
The political effects of fear and insecurity	Gemma Galdon Clavell, University of Barcelona (UB)	
Policy-making and surveillance	William Webster, University of Stirling (STIR); Charles Raab, University of Edinburgh (UEdin)	Charles Leleux, University of Stirling (STIR); Beatrix Vissy, Eotvos Karoly Policy Institute (EKINT)
Accountability	Charles Raab, University of Edinburgh (UEdin)	
Transparency	Ivan Szekely, Eotvos Karoly Policy Institute (EKINT)	Beatrix Vissy, Eotvos Karoly Policy Institute (EKINT)
Rights, freedoms and the rule of law	Ivan Szekely, Eotvos Karoly Policy Institute (EKINT); Paul De Hert, Vrije Universiteit Brussel (VUB)	Antonella Galetta, Vrije Universiteit Brussel (VUB)
The governance of surveillance	Charles Raab, University of Edinburgh (UEdin)	
Conclusions about the political perspective	Charles Raab, University of Edinburgh (UEdin)	

IRISS WORK PACKAGE 2

DELIVERABLE D2.2: THE POLITICAL PERSPECTIVE

Contents

EXECUTIVE SUMMARY: THE POLITICAL PERSPECTIVE

Task Description

This Task will review the key contributions to knowledge emerging from political (including political science and policy studies) perspectives of surveillance and democracy. Included within this perspective are approaches which consider changes in democratic values, such as accountability, transparency, equality, the rule of law, rights and freedoms, those which consider changes in democratic policy-making practices and procedures, and how these have changed over time in different democratic settings.

Overview

This Task considers what the literature on surveillance has to say with regard to several closely related issues that are highly relevant to an understanding of social and political effects. In Chapter 1, we start with a discussion of fear and insecurity as powerful forces – often encouraged by the mass media – underlying the demand for an intensification of surveillance. As the phenomenon of fear plays a part in social and political control, we highlight the crucial role of the mass media in inculcating and communicating fear through its narratives that contribute to 'moral panics', the creation of 'folk devils', and the amplification of deviance. We include an account of the way in which the climate of fear, in turn, serves to shape the technologies of surveillance and the public demand for such tools in the 'risk society'. We then consider the resilience of societies in the face of terrorist and other threats, posing several questions that open up important dimensions for further investigation, before looking extensively at the experience of surveillance in countries recently emerging from the control of repressive, non-democratic regimes and moving towards the democratic end of the spectrum of political systems. We finally highlight the distortions of democratic debate and decision-making brought about by the climate of fear and the surveillance that it sustains.

We subscribe to the view that surveillance can – albeit with difficulty, and with considerable variation across jurisdictions, levels of jurisdiction, and types of surveillance – be brought within the limits expected in democratic, accountable political systems governed by the rule of law. In reversing the discussion to explore this view, Chapter 2 therefore deals with surveillance as a tool that is subject to regulation, limitation and control. We examine policy-making for surveillance, both in terms of putting surveillance on a legitimate footing and keeping it in bounds through the actions of political and governmental systems. Our discussion of policy-making is illustrated with the case of data retention, a policy subject that has been greatly controversial in the EU and between it and third countries in recent years. We investigate accountability and transparency as central norms of democratic, non-authoritarian political systems, norms that also play their part in the control of surveillance whether the latter is deployed by organisations in the public or private sector. Accountability is one method of keeping surveillance and its users in check, but the discussion reveals current deficiencies in accountability practices in the context of data protection. Transparency is another important check because it scrutinises the use of power in a democracy and acts as a vehicle for public participation in debates. The relationship of mutual dependence between transparency

and privacy is explored at some length, before the need for transparency in a democracy is discussed in terms of factors that inhibit and promote it, and some transparency-based privacy solutions are canvassed. The rule of law as a pillar of democratic constitutional states, and the position of rights and freedoms as criteria for evaluating surveillance, are also discussed, while the governance of surveillance is described in terms of the repertory of instruments and actors that expand the possibilities beyond the enactment, implementation and adjudication of statutory law or other legal provisions. Moving on, the governance of surveillance is given an overview in terms of the networks of state and societal actors – going beyond government itself – that are involved in regulating surveillance practices and protecting privacy through the use of interrelated regulatory instruments.

Details of the main subject areas reviewed by the Task Partners

The media are implicated in the surveillance process by making crime newsworthy, by amplifying fears, and by constructing 'folk devils' and 'moral panics', although such imputations in the literature should be regarded with circumspection. Nevertheless, the media do play a large part in shaping attitudes towards dangers and the dangerous, and in contributing to a climate in which surveillance, through the use of a variety of technologies, seems an attractive solution in what criminologists and others have called a 'risk society'. Public insecurity, in turn, is said to inhibit and distort policy debate and decision-making by promoting what is politically popular. This promotion brushes aside a fuller evaluation of the side-effects and economic drawbacks which might otherwise suggest that solutions to crime, terrorism, and other problems can be addressed by alternative strategies and policies that do not necessarily involve intrusive surveillance. How to deal with risk is a subject for considering the relationship between resilience and prevention and precaution, and this question is aired with reference to literature on individual resilience in the face of real or perceived threats. Important research questions arise from this.

Several pages are devoted to an investigation of the experience of surveillance in different democratic contexts that include former repressive regimes and the new democracies that have succeeded them in the former "Soviet Bloc" countries as well as in the former autocratic regimes in Southern Europe. The role of state-controlled surveillance organisations is discussed, as well as the particular circumstances and problems of dealing with the surveillance and secrecy legacies in these new democracies. Public attitudes of fear and distrust, and appreciation of rights and freedoms, have been powerfully shaped by living under these non-democratic regimes, and there remain many unanswered questions about how the different successor systems, and their populations, will deal with the continuing reality of surveillance in the midst of their democratising efforts.

One of the political effects of fear and insecurity even in 'mature' democracies' is the way they distort debate and political decision-making towards reactive, ill-considered policies and measures that overlook unwanted side-effects, tend to ignore contradictory evidence of the efficacy of policies, and brush aside considerations of right and liberties. On a broader canvas, understanding the political perspective involves looking at policy-making and surveillance in terms of the dispersal of surveillance policies over a range of separate domains and settings (e.g., education

and transport), policy idioms, and jurisdictions, and embedded in various practices, including the delivery of public services, e-government, and many others. Data retention is not normally thought of as a form of surveillance because it is a non-visual, non-real time, empirically unnoticeable form of observation and control of citizens. It is pervasive, involving both the public and private sectors in a relationship that requires a flow of information that blurs the boundaries of responsibility for posing dangers to privacy. We discuss data retention as a case in the study of surveillance policy. Data retention emerged on the EU policy agenda as part of counter-terrorism efforts, resulting in the Data Retention Directive of 2006. There are several critical perceptions of data retention in different democratic contexts. Member States regard it as valuable or indispensable, but little statistical or other evidence exists for such conclusions to be reached; thus they are political rather than evidence-based, and some evidence supports the opposite case. Data retention is seen as undermining democracy and a free society by eroding the rights to privacy and anonymity, the presumption of innocence, and social confidence. Some survey evidence shows that data retention chills social and political relations and practices among citizens, and on freedoms. Some Member State judicial authorities have ruled data retention unconstitutional. Cost-benefit analyses have raised doubts about efficiency and economic benefits of data retention.

Looking at ways of regulating, limiting and controlling surveillance, the discussion then dwells at some length and in depth on the importance of the accountability of surveillance in a democratic society in the instance of data protection, in which accountability is being heavily promoted as a regulatory strategy by the EU and the private sector, especially following major data losses and breaches. The argument is that, while the development of accountability as part of information governance is a good step, it confuses responsibility for actions and performances of functions (e.g., surveillance) with answerability for these functions through publicly available accounts, or 'stories' that could be challenged. Accountability in this sense would be consistent with other areas of democratic political practice. It bears a close relationship with transparency, which is also discussed at length and in several dimensions as an attribute of a democratic polity promoting public debate and participation. The relationship between privacy and transparency is highly important, and is argued to be one of interdependence and complementarity. The exercise of privacy rights is contingent upon the transparency of surveillance practices, and the success of transparency mechanisms depends on the cognitive, social and legal status of the audience for the available information.

Moving on to consider the surveillance in relation to rights, freedoms and the rule of law, we point out that the rule of law has formal and substantive dimensions, respectively connoting rule by law, legislative processes, and consent, on the one hand, and individual rights, justice and the right to dignity, and substantive equality of welfare, on the other. Privacy and data protection are directly implicated in all of this, with privacy as a tool of opacity and data protection as a tool of transparency. The European Court of Human Rights has struggled to reconcile surveillance with democracy by means of interpretations of the rule of law in specific cases. This discussion of law, rights and freedoms leads to an analysis of the broader governance of surveillance through a range of instruments of which the legal order and the rule of law are not the only ones currently experienced or capable of further development.

‘Surveillance policy’ as such is elusive and not singular: discerning its content is not straightforward, and understanding the processes through which it is made and implemented requires complex analysis, as the discussion of governance then shows. The ubiquity and variety of surveillance technologies and practices are governed – albeit with limited and variable success – by regimes at various jurisdictional levels (e.g., local, national, regional, global) and with various regulatory tools. Among these are laws; regulatory bodies such as data protection authorities; codes of practice; technological instruments such as privacy-enhancing technologies, privacy by design, encryption, identity assurance systems using anonymity; and the promotion of greater public awareness so that they may safeguard their own privacy. The regulatory landscape has shifted in many respects towards an interest in newer instruments that might be able to cope better with new contexts – the online and social-networking environment, for instance – than can more traditional, law-based instruments, although the latter remain indispensable. There is also a wide range of policy actors, in which formal ‘policy-makers’ and regulators are not alone. Whether or not the governance of surveillance is, or can be, carried out by coherent, well-integrated, and strategically deployed actors, tools, and principles is a crucial question.

Key themes and emergent findings

The discussions outlined above point towards several provisional themes and findings:

a. surveillance practices of all kinds impinge on a large range of rights, freedoms, liberties, and social and political relationships and processes that affect the nature and texture of life in democratic societies and political systems;

b. public attitudes, perceptions, fears, expectations and demands are shaped by many forces, among which the mass media are one of the most powerful, tending towards a particular appreciation of surveillance, its technologies, and its role in reducing threats and the level of fear;

c. social insecurity feeds policy demands for surveillance that tend to limit genuine debate and to ignore the disadvantages and externalities of making life safer and more secure through surveillance, and societal resilience or, on the other hand, precautionary anticipation of threats, are at issue in these processes;

d. the accountability and transparency of surveillance, and the rule of law, are essential in a democratic society, and need to be improved and made potent in order to limit surveillance;

e. the governance of surveillance, and surveillance policy-making, are highly complex and sometimes ephemeral processes that need to be comprehended and rationalised if surveillance is to be regulated in accordance with democratic values.

Conclusion

This Task has something in common with others in IRISS, although it introduces new perspectives and avenues of analysis, and approaches fresh topics that bear upon our understanding of the political dimensions of surveillance and its regulation. Empirical evidence is often at a premium, however, when assertions are made about the benefits or disadvantages of surveillance to the experience of living in democratic society. Nevertheless, the themes identified above provide ample scope for further theoretical work and empirical research oriented towards practical improvement in the resilience of democratic societies faced both with many threats of criminal and terrorist behaviour, and with the dangers that accompany the surveillance tools employed to counter these.

1. CHAPTER 1: SURVEILLANCE AS A TOOL FOR SOCIAL AND POLITICAL CONTROL

1.1 THE INDUCTION OF FEAR BY THE MEDIA

In this section and the next, attention is given to the phenomenon of fear, which provides an important context within which surveillance plays a part in social and political control. Surveillance practices both contribute to the construction of fear and offer themselves as tools for allaying it. Fear is powerfully communicated and disseminated through the media. First, we discuss the part played by the media in inducing fear and in identifying and constructing the subjects, objects, and processes on which surveillance attention may be focused. In the next section of Task 2.2, we look at the way in which the use of surveillance technologies is shaped through fear-shaping narratives.

We begin by looking at a powerful generator of political activity in the field of surveillance – fear – and how public moods and demands are shaped by media treatments of social and political events and developments. Media discourse serves to create a climate in which surveillance may be seen as a desirable and appropriate response for controlling certain phenomena or behaviour, or at least for allaying the fear that such "distortions" of social life as crime, disorder or terrorism are contrary to valued norms and practices of civilised society and public order that need to be restored or reinforced. On the other hand, surveillance itself can contribute to a climate of fear. This is because surveillance devices and practices may leave people uncertain about their safety because the very "need" for, and ubiquity of, surveillance conveys the impression that they live in dangerous times or places, at least until specific applications of surveillance are normalised and routinised, as they are, for example, in the transport systems of most EU countries. In policy processes, this fear, perception of danger, and appreciation of desirable safety and security systems may become translated into popular expectation of political and governmental action. Political and governmental actors find it hard to go against the grain of this pressure and desire, thus fuelling the demand for legislative or administrative measures of surveillance and restricting the force that regulatory measures, and the human rights or civil liberties that such measures uphold, might bring to the policy table.

1.1.1 The media and fear in modern society

This subsection deals with theoretical reflection on the connection between media consumption and fear, which has been the subject of mainly criminological research up to now. In the interests of clarity we illustrate briefly the current state of research as a communication process; however, some relevant observations must be made about this.

First, "the media" are mainly treated as one homogeneous actor, although there have been massive changes in the media landscape over the past decades, as we point out in a later subsection. In the classic surveys on the connection between crime, news, and fear, the prevailing question was about the extent to which there are different effects of media consumption depending on whether it is print media (daily

newspaper or journal), radio, or television (both local and national).[1] Today's media landscape, however, can no longer be described as an oligopolistic constellation with only a few well known actors offering all of the information. There are an enormous, and global, number of information sources covering all of political, cultural, economic life. Another massive difference lies in the fact that information sources are no longer restricted to national borders: people today can easily read, watch and listen to media information from all over the world, getting different perspectives on a subject.[2] A last point is that the differentiation between text, audio, and visual content can no longer be maintained if one considers news sites on the contemporary Internet, where all forms of media are jointly used.[3]

Second, the role of fear is, as Hankiss claims, "much neglected in the social sciences": it does receive "serious attention in philosophy, theology and psychiatry, less in anthropology and social psychology, and least of all in sociology".[4] As a result of this under-theorisation of fear, empirical research on risk and uncertainty increases. Furedi tries to sum up the contemporary condition in contrast to the "age of anxiety",[5] a label given to the 20th century by some authors.[6] The prevailing "culture of fear"[7] is however characterised by the construction of a multiplicity of specific objects of fears (crime, disease, poverty, and so on), which in the short run gives (risk-averse or -accepting) options for action. In that respect, asking how the "induction of fear by the media" works, one has to face questions of risk and action-taking as well. It is about constructing frightening perceptions of a certain situation, but also about connecting demands for collective (political) or individual action to it. The broad field of "crime" or "deviant behaviour", which is the focus of this section, has served as a source of good examples of examining this process at work.[8]

A general consensus among researchers concerns the fact, according to Young, that "in our extremely socially segregated society", information about deviant behaviour comes almost exclusively from the media: "Direct experience of individuals with

[1] See for example Altheide, David, "The News Media, the Problem Frame, and the Production of Fear", *The Sociological Quarterly*, Vol. 38 No. 4, 1997, pp. 647-668, showing the importance of TV News for the perception of nationwide problems; see also Chaddee, Dick and Jason Ditton, "Fear of crime and the media: Assessing the lack of relationship", *Crime Media Culture*, Vol. 1, 2005, pp: 322-331.

[2] Criminological research has also tried to analyse differences in the reception of certain forms of media among people. For those audience effects see for example: Banks, Mark, "Spaces of (in)security: Media and fear of crime in a local context", *Crime Media Culture*, Vol. 1, 2005, pp.169-187; Chiricos, Ted, Sarah Eschholz and Marc Gertz, "Crime, News and Fear of Crime: Toward an Identification of Audience Effects", *Social Problems*, Vol. 44, No. 3, 1997, pp. 342-357.

[3] McRobbie, Angela, and Sarah L. Thornton, "Rethinking 'Moral Panic' for Multi-Mediated Social Worlds", *British Journal of Sociology*, Vol. 46, No.4, 1995, pp. 559-574. They have aimed at theorising the "multi-mediated social world" in this respect.

[4] Hankiss, Elemér,: *Fears And Symbols; An Introduction to the Study of Western Civilisation*, Central European Press, Budapest, 2001, p. 14.

[5] May, Rollo, *The Meaning of Anxiety*, The Ronald Press Company, New York, NY, 1950.

[6] Furedi, Frank, "The only thing we have to fear is the ‚culture of fear' itself", 2007, Available on: http://www.spiked-online.com/index.php?/site/article/3053/

[7] Furedi, Frank, *Culture of Fear. Risk-Taking and the Morality of Low Expectation, Cassell*, London, 2006.

[8] Fear of "disease" is another good example; see Clarke, Juanne N., Everest, Michelle M. (2006): "Cancer in the Mass Media: Fear, uncertainty and the medical model", in: *Social Science and Medicine*, Vol. 62, 2006, pp. 2951-2600.

behaviour different from our own conventions and values is rare." [9] Grupp speaks of a shift from a "fearsome life towards a life with fearsome media".[10] Or, as Marsh and Melville put it:

> "[...] in order to understand the reaction to deviance by the public and the authorities it is vital to consider the nature of information that they receive. In modern societies most information is received second hand, usually processed by the mass media and so subject to their definitions of *what constitutes 'news'* and *how it is presented*. And this information is also affected by the constraints which newspapers and broadcasters have to operate under – both commercial and *political constraints*." [11]

Thus there are always two questions to which research on the induction of fear by the media must pay attention: how and why certain acts are considered and presented as despicable crime; and how and why crimes are worthy of being presented as news. In other words, it is about analysing why specific issues are worth being feared and worth being reported.

1.1.2 Moral panics, folk devils, and the amplification of deviance

In the same vein as Young's classic essay,[12] much research has focused on why and how certain crimes are presented in a very sensational and anxious way. The basic argument is that the reporting of deviant behaviour constitutes the (desired) self-perception of a society. The degree of indignation can then be seen as a measure of how threatening a certain crime is towards the system of values of a society. In the case of drug use, Young states: "It is when drug use is seen as unrelated to productivity, when it leads to undeserved pleasures, when it gives rise to experiences which question the taken-for-granted reality, that the forces of condemnation are brought into play".[13]

These "forces of condemnation" can be analysed by looking at the nature of information given by the media, says Cohen.[14] In his study, Cohen gives an insight of the "media inventory" of the "manufactured news" on the incidents of riots caused by juvenile delinquents ("Mods" and "Rockers") in Britain in the 1960s. Comparing facts with reports, he finds a "gallery of folk types – heroes, saints, fools, villains, and

---

[9] Young, Jock, "The Myth of the Drug Taker in the Mass Media", in Stanley Cohen and Jock Young (eds.), *The Manufacture of News*, Constable, London, 1973, p. 314.

[10] Grupp, Stefanie, "Political Implications of a Discourse of Fear: The Mass Mediated Discourse of Fear in the Aftermath of 9/11", (unpublished paper: Berlin): 43

[11] Marsh, Ian and Gaynor Melville, "Moral Panics and the British Media – A Look at Some Contemporary 'Folk Devils'", *Internet Journal of Criminology*, 2011 (online) Available at: http://www.internetjournalofcriminology.com/Marsh_Melville_Moral_Panics_and_the_British_Media_March_2011.pdf, p. 3; emphasis in original. [Accessed 23 October 2012] A poll showed that people say that their feelings about crime are based 65% on what they see and read in the media and 21% on experience; see Altheide, David, "The News Media, the Problem Frame, and the Production of Fear", *The Sociological Quarterly*, Vol. 38 No. 4, 1997, p. 649.

[12] Young, Jock, "The Myth of the Drug Taker in the Mass Media", in Stanley Cohen and Jock Young (eds.), *The Manufacture of News*, Constable, London, 1973.

[13] Young, Jock, "The Myth of the Drug Taker in the Mass Media", in Stanley Cohen and Jock Young (eds.), *The Manufacture of News*, Constable, London, 1973, p. 315.

[14] Cohen, Stanley, *Folk Devils and Moral Panics.* Paladin, St Albans, 1973.

devils"[15] produced within a discourse characterised by exaggeration and distortion, dubious prediction, and symbolisation.[16] The first two are discussed below in a more generalised way, whereas the creation and circulation of symbols as signals of fear is more informative here. Such symbolisation has three processes: "a word (mod) becomes symbolic of a certain status (delinquent or deviant); objects (hairstyle, clothing) symbolize the word; the objects themselves become symbolic of the status (and the emotions attached to the status)." Similar constellations are seen for other "moral panics" in the past;[17] in the recent past, "hoodies" and "paedophiles" have created similar forms of attention, and the media discourse on "terrorists" – sometimes portrayed as Arab-named, bearded, white-clothed males – is likely to produce similar outcomes.

The creation of "folk devils" has largely been discussed within the "amplification of deviance" thesis, which can be summed up as follows: "An initial act of deviance ... is responded to punitively. The … group of deviants is isolated … and this operates to alienate them from conventional society. They perceive themselves as more deviant, group themselves with others in similar position, and this leads to more deviance. This process is of course not seen as deterministic. For example there are differentiations being made among deviant people: the sick, (who can't help it), the innocent (who are corrupted), the wicked (who are corrupt) …"[18]

The model of moral panics and folk devils, more or less connected with the amplification-of-deviance thesis, is nowadays criticised as being outdated in a "multi mediated society".[19] The main point of criticism is that moral panic can be seen as just a form of attention that many actors are actually looking for, rather than trying to avoid; or, in the words of McRobbie and Thornton, as the "culmination and fulfillment of youth cultural agendas in so far as negative news coverage baptizes transgression".[20] "Niche" and "micro media" may articulate single viewpoints or whole identities of youth culture, so that there is never one dominant, uncontested moral perspective on a certain phenomenon. As a result of this, multiple moral panics can be at work at the same time, each of them trying to get more attention; Marsh and Melville conclude in this respect, that "in a media saturated world, moral panics have less impact as nothing shocks us anymore."[21] This analysis and conclusion are perhaps overstated, because the process of creation of societal or international moral panics and folk devils can still be observed, and provides rationales for the surveillance of persons or groups constructed in these ways.

---

[15] Cohen, Stanley, *Folk Devils and Moral Panics*, Paladin, St Albans, 1973, p. 17.
[16] Cohen, Stanley, *Folk Devils and Moral Panics*, Paladin, St Albans, 1973, p. 30
[17] Cohen, Stanley, *Folk Devils and Moral Panics.* Paladin. St Albans, 1973, p. 40.
[18] Cohen, Stanley, *Folk Devils and Moral Panics.* St Albans: Paladin, 1973, p. 18.
[19] McRobbie, Angela, and Sarah L. Thornton, "Rethinking 'Moral Panic' for Multi-Mediated Social Worlds", *British Journal of Sociology*, Vol. 46, No. 4, 1995, pp. 559-574. Cohen's analysis has been subject to other conceptual criticism over the years. For examples, see Jewkes, Yvonne, *Media and Crime*, Sage, Thousand Oaks, CA, 2004, pp. 76–77; Hall, Steve, *Theorizing Crime and Deviance: A New Perspective*. Sage, London, 2012.
[20] McRobbie, Angela, and Sarah L. Thornton, "Rethinking 'Moral Panic' for Multi-Mediated Social Worlds", *British Journal of Sociology*, Vol. 46, No. 4, 1995, pp. 559-574.
[21] Marsh, Ian and Gaynor Melville, "Moral Panics and the British Media – A Look at Some Contemporary 'Folk Devils'", *Internet Journal of Criminology*, 2011 [online] Available at: http://www.internetjournalofcriminology.com/Marsh_Melville_Moral_Panics_and_the_British_Media_March_2011.pdf [Accessed 23 October 2012]

1.1.3 What makes crime news?

Research on the newsworthiness of crime started in the 1970s with the work of Galtung and Ruge and of Chibnall.[22] In the 1980s, Katz asked how the daily appetite for news is satisfied by the media.[23] Jewkes sums up that research as leading to a 12-point-catalogue of criteria ("news values"), that has to be fulfilled to make a crime newsworthy:[24] threshold[25]; predictability;[26] simplification;[27] individualism; risk; sex; celebrity or high-status persons; proximity; violence; spectacle or graphic imagery; children; and conservative ideology.[28] Not all of these contribute to a feeling of fear to the same extent. "Risk" of course matters to a high degree: Furedi[29] cites Guzelian, who says that "most fears in America's electronic age" are the results of "risk-information (whether correct or false), that is communicated to society". Another element of the "feeling rules"[30] relating to fear is addressed by Elin, who states that fear has "come home" and become privatised: that is, the creation of "proximity" and "individualism" of a reported crime (geographically as well as culturally) should be especially mentioned as inducing fear, whereas the involvement of a high-status person, for example, may not have that effect.[31]

Another approach in researching the transformation of crime into news is made by Altheide, who analyses the way the reports work by looking at the textual structure more than on the content of a report.[32] Based on that, he tries to develop a model to explain and predict how a certain topic develops, that is, gains attention in the "news environment". He finds that all contents are being presented within a "problem frame", which strongly appeals to fears[33] and has the following characteristics: has a narrative structure; refers to universal moral meanings; refers to a specific time and place; creates an unambiguous judgment of the situation; has a focus on disorder (e.g., irresponsible behaviour or uncoordinated (re-) actions); and is "culturally resonant".[34] Concerning the last point, Altheide links this "problem frame" to popular culture

[22] Galtung, Johan and Mari Holmboe Ruge, "Structuring and selecting the news", in Stanley Cohen and Jock Young (eds.), *The Manufacture of News*, Constable, London, 1973; Chibnall, Steve, *Law and Order News*, London, Tavistock, 1977.
[23] Katz, Jack, "What makes crime 'news'?", *Media, Culture and Society*, Vol. 9, 1987, p. 47.
[24] Jewkes, Yvonne, "The Construction of Crime News" [2004], in Chris. Greer (ed.), *Crime and Media: A Reader*, Routledge, London, 2010, pp: 215-227.
[25] For example regarding statistical values ("more than one incident per week"), or a non-preceded degree of harm/violence.
[26] For that argument see also: Cohen, Stanley, *Folk Devils and Moral Panics.* St Albans, Paladin, 1973, p. 38
[27] Simplification can be seen as was what was split up into "exaggeration" and "distortion" in Cohen, Stanley, *Folk Devils and Moral Panics.* St Albans: Paladin, 1973, p. 31.
[28] This connection is shown in Beckett, Katherine, *Making Crime Pay: Law and Order in Contemporary American Politics*, Oxford University Press, New York, 1999.
[29] Furedi, Frank, "The only thing we have to fear is the ‚culture of fear' itself", 2007, p.3, Available on: http://www.spiked-online.com/index.php?/site/article/3053/.
[30] Hochschild, Arlie R, "Emotion Work, Feeling Rules, and Social Structure", *American Journal of Sociology*, Vol. 85, No. 3, 1979, pp. 551-575.
[31] Elin, Nan, *Postmodern Urbanism*, Princeton University Press, New York, 1999.
[32] Altheide, David, "The News Media, the Problem Frame, and the Production of Fear", *The Sociological Quarterly*, Vol. 38 No. 4, 1997, pp. 647-668.
[33] Altheide, David, "The News Media, the Problem Frame, and the Production of Fear", *The Sociological Quarterly*, Vol. 38 No. 4, 1997, p. 652.
[34] Altheide, David, "The News Media, the Problem Frame, and the Production of Fear", *The Sociological Quarterly*, Vol. 38 No. 4, 1997, p. 655.

(movies, shows, music), establishing an "entertainment perspective" that has to be co-produced by the media to make the crime attractive to readers and also to make it easier to remember.[35] By connecting crime facts with cultural knowledge in that way, by blurring the borders between reality and fiction, media reports become "testimonies of fear",[36] closely related to "discourses of blame" and responsibilities.[37] Similar to that, Katz sees a secondary function in reading crime news in enabling people to take a stand on existential moral dilemmas.[38]

Altheide's approach to frames (concerning the structure of the text) is complemented by simple content analyses, focusing on regularities in the vocabularies used. For example, he found that the term "fear" itself was used almost twice as often in media reports in general but even three times as much in the headlines, comparing datasets of American newspapers in 1984 and 1994. Television programmes showed an even higher increase for the same period. Since fear, as argued above, always implies an appeal to action, many metaphors can be found that try to symbolise this acute demand for action ("battle metaphors").

Besides the news value of the crime itself and the textual manner in which it is presented, a third factor for the transformation of crime into news lies in the use of visual elements. Hall's position has not been seriously challenged since then, but may even have been strengthened: news photos now and then "repress their ideological dimensions by offering themselves as literal visual transcriptions of the 'real world'."[39] This "function of grounding and witnessing" is ever more accomplished, not only by means of CCTV cameras surveilling many public spaces, but as most people today are technically able and medially encouraged to surveil their environment.[40]

1.2 FEARS SHAPING THE USE OF TECHNOLOGIES

We now analyse the role of fear within the process of deploying specific surveillance technologies, in particular after the terrorist attacks in 2001. We discuss the way in which fear is theorised in the social sciences, and the other factors that may shape the deployment of technologies.

[35] Altheide, David, "The News Media, the Problem Frame, and the Production of Fear", *The Sociological Quarterly*, Vol. 38 No. 4, 1997, p. 652.
[36] Altheide, David, "The News Media, the Problem Frame, and the Production of Fear", *The Sociological Quarterly*, Vol. 38 No. 4, 1997, p. 664.
[37] Altheide, David, "The News Media, the Problem Frame, and the Production of Fear", *The Sociological Quarterly*, Vol. 38 No. 4, 1997, p. 656. Altheide (p. 651) argues that this allows of course for the presence of conflicting frames, as for example "drug use" may be seen as a "public health issue" or as "criminal justice issue".
[38] Katz, Jack, "What makes crime 'news'?", *Media, Culture and Society*, Vol. 9, 1987, p. 71.
[39] Hall, Stuart, "The Determination of News Photographs" [1973], in Chris Greer (ed.), *Crime and Media: A Reader*, Routledge, London, 2010, p. 132.
[40] See, for example, Bidlo, Oliver, "Ins elektronische Panoptikum der sozialen Kontrolle oder: Das Bild hat immer recht", in Nils Zurawski (ed.), *Überwachungspraxen – Praktiken der Überwachung*, Budrich UniPress, Opladen, 2011, pp. 35-46.

1.2.1 Age of anxiety, culture of fear, risk society

The term "fear" plays an important role for many intellectual diagnoses of contemporary society. Furedi discusses the cultural foundations[41] of an emerging "Politics of Fear",[42] strongly distinguishing it from an "age of anxiety", which the 20th century has been labelled.[43] Sunstein discusses similar phenomena, focusing on paralysing effects due to a mixture of a shortage *and* an overload of knowledge at the same time.[44] Especially referring to technological innovations, this paradoxical situation can be illustrated precisely. Unquestionably, technological innovations will have more and different effects than just the ones they were designed for; but it is impossible to be aware of all consequences in advance. This is why Furedi claims that "further developments in the sphere of science and technology tend to be greeted with apprehension rather than celebration. So, for example, recent advances in genetics and nanotechnology are regarded as creating more problems than benefits to society".[45] This constellation of uncertain developments has replaced the attempts to theorise fear by risk analysis[46], which has, in any case, not delivered undisputed principles to handle "risky situations".

If we transfer these thoughts about the societal perception of technologies in general to the field of surveillance technologies in particular, we find that one outcome of the climate of excessive fear and insecurity in the risk-society model is the public demand for extended systems of surveillance to "trace population movements in time and space" and to "risk-profile populations".[47] On the technological side, these demands can be well met: Nellis speaks of an "incessant oversight" that is possible via the satellite tracking of offenders,[48] covering "any space in which people, objects or words move".[49] This goes together with how Spalek and Lambert describe late modern society, "defined by a continuous probing of beliefs, and increasing reflexivity, where 'the deviant other is everywhere' and 'everyone is a potential deviant'".[50]

Thus, we may find the following constellation highly influential for the deployment of new (surveillance) technologies:

---

[41] Furedi, Frank, *Culture of Fear: Risk-Taking and the Morality of Low Expectation*, Cassell, London, 2006.
[42] Furedi, Frank, *Politics of Fear*, Continuum Press, New York, 2005.
[43] May, Rollo, *The Meaning of Anxiety*, The Ronald Press Company, New York, NY, 1950.
[44] Sunstein, Cass R., *The Laws of Fear: Beyond the Precautionary Principle*, Cambridge University Press, Cambridge, 2005.
[45] Furedi, Frank, *Politics of Fear*, Continuum Press, New York, NY, 2005, p. 167.
[46] Furedi, Frank, "The only thing we have to fear is the 'culture of fear' itself", available on: http://www.spiked-online.com/index.php?/site/article/3053/
[47] Ericson, Richard V., and Kevin D. Haggerty, *Policing the Risk Society*, Oxford University Press, Oxford, 1997, pp. 7-8.
[48] Nellis, Mike, "Tracking offenders by satellite – progress or cost-cutting?", *Criminal Justice Matters*, Vol. 68, No. 1, 2007, pp. 10-11.
[49] Bennett, Colin J. and Priscilla M. Regan, "Editorial: Surveillance and mobilities", *Surveillance & Society*, Vol. 1, No. 4, p. 449-445. Similarly, Murakami Wood describes a "neurocity", that has a completely "smart" infrastructure and that is surveilled furthermore by remote control, mobile surveillance agents (robotics); both filling fully connected databases with tons of information about everything what happens in the city. Murakami Wood, David, "Securing the Neurocity", *Criminal Justice Matters*, Vol. 68, No. 1, 2007, pp. 37-38.
[50] Spalek, Basia and Bob Lambert, "Muslim communities under surveillance", *Criminal Justice Matters*, Vol. 68, No. 1, 2007, pp. 12-13. The internal quotations are from Young, Jock, *The Inclusive Society*, Sage, London, 1999.

- a categorical mistrust of new technologies in general, caused by the assumption that not all of their effects can be controlled or even recognised "in time";[51]
- the technological capability of gathering all possible data, of every person, at any time and in any place;
- the conviction that surveillance should not focus only on already convicted offenders, but also and especially on potential offenders/suspects;
- the conviction that potential offenders might not be found only in routinely suspected areas of society, but throughout the entire civilian population.

This constellation creates a two-sided continuum of fear, in which the deployment of technologies takes shape. On the one side we observe a well known "fear of crime" and "fear of terrorism", that demands all sorts of precautionary actions to reach a more effective and more efficient control of criminal activity. On the other side there arise fears on two different levels: at the individual level, the problem of an increased intrusion on privacy arises; on the societal level there are fears concerning more aggravated social inequality.

1.3 SOCIETAL RESILIENCE TO TERRORIST AND OTHER THREATS

Stepping back from the thrust of the argument above and its broad-brush, persuasive quality, it is important to note that societies are not fated to capitulate to the climate of fear described above, and that reactions to terrorism and crime vary, with variable policy or decision outcomes. Contemporary societies differ in the extent to which they are relaxed about perceived terrorist and other threats. This prompts questions about resilience and its meaning, to which this section contributes some groundwork, ending by posing some specific matters for possible further investigation.

Consider, first, the following episode in the Czech Republic:

Early one morning in June, 2007, a traditional programme on Czech TV's second channel that offers long takes of Czech countryside, accompanied with weather information and elevator soundtrack, switched to a camera placed in a mountain resort in Krkonoše. Instead of seeing hazy pictures of the sleepy resort, many thousands of viewers were confronted with an unusually dynamic scene: a flash of light, followed by a spreading mushroom cloud, similar to an atomic bomb explosion. A ticker on the screen said 'ztohoven.com'. An art collective, Ztohoven, hacked into the live TV broadcast as a part of their Media Reality project. The group later released a press statement declaring they were "neither a terrorist organization nor a political group. Our aim is not to intimidate society or manipulate it, which is something we witness on a daily basis both in the real world and in the one created by the media. On June 17 2007, [we] attacked the space of TV broadcasting, distorting it, questioning its truthfulness and its credibility."

[51] This more or less actively influenced process, of unknown or undesired effects emerging while the technology is already operating, or of new purposes being served by a technique, is often called "function creep"; see Lyon, David, *Identifying Citizens: ID Cards as Surveillance*, Polity Press, Cambridge, 2009, p. 58.

A criminal investigation was launched, and three of the group members were charged with spreading false information and faced a potential prison term of up to three years. After two years, all of members of Ztohoven were found not guilty and an administrative council later refused even to fine them for an administrative infraction.[52] While Czech TV criticised the nuclear stunt of the group as "very inadvisable", with a potential to provoke "panic among a wide group of people", other reactions were more moderate. According to the *New York Times*, although "some Czechs expressed outrage over Ztohoven's action ..., in general it drew a mild, tolerant, even amused public response, in contrast to how terrorism-related pranks, or what might seem like them, have been widely greeted elsewhere."[53]

Although any cross-societal comparison would be conjectural, how would such a prank have been likely to play on a morning weather show in Columbus, Ohio? Chan[54] surveyed similar art projects in the US and Great Britain that provoked a substantially different reaction from the one in the Czech Republic, and concluded that "the 'suspicious package' has infiltrated our consciousness through government campaigns for citizens to take part in the war against terror". For Ericson, "these artistic performances have raised awareness of the extent to which societies such as ours have become so steeped in suspicion that there is no room for discretion...So what is it about this 'day and age' that causes public art to be regarded as a 'criminal activity'? Obviously, the political context of the 'war on terror' is central to the new culture of suspicion". [55]

The OECD report of 2003, *Emerging Systemic Risks in the 21st Century*, identified five major "risk clusters" that modern societies have to be prepared for: natural disasters, technological accidents, infectious diseases, terrorism-related risks, and food safety.[56] All these threats are real; how societies react and respond to them, however, depends on a complex interaction of various factors, some of them real, some of them socially constructed. Resilience, or the "ability of a substance or object to spring back into shape", gained prominence in security and crisis management studies after 2001.[57] Sims opines that in the US homeland security realm, resilience is the word of the day.[58] The UK Resilience website of the Cabinet Office defines its mission as to "reduce the risk from emergencies so that people can go about their

---

[52] The Media reality project was later awarded NG333 prize by the National Gallery for "directness" in December, 2007.

[53] Kimmelman, Michael, "That Mushroom Cloud? They're Just Svejking Around", *The New York Times*, January 24, 2008. According to Kimmelman, "the incident instead has highlighted an old Czech tradition of tomfoolery that is a particular matter of national cultural pride". http://www.nytimes.com/2008/01/24/arts/design/24abroad.html?_r=1&pagewanted=all].

[54] Chan, J., "Dangerous art and suspicious packages", *Law Text Culture*, Vol. 11, No. 1, 2007, pp. 51-69. http://ro.uow.edu.au/ltc/vol11/iss1/3

[55] Ericson, Richard V., *Crime in an Insecure World*, Polity Press, Cambridge, 2007.

[56] OECD, *Emerging Systemic Risks in the 21st Century: An Agenda for Action*, 2003, http://www.oecd.org/sti/futures/globalprospects/37944611.pdf

[57] Even Google's Ngram Viewer that reveals how often a word or phrase appears in books over time confirms this rise of prominence of the concept of resilience. See http://books.google.com/ngrams/graph?content=resilience&year_start=1800&year_end=2008&corpus=0&smoothing=3

[58] Sims, Benjamin., "Resilience and Homeland Security: Patriotism, Anxiety, and Complex System Dynamics", http://limn.it/resilience-and-homeland-security-patriotism-anxiety-and-complex-system-dynamics/

business freely and with confidence" by providing contingency advice and guidance to the public and at every level to detect, prevent, and, if necessary, to handle and recover from disruptive challenges".[59]

The idea of *resilience* contrasts directly with *prevention*, in which the aim is to reduce risk to zero by preventing a threat from being realised. Existing research, unsurprisingly, offers a plethora of definitions of resilience that are influenced by respective fields in which it is conduced, ranging from engineering (from which the concept originates), technology and communications, to ecology, disaster research, psychology, sociology, geography, anthropology, to public health. All of them, however, include some variation on adaptability and the ability (of the individual or the system) to "bounce back". As Vasu points out, "the elements constituting social resilience are multi faceted and the interaction of these elements with each other is frustratingly opaque. This is because these elements range from the psychological and social to the normative[60] and also extend to the politics of both governance and culture". [61]

On the micro-level, research focuses on individuals and their responses to threats such as terrorist attacks. Kindt bases individual resilience on (1) individual characteristics (optimism, self-efficacy, mastery, and coherence); (2) social ties (that affect an individual's access to resources and communal support); and (3) coping strategies and problem solving skills.[62] For Verleye *et al*., additional elements for a better conceptualisation of individual resilience are needed, including the presence of other major life stressors, perceived risk and fear, and mental distance from the ongoing terrorist threat. [63] A multidisciplinary approach combined with macro-level analysis of resilience informs a study by Norris *et al*.[64] Their theory of resilience encompasses contemporary understandings of stress, adaptation, wellness, and resource dynamics.

---

[59] The Cabinet Office, "UK Resilience", http://www.cabinetoffice.gov.uk/content/civil-contingencies/

[60] Manyena argues strongly in favour of a process-oriented understanding of resilience, because "traditional practice of disaster management…has propensity to follow a paternalistic mode…Outcome-oriented disaster resilience programmes are inclined to adopt command and control styles that risk preserving the status quo, and which might entrench exclusion, and take attention away from the inequality, oppression and entitlement loss that results in cases of proneness to insecurity and disaster." For more see: Manyena, S. Bernard, "The concept of resilience revisited", *Disasters*, Vol. 30, 2006, pp. 433-450.

[61] Vasu, Norman, "Grace in Times of Friction: The Complexity of Social Resilience", *RSIS Commentaries*, No. 72, 2007, pp. 1-3, at p.1:

http://www.rsis.edu.sg/publications/Perspective/RSIS0722007.pdf

[62] Kindt, Michael, "Building Population Resilience to Terror Attacks: Unlearned Lessons from Military and Civilian Experience", U.S. Air Force Counterproliferation Center, Maxwell Air Force Base, Alabama, 2006, http://cpc.au.af.mil/PDF/monograph/buildingpopres.pdf

[63] Verleye, Gino, Pieter Maeseele, Isabelle Stevens and Anne Speckhard, "Resilience in an Age of Terrorism: Psychology, Media and Communication", in M. Brooke Rogers, Christopher A. Lewis, Kate M. Loewenthal, R. Amlot and Marco Cinnirella, (eds.) *Aspects of Terrorism and Martyrdom: Dying for God, Dying for Good*. The Edwin Mellin Press, Lampeter, 2009. Some researchers offer practical recommendations. Flynn argues that every individual American will have to take responsibility for their own resilience, taking relatively easy steps that include buying a three-day emergency kit; developing a family emergency contact plan; and visiting websites maintained by the Red Cross and other organizations: "such efforts can provide real peace of mind and save lives when disaster strikes." See: Flynn, Stephen E., "America the Resilient", *Foreign Affairs*, Volume 87, No. 2, 2008, pp. 2-8, p. 8.

[64] Norris, Fran H., Susan P. Stevens, Betty Pfefferbaum, Karen F. Wyche, and Rose L. Pfefferbaum, "Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness", *American Journal of Community Psychology*, Vol. 41, 2008, pp. 127-150.

It is process-oriented, constructed as a linkage of a network of adaptive capacities (resources with dynamic attributes) to adaptation[65] after a disturbance or adversity. These capacities (economic development, social capital, information and communication, and community competence) together provide a strategy for disaster readiness.

It is obvious that the concept of resilience has inspirational qualities and is often used in this manner, either in political speeches[66], official policy documents, and even in award recognition of outstanding efforts in crisis:[67] it is better to be thought resilient than brittle and susceptible to fracture. It is open to discussion whether resilience brings a qualitatively new approach to governance. One may imagine that, for Ericson, resilience may be no more than a new spin on the politics of uncertainty that supplemented traditional risk management and led to the institutionalisation of precautionary logics and crime control.[68] Even for Norris *et al*. "there is something to be said for viewing [resilience] as an inevitable, inherent, universal quality of the human spirit ...Communities with high rates of post-traumatic stress disorder or substance abuse or domestic violence or child maltreatment cannot be said to be well. If these or similarly severe problems emerge and persist in the aftermath of a disaster, the community has not exhibited resilience". [69]

Two broad points emerge from the discussion in this chapter. First, how events are transformed into crises is in large part due to social construction. It is the "process by which some insecurities are perceived as dire and others inconsequential, some as the domain of the state and others the responsibility of individuals..."[70] It is the media that

---

[65] Adaptation "is manifest in population wellness, defined as high and non-disparate levels of mental and behavioral health, functioning, and quality of life"; see Norris, Fran H., Susan P. Stevens, Betty Pfefferbaum, Karen F. Wyche and Rose L. Pfefferbaum, "Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness", *American Journal of Community Psychology*, Vol. 41, 2008, pp. 132-134.

[66] The term is used prominently in policy speeches and documents. For example see Sims, Benjamin, "Resilience and Homeland Security: Patriotism, Anxiety, and Complex System Dynamics":

http://search.dhs.gov/search/news?utf8=%E2%9C%93&sc=0&query=resilience&locale=en&m=false&channel=272&affiliate=dhs&commit=Search. For recent policy documents see for example HM Government, "Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review", 2010. Available at:

http://www.direct.gov.uk/prod_consum_dg/groups/dg_digitalassets/@dg/@en/documents/digitalasset/dg_191634.pdf?CID=PDF&PLA=furl&CRE=sdsr or FEMA, "Crisis Response and Disaster Resilience 2030: Forging Strategic Action in an Age of Uncertainty", January 2012, http://www.fema.gov/library/viewRecord.do?id=4995

[67] Department of Homeland Security announced in 2012 the creation of The Rick Rescorla National Award for Resilience to recognise "outstanding response to a catastrophic incident and leadership in fostering resilient and prepared communities". See "Secretary Napolitano Announces The Creation Of The Rick Rescorla National Award For Resilience", http://www.dhs.gov/news/2012/03/27/secretary-napolitano-announces-creation-rick-rescorla-national-award-resilience. UK Resilience web offers, as a part of community resilience section, an awards helpsheet that was developed "if you wish to recognise a community member who has engaged with resilience and recovery work", http://www.cabinetoffice.gov.uk/resource-library/community-resilience-awards

[68] Ericson, Richard V., *Crime in an Insecure World*, Polity Press, Cambridge, 2007.

[69] Norris, Fran H., Susan P. Stevens, Betty Pfefferbaum, Karen F. Wyche, Rose L. Pfefferbaum, "Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness", American Journal of Community Psychology, Vol. 41, 2008, pp. 127-150, p. 146.

[70] Monahan, Torin, *Surveillance in the Time of Insecurity*. Rutgers University Press, New Brunswick, 2010, p. 2

have "a central role in creating and modulating crises"[71]. To Roberts, "perceptions of the significance of crises, and the obligations of governments in relation to crises, are largely shaped by the structure of the infosphere. [That] has changed radically in the last three decades."[72] Moreover, the media-driven amplification of crises allows terrorists, for example, "to reach civilians far removed from the actual attack who are then psychologically victimized by it – suffering from anxiety and terror that they too can become victims".[73] In this sense, terrorism is "nowadays essentially a media experienced phenomena [sic] versus actual experience".[74] But a cautionary note is that not all crises are manufactured by either the media or other special interests, and not all events are amplified into crises or panics. How the public can distinguish between threats that are real and those that are invented, and how public policy can respond in this climate of uncertainty, are questions of prime importance on both the explanatory and policy levels.

Second, and to complicate matters more, our reactions to crisis are constituted and shaped by cultural assumptions and political conditions. While all the concepts that define resilience are universal and relevant in every society, "the manifestations and collaterals of these constructs are undoubtedly culture-specific" and may "vary substantially across cultures".[75] An essential part of resilience-building entails introduction, implementation or strengthening of surveillance to address (in)security.[76] This opens several interesting questions that would be worth exploring beyond the scope of this Task:

> How are different types of risk clusters interlinked with surveillance?
> How easily do policy solutions that target societal resilience transfer from country to country?
> How big is the "resilience-building" spillover to other public policies?

---

[71] Boin, Arjen, Paul 't Hart, Eric Stern and Bengt Sundelius, *The Politics of Crisis Management: Public Leadership under Pressure*. Cambridge University Press, New York, 2005, pp. 72-75.

[72] Roberts, Alasdair S.,"Building Resilience: Macrodynamic Constraints on Governmental Response to Crises", *Suffolk University Law School Research Paper* 09-23, March 16, 2009, p. 8, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1361301

[73] Speckhard, Anne, "Modeling Psycho-Social Resilience to Terrorism", in NATO, *Psychosocial, Organizational and Cultural Aspects of Terrorism*, Final Report of the NATO Human Factors and Medicine Research Task Group 140, November 2011:

http://www.cso.nato.int/pubs/rdp.asp?RDP=RTO-TR-HFM-140]

[74] Speckhard, Anne, "Modeling Psycho-Social Resilience to Terrorism", in NATO, *Psychosocial, Organizational and Cultural Aspects of Terrorism*, Final Report of the NATO Human Factors and Medicine Research Task Group 140, November 2011:

http://www.cso.nato.int/pubs/rdp.asp?RDP=RTO-TR-HFM-140

[75] E.g., degree of filial responsibility, reciprocity norms, relative comfort with kin and non-kin, modes of expressing emotional support, openness to change, acceptability of resettlement: For more see: Norris, Fran H., Susan P. Stevens, Betty Pfefferbaum, Karen F. Wyche, and Rose L. Pfefferbaum, "Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness", *American Journal of Community Psychology*, Vol. 41, 2008, p. 145.

[76] For an extensive critique of the culture of fear, the expansion of surveillance and the neoliberal policy shift that produce public-private collusion, see Monahan, Torin, *Surveillance in the Time of Insecurity*. Rutgers University Press, New Brunswick, NJ, 2010. His argument is that these phenomena are mutually constitutive, producing public-private partnerships collusion and the distribution of responsibility for security to individual citizen.

Does public support for (increased) surveillance differ between countries that have recently experienced events that have tested resilience and those with limited or no such recent experience?
How path-dependent are the adaptive capacities of former communist societies that spent decades under threats ranging from the "enemy within", that gave rise to omnipresent state service (e.g., Stasi, KGB, STB, *Securitate*), to the ever-present threat of global nuclear conflict, to nuclear disaster (e.g., Chernobyl in 1986)?

1.4 EXPERIENCING SURVEILLANCE IN DIFFERENT DEMOCRATIC CONTEXTS, INCLUDING NEW DEMOCRACIES AND FORMER REPRESSIVE REGIMES

The numerous forms of surveillance, especially those concerning the relationship between the citizens and the state, are realised and experienced differently in different democratic contexts. This concerns not only the present political and social systems but also previous systems, that is, the legacy of the former repressive regimes in the so-called new democracies. The historical experience of present-day democracies has a significant influence on how citizens react to and cope with surveillance. Haggerty and Samatas claim that surveillance *at the surface* seems to be antagonistic to democracy, and ultimately leads to totalitarianism.[77] However, surveillance – even in its institutionalised forms – is a legitimate element of democratic systems as well. The fundamental difference between dictatorial and democratic systems with regard to surveillance lies in its accountability: while in a dictatorial system state surveillance cannot be overseen and controlled by the citizens, at least in an institutionalized form, in democracies there are institutions and mechanisms established for this purpose (although in practice such systems cannot be easily overseen and controlled either). In addition, in a democratic constitutional state, a precondition of legitimate surveillance is that it must have a morally acceptable ground (although most repressive regimes justify surveillance by declaring moral principles, for example, to protect the country and its citizens from harmful influence). Apart from theoretical dilemmas – for example, which countries can be regarded as democracies, and whether a democracy can be regarded as "democratic" in every respect – the borderline between "democratic" and "dictatorial" surveillance is not clear-cut. For example, the current shifts from Foucault's panoptic society to today's control or actuarial societies, from the old penology to "New Penology", and from "new" surveillance technologies to "future and emerging" technologies (FETs) serving ubiquitous, "predictive" surveillance, can be observed in a wide range of systems on the normative continuum. Of course, the final aim of surveillance is different, in dictatorial systems, in which – governed by the idea of centralisation – it serves the interests of a much narrower political elite than in democracies. The differences in the nature of surveillance in the different democratic contexts, however, can best be detected in "classic", institutionalised state surveillance, exercised by specific institutions and agents, serving political and ideological purposes; therefore we concentrate on this kind of surveillance in the following sections. However, we do not focus upon the dichotomy

[77] Haggerty, Kevin D. and Minas Samatas, "Surveillance and democracy: an unsettled relationship", in Haggerty, Kevin D. and Minas Samatas (eds.), *Surveillance and democracy*, Routledge, London, 2010.

of democratic and repressive regimes, but rather on different democratic contexts, with special regard to new democracies or former repressive regimes.

1.4.1 Surveillance practices in repressive regimes

Throughout history, numerous repressive regimes had built surveillance networks and institutions against their citizens. Our approach in 21st century Europe has been shaped perhaps the most by the practice of 20th century dictatorial systems. Here we should consider not only the countries of the former Soviet Bloc but also what had been well-established democracies in Western Europe, both in the interwar period and after World War Two. Although the activity of the secret police of Nazi Germany and its allies is a well-known topic among surveillance historians, similar to the attempts to set up a totalitarian-style citizen registration,[78] the realisation of the ultimate *Überwachungsstaat* ("surveillance state") is best perceived in post-war East Germany, in the Soviet Union, and in and its satellite states. This is due not only to Orwell's accurate and merciless vision publicised as early as the late 1940s,[79] but in a sense also to the historical remorse of Western European countries, the pre- and post-war surveillance practices of which were indirectly legitimised by the ideology of the Soviet system.

The organisations specialised for keeping citizens – potential "internal enemies of the system" – under surveillance in countries of the Soviet Bloc were the KGB in the Soviet Union, *Stasi* in East Germany, STB in Czechoslovakia, *Securitate* in Romania, or the "III/III Division" in Hungary. They followed similar ideologies and performed similar tasks; however, national and cultural differences were not negligible. As a US scholar who had been doing research in Socialist Romania for 25 years recalled, the surveillance practice (and its deficiencies) of the *Securitate* demonstrated the weakness of the system rather than its strength.[80] In contrast, the far-flung activities and precision of the *Stasi* can be demonstrated by the personal story of a Canadian professor, who had visited East German archives and co-operatives several times, and – as it turned out after 1989 – had been registered by the *Stasi* many years before he would have even thought of visiting the country.[81] The effects these state-controlled surveillance practices had on society, however, were similar. As Szekely describes, "By keeping the 'internal enemies' of the system under surveillance, the secret services and their civilian collaborators perpetuated a situation in which no one could be sure just how much the next person knew about him or her. This constant sense of doubt and distrust massively disfigured human relationships on both the personal and the social levels."[82] The same argumentation had served as one of the fundamental

[78] For example, the alleged collaboration of the IBM with the Nazi regime in the 1993 German census, which identified Jews in the population of Germany; see Black, Edwin, *IBM and the Holocaust*, Little Brown, Boston, MA, 2001.

[79] *Animal Farm* was first published in 1945, *1984* in 1949.

[80] Verdery, Katherine, "Anthropological adventures with Romania's Wizard of Oz, 1973-1989", *Focaal*, Vol. 43, 2004, pp. 134-145.

[81] Information courtesy of Professor Scott M. Eddie, University of Toronto.

[82] Szekely, Ivan, "Changing attitudes in a changing society? Information privacy in Hungary 1989–2006", in Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon, and Yolande E. Chan (eds.), *Privacy, Surveillance and the Globalization of Personal Information: International Comparisons*, McGill-Queen's University Press, Montreal & Kingston, 2010. Los connects this phenomenon with "social atomization"; see Los, Maria, "Looking into the future: surveillance, globalization and the totalitarian potential", in Lyon, David (ed.), *Theorizing surveillance: the*

statements of the famous 1983 census decision of the German Constitutional Court, which reads: "...whoever cannot measure the knowledge of possible communication partners to any degree, can be fundamentally limited in his personal freedom...".[83]

Although in Europe the Soviet political system was regarded as the emblematic example of the surveillance state, in the same period of the 20th century several Southern European countries suffered from dictatorial regimes, which also had extensive, state-controlled surveillance systems.[84] In Spain and Portugal, dictatorial regimes occupied a significant part of the last century – ending only in 1975 and 1974, respectively – and both established their organisations responsible for keeping the civilian population under surveillance (TOP and SECED in Spain, PIDE in Portugal). In the relatively short historical period of dictatorship in Italy, the Mussolini regime had built up its Organisation for Vigilance and Repression of Anti-Fascism (Ovra) already by the end of the 1920s. Greece had a short military dictatorship but a long period of post-war repressive political regime. These regimes and their surveillance systems relied on networks of informants and centralised filing systems, first spying on communists and anti-fascists, later on "all aspects of national life".[85]

This characteristic of state-controlled surveillance systems seems to be universal: in other continents and cultures, the respective surveillance organisations set up similar networks and applied similar means, including the activities of "private collaborators". During the 1973-1990 military rule in Chile, for example, one of the pillars of the regime was the surveillance activities of the secret police, the DINA, which, in collaboration with the foreign department, extended its operation to other countries, too, where opposition Chileans were living.[86] Similar practice can be observed in other Latin American countries during repressive political regimes.

---

panopticon and beyond, Willan Publishing, Cullompton, 2006. See also Garton Ash, Timothy, *The File: A Personal History*, HarperCollins, London, 1997.

[83] 1. BvR 209/83 paragraph C II.1, p. 43, quoted in English in, among others, Federrath, Hannes, Marit Hansen and Michael Waidner, "Andreas Pfitzmann 1958-2010: Pioneeer of Technical Privacy Protection in the Information Society", in Fischer-Hübner, Simone, Penny Duquenoy, Marit Hansen, Ronald Leenes and Ge Zhang (eds.), *Privacy and Identity Management for Life*, Springer, 2011, pp. 349-352.

[84] The Living in Surveillance Societies (LiSS) COST Action, a four-year European research program supported by the European Commission, devoted its annual international conference held in Iasi, Romania in 2011 to the theme of surveillance in post-dictatorial societies. The proceedings of the conference have been published as Webster, William C., Doina Balahur, Nils Zurawski, Kees Boersma, Bence Ságvári and Christel Backman (eds.), *Living in Surveillance Societies: The Ghosts of Surveillance. Proceedings of LiSS Conference 2*, Editura Universităţii „Alexandru Ioan Cuza", Iasi, 2011.

[85] Samatas, Minas, Chiara Fonio, Catarina Frois and Gemma Galdon Clavell, "Authoritarian Surveillance and its Legacy in South-European Societies: Greece, Italy, Spain, Portugal", in Webster, William C., Doina Balahur, Nils Zurawski, Kees Boersma, Bence Ságvári and Christel Backman (eds.), *Living in Surveillance Societies: The Ghosts of Surveillance. Proceedings of LiSS Conference 2*, Editura Universităţii „Alexandru Ioan Cuza", Iasi, 2011.

[86] *Report of the Chilean National Commission on Truth and Reconciliation*, University of Notre Dame Press, Notre Dame, IN, 1993.

Resistance or resilience towards such state-controlled surveillance can take several forms. As Los emphasises,[87] people in communist regimes developed a strong control over their body language in order to produce a uniform appearance and mask their opinions. The expression "Not over the phone!" was widely used both in its actual and symbolic meanings. Opposition intellectuals tried to reduce their constant stress by publicly and privately joking about the ubiquitous surveillance, for example, talking into the light switch on the wall as if it were a microphone (and sometimes it really was). Inverse surveillance was extremely rare and dangerous to conduct in these political systems.[88]

1.4.2 Surveillance and the change of political systems

In the turbulent periods of profound change of these political systems, the surveillance practice of the previous regime and the dossiers of citizens earlier regarded as "internal enemies" has gained special significance, both in politics and in public opinion. One of the principal political demands in such periods has concerned the accessibility of these dossiers; this has often become symbolic of the changes. Similarly, in the eyes of the public, agents and spies who performed surveillance against the citizens have easily become scapegoats responsible for all the wrongdoings of the past regime. In order to handle this problem of a partly legal, partly moral nature, countries undergoing such system change have been seeking various solutions, including legal ones, and have created various versions of instruments for "lustration", which is explained below. Although not a European specificity, lustration can be analysed most comprehensively in the practice of new European democracies.

In essence, lustration has three main functions: (a) screening the past of former agents and collaborators and filtering them out from present political life; (b) showing how the system was working, thereby offering an informational recompense to the society; and (c) providing access for the individual subjects of surveillance to their dossiers, i.e., guaranteeing their informational self-determination. The first element is of a sanctioning character, the second is that of a collective right, while the third is guaranteeing an individual right to the persons concerned. In practice, the newly democratic regimes have laid different emphases on each of these functions, thereby creating national versions of lustration. At the two ends of the spectrum are the German and the Hungarian solutions: in Germany, the identity of the agents and informants became publicly known and those found guilty were prevented from fulfilling public functions, while in Hungary agents could resign from their functions in public life on the quiet, and if they wanted to stay, the greatest sanction was the public exposure of their past.

[87] Los, Maria, "A trans-systemic surveillance: The legacy of communist surveillance in the digital age", in Haggerty, Kevin D. and Minas Samatas (eds.), *Surveillance and Democracy*, Routledge, London, 2010.

[88] Photos taken by opposition activists in Prague and Budapest of secret police agents during their clandestine actions was exhibited in the OSA Archivum in early 2011 as one of the few examples of inverse surveillance during communism; see:
http://osaarchivum.org/galeria/catalogue/2011/surveillance/index.html

Despite the sublime ideas and the few cathartic public events – such as the so-called Hungarian Watergate, or Duna-gate scandal,[89] when a renegade intelligence officer of the infamous III/III Division ended up in front of the television cameras making a public confession – lustration proved to be an imperfect tool for revealing the surveillance practice of the past regimes and became the arena of political struggles, blackmailing, and falsifying documentary evidence. It deserves noting that the old secret services did not stop conducting their surveillance activities even during the turbulent periods of profound political changes, although in some cases this could be regarded as the aimless and dysfunctional reflex of an apparatus left to its own devices.

1.4.3 Public perceptions of surveillance in post-dictatorial systems

It is not surprising that the impact of surveillance practice of repressive regimes lasts longer than the regimes themselves. This is partly due to the unsolved problems, such as lustration, after the political changes, and partly due to the long life and inheritable nature of patterns of resistance and resilience towards surveillance. A further important factor is the role of former agents and collaborators in the new political era: one part of them remained in the bonds of newly democratised secret services – although the elderly or discredited members of the old guard have been replaced –, another part entered in the newly booming private security and investigating business, which absorbed a significant proportion of the personnel and knowledge of the former surveillance organisations; again another part succeeded in transforming their power and networks into other sectors of the political or business elite. According to Los, in the former communist countries the surviving secret knowledge made it difficult to institutionalise any form of accountability. [90]

As Los also points out,[91] a decisive factor was the conversion of fear: the pervasive fear of the repressive regime and its institutions and agents was quickly replaced by a fear of crime – and we can add that this did not only create a demand for the new security industry, but also created a basis for the legitimacy of maintaining, and even increasing, the level of surveillance in general. Naturally, fear of crime as the basis for the legitimacy of surveillance is not a post-communist characteristic: in South Africa, for example, there was no need to convert the fear of the state to the fear of crime: the level of crime had always been high and constituted a continuous basis for the legitimacy of surveillance, while in the UK apparently crime and the fear of crime have been decisive factors for applying CCTV cameras on a wide scale.

The surviving patterns of (real or counterfeit) conformity towards the ruling political system may also have a role in the popularity of clichés like "if you have done nothing wrong or have nothing to hide you have nothing to fear" in some new democracies. According the Szekely,[92] in these societies the threshold of abstraction

[89] Szekely, Ivan, "Hungary", in James B. Rule and Graham Greenleaf (eds.), *Global Privacy Protection: The First Generation*, Edward Elgar Publishing Ltd., 2008.
[90] Los, Maria, "A trans-systemic surveillance: The legacy of communist surveillance in the digital age", in Haggerty, Kevin D. and Minas Samatas (eds.), *Surveillance and Democracy*, Routledge, London, 2010.
[91] Los, Maria, "Post-communist fear of crime and the commercialization of security", *Theoretical Criminology*, Vol. 6, No. 2, 2002.
[92] Szekely, Ivan, "Changing attitudes in a changing society? Information privacy in Hungary 1989–2006", in Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon, and Yolande E. Chan

(above which people do not realise the intrusion in their privacy)[93] is lower in this area than in more experienced democracies. A further general conclusion by Los is that societies experiencing the prolonged dictatorships of the 20th century virtually skipped the period of (democratic) modernity and jumped directly into the surveillance culture of postmodernity, which renders obsolete any unified concept of the self. Combined with the cultural consequences of globalisation and the rapid development of technology, the lack of historical experience in adaptation to new, decentralised forms of surveillance makes the disintegrating personality even more vulnerable in such new democracies. This seems to resonate at another level – the level of everyday practice – with Szekely's observation, according to which the members of these societies are less experienced and more gullible vis-à-vis business and marketing offers, including industry-driven surveillance.[94]

Differences in national history also constitute an important factor in the present-day perception of surveillance in post-dictatorial societies. In Greece, decades after the collapse of the dictatorship, there remains a deep mistrust of any state or police surveillance even for legitimate purposes (such as traffic control, etc.), while citizens are conspicuously uninterested in private surveillance and data collection. Watching is less important than filing; these characteristics are sometimes called the "Greek surveillance paradox".[95] In Italy, the discretionary powers and a lack of radical reform of the police until recent times have emphasised the socio-cultural legacy of the dictatorship and have led to the consideration of surveillance practices as integral to the security apparatus of public bodies and private organisations.[96] In Portugal, it is not the aim of securitising the country, but a pattern of developmental policies that led to the widespread use of CCTV cameras and related equipment: gaining competitiveness, using new technologies, "recovering the lost time" are major driving forces behind a new culture of surveillance.[97]

(eds.), *Privacy, Surveillance and the Globalization of Personal Information: International Comparisons*, McGill-Queen's University Press, Montreal & Kingston, 2010.

[93] According to this hypothesis, it is not the violation of privacy in itself that counts but its perceptibility: the more abstract, the less important, no matter how grave the violation is. In Szekely's example, if policemen stop people frequently and ask for their ID cards, people soon protest against the "police state", however, if the same policemen check the same people without stopping them, probably nobody objects.

[94] Szekely, Ivan, "Hungary", in James B. Rule and Graham Greenleaf (eds.), *Global Privacy Protection: The First Generation*, Edward Elgar Publishing Ltd., 2008.

[95] Samatas, Minas, Chiara Fonio, Catarina Frois and Gemma Galdon Clavell, "Authoritarian Surveillance and its Legacy in South-European Societies: Greece, Italy, Spain, Portugal", in Webster, William C., Doina Balahur, Nils Zurawski, Kees Boersma, Bence Ságvári and Christel Backman (eds.), *Living in Surveillance Societies: The Ghosts of Surveillance. Proceedings of LiSS Conference 2*, Editura Universităţii „Alexandru Ioan Cuza", Iasi, 2011.

[96] Samatas, Minas, Chiara Fonio, Catarina Frois and Gemma Galdon Clavell, "Authoritarian Surveillance and its Legacy in South-European Societies: Greece, Italy, Spain, Portugal", in Webster, William C., Doina Balahur, Nils Zurawski, Kees Boersma, Bence Ságvári and Christel Backman (eds.), *Living in Surveillance Societies: The Ghosts of Surveillance. Proceedings of LiSS Conference 2*, Editura Universităţii „Alexandru Ioan Cuza", Iasi, 2011.

[97] Samatas, Minas, Chiara Fonio, Catarina Frois and Gemma Galdon Clavell, "Authoritarian Surveillance and its Legacy in South-European Societies: Greece, Italy, Spain, Portugal", in Webster, William C., Doina Balahur, Nils Zurawski, Kees Boersma, Bence Ságvári and Christel Backman (eds.), *Living in Surveillance Societies: The Ghosts of Surveillance. Proceedings of LiSS Conference 2*, Editura Universităţii „Alexandru Ioan Cuza", Iasi, 2011.

Temporal changes in the perception of surveillance, and in general in the respect for rights and liberties, show a typical pattern in societies undergoing transition from dictatorship. In the initial euphoria, the new rights and freedoms, including information rights, have a high respect in society, are publicised in the media, and constitute an important element of the political agenda. However, when the euphoric elation and the momentum of metamorphosis is spent, career, profit, business, and political power all take precedence over respect for individual rights. This is especially true for the new, much more technocratic generation, which has grown up since the political changes began.[98] These temporal changes significantly influence the public perception of surveillance in the different historical periods. Taking all the above factors into consideration, it is still questionable whether and when a new surveillance culture mixing a seductive menu-culture – as Los puts it – with a belligerent securitisation culture will supersede the differences of the political biographies of "old" and "new" democracies.

1.4.4 Closing remarks on democracy and non-democratic surveillance

Although it is not the task of this section to analyse the legitimacy of the surveillance practice in today's democratic countries, we should note that there exists no "ideal" version of democracy, only different realisations of democratic ideals in different political and cultural environments. There are political systems that are formally democratic, but there is much room for criticism of the way power is exercised, or of the practical realisation of democratic rules of game. For example, in the past, the Soviet Union introduced the so-called "democratic centralism" (which was rather more centralism than democratic), and the post-civil war Greek system can be described as a semi-parliamentary, "guided democracy" (in reality, an oppressive anti-Communist socio-political control system).[99] The different Western European democratic traditions have also resulted in national or regional specificities, even under the umbrella of the EU – which can also be regarded as an autonomous system in itself – not to mention the approaches of other geo-political regions and cultures. The new European democracies did not adopt a uniform democratic system either; the differing historical experiences, the geo-political and cultural regions and the *longue durée* societal processes all have had an impact on the versions of democracy these countries are trying to realise.

Consequently, the national modalities of surveillance systems are oriented to different ideas and perceptions, despite the strong trends of globalisation. However, if there existed an ideal democracy, present-day surveillance practice would trespass its borderlines in many respects, as empirical evidence and experience shows. This sets a difficult task both for researchers in surveillance studies and for committed democrats, as well as for the law enforcement sector, the members of which have

[98] Szekely, Ivan, "Hungary", in James B. Rule and Graham Greenleaf (eds.), *Global Privacy Protection: The First Generation*, Edward Elgar Publishing Ltd., 2008.

[99] Samatas, Minas, Chiara Fonio, Catarina Frois and Gemma Galdon Clavell, "Authoritarian Surveillance and its Legacy in South-European Societies: Greece, Italy, Spain, Portugal", in Webster, William C., Doina Balahur, Nils Zurawski, Kees Boersma, Bence Ságvári and Christel Backman (eds.), *Living in Surveillance Societies: The Ghosts of Surveillance. Proceedings of LiSS Conference 2*, Editura Universităţii „Alexandru Ioan Cuza", Iasi, 2011.

always regarded individual rights as a disturbing factor in the work they are entrusted with in the great division of labour in society, and the efficiency and importance of which they deeply believe in. Similarly much burden is placed on those "applied" philosophers and ideologists whose task is to prove the democratic, constitutional nature of present-day surveillance.

1.5 THE POLITICAL EFFECTS OF FEAR AND INSECURITY

We have already considered the question of resilience in the face of real or supposed threats. Previous sections have set the scene for looking at some of the political repercussions of the climate of fear and insecurity. The present section considers these briefly in terms of the effect on decision-making and political debate, as a precursor to the lengthier discussion of policy-making and the regulation of surveillance, which form the substance of Chapter 2.

1.5.1 The distortion of debate and decision

Security and insecurity have been important in the policy discourse for a long time. In 1994, Rudolph Giuliani won the election to become the Mayor of New York on the promise of implementing a "tough on crime" approach at a time when insecurity was high in the public agenda. Since the 2001 attack on the Twin Towers, security concerns have incorporated the terrorist threat, and fear has become a fixed item in public discourse. This pressure to act, react and prevent, to respond to people's fears and sense of insecurity, affects the policy process in significant ways, as people demand to *see* that something is being done to protect them. As Bruce Schneier explains, this results in an increasing recourse to what he calls "security theatre": "a cheaper alternative to real security", a set of "palliative" measures that "provide the feeling of security instead of the reality".[100] This can be due to several reasons, but for the issue of debate and decision-making, security theatre provides a fast, visible and effective (theatrical) way to show that "something is being done" about insecurity. In their study on the growth of CCTV, one of the most visible responses to insecurity in urban areas, Norris *et al.* emphasis the way in which "the political appeal of CCTV has less to do with CCTV's proven effectiveness in reducing crime and far more to do with its symbolic value that something was being done about the problem of crime'.[101]

In the field of security policy, thus, there has been an increasing departure from statistics and other forms of evidence that can be amenable to scientific analysis and challenge, and a growing reliance on feelings and perceptions, as Svenonius observes.[102] This focus on people's perception of insecurity as "evidence" is one of the drivers behind the increasing reliance on surveillance technology in security policy, together with the fact that relying on privately-provided technological solutions is a good fit to the commercial logic so pervasive in 21st-century urban management. In this context, however, what does and does not constitute a threat ends

[100] Schneier, Bruce. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. Copernicus Books, New York, 2003, p. 38.
[101] Norris, Clive, Michael McCahill and David Murakami Wood, "The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space", *Surveillance & Society*, Vol. 2, Nos. 2-3, 2004. p. 123.
[102] Svenonius, Ola. *Sensitising Urban Transport Security: Surveillance and Policing in Berlin, Stockholm, and Warsaw*, PhD thesis, Södertörn University, Stockholm, 2011.

up being decided by a combination of media-amplified panics (discussed earlier) rushed public debates, commercial self-interest and political pressure.

Assessing the effectiveness or cost-efficiency of surveillance and security policies and technologies is not a priority in this environment; nor is the search for more subtle, less dramatic alternative policies. But even when evaluations emerge to show that some of the policy decisions taken to combat crime and the fear of crime through surveillance technologies do not work, or do not work sufficiently well to justify the policy and expenditure, these are usually not revised. As Norris *et al.* argue in relation to CCTV, we must look beyond efficiency "to explain the explosive growth of CCTV surveillance, and these [other reasons] include the common sense notion that it must work, its popularity with the public, the Government's need to be seen to be doing something about crime and the publicity surrounding CCTV in high profile cases".[103]

Debate and rational, accountable decision-making suffer in a climate of fear and of a deterministic perspective on technology, and the necessary relationship between public problems and policy solutions – key to good policy-making – risks being lost. Moreover, negative externalities related to the political, social and economic cost of such policies are often overlooked, as the chosen policy solutions are not assessed in relation to their potentially less harmful or costly alternatives. A pertinent case in point here is aviation security. Since the 9/11 attacks, using hijacked aircraft, aviation security has become a priority in the whole world, and anti-terrorist, surveillance practices have become a common feature of air travel. However, there is little evidence available about the usefulness and proportionality of cost-effectiveness of such measures,[104] and the relationship between the security problems that emerge and the technological solutions that are implemented as a result is often obscure and sheltered from public or political debate.

On Christmas Day 2010, for instance, a person was arrested after attempting to explode a device sewn to his underwear on an Amsterdam-Detroit Northwest Airlines flight. The perpetrator had previously raised suspicion with the UK Border Agency and British intelligence, and his own father had reported him to the US embassy in Abuja (Nigeria) for his religious extremism. He was therefore added to several databases in the US and the UK, but the information was neither shared nor investigated further; thus he managed to board a plane in Amsterdam, even though he eventually failed to detonate the explosives he was carrying. From a policy perspective, one of the obvious diagnoses of "what went wrong" would point to the use of databases and the inefficiency of intelligence to address reported cases in a fast and effective manner. A coherent solution would need to address these shortcomings. In the days after the event, however, most headlines shifted the focus: "Detroit terror attack: pressure grows for full body scanners at British airports", said *The Telegraph* on December 30th, 2010. The fact that it was unclear whether such devices would have identified the explosives the man was carrying seemed irrelevant, and this event marked the beginning of the proliferation of full-body scanners at airports across the globe, arguably infringing passengers' rights and substantially affecting air travel,

[103] Norris, Clive, Michael McCahill and David Murakami Wood, "The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space", *Surveillance & Society*, Vol. 2, Nos. 2-3, 2004. p. 124.
[104] Kraft, Michael E. and Scott R. Furlong. *Public Policy. Politics, Analysis, and Alternatives*, Sage/CQ Press, London, 2012 (4th edition).

even though the link between the actual threat and the adopted solution remains difficult to establish.

The problem does not only lie with the possibility of having an informed debate over surveillance solutions to security problems, but also on the possibility of making the decision-making process dependent on evaluation of their negative externalities and cost-effectiveness. The preventive law enforcement agenda put forward after 9/11 has resulted in increased surveillance powers for public and private bodies alike, and an increased reliance on data-mining, profiling, and storing.[105]

All this has implications for people's rights and civil liberties. But a key element that is often overlooked when addressing this issue is the fact that, as observed with CCTV, the tools to monitor the efficacy of such policy decisions and alter them if proven deficient or not proportional are rarely used, and the drive toward security seems to justify unaccountable decision-making and policy.

[105] Bloss, William, "Escalating U.S. Police Surveillance after 9/11: an Examination of Causes and Effects", *Surveillance & Society*, Vol. 4, No. 3, 2007, pp. 208-228. Later in Task 2.2, figures are given for the US government's requests to companies for retained communications data.

2. CHAPTER 2: SURVEILLANCE AS A TOOL THAT IS SUBJECT TO REGULATION, LIMITATION AND CONTROL

We subscribe to the view that surveillance can – albeit with difficulty, and with considerable variation across jurisdictions, levels of jurisdiction, and types of surveillance – be brought within the limits expected in democratic, accountable political systems governed by the rule of law. In this chapter, we therefore turn to examine policy-making for surveillance, both how surveillance is put on a legitimate footing and how it can be kept in bounds through the actions of political and governmental systems. Our discussion of policy-making is illustrated with the case of data retention, a policy subject that has been greatly controversial in the EU and between it and third countries in recent years. We investigate accountability and transparency as central norms of democratic, non-authoritarian political systems, norms that also play their part in the control of surveillance whether the latter is deployed by organisations in the public or private sector. The rule of law, and the position of rights and freedoms as criteria for evaluating surveillance, is also discussed, while the governance of surveillance is described in terms of the repertory of instruments and actors that expand the possibilities beyond the enactment, implementation and adjudication of statutory law or other legal provisions. Our account of the political perspective, and of the processes, organisations and actors that play important parts in countering surveillance, acknowledges the important role of everyday individual resistance to surveillance, which was discussed in Deliverable 2.1. This can be seen as a response that has political significance separate from the activities of more formal activist or protest groups and organisations that aim to influence policy through the better recognised channels of a democratic political system.

2.1 POLICY-MAKING AND SURVEILLANCE

Decision-making is an integral part of policy. For policy solutions to be implemented, problems have to be defined, decisions need to be made and resources must be found and allocated. For a long time, policy-making was seen and explained in some textbooks as a rational exercise carried out by rational actors working logically and scientifically in perfect information settings, where decision-makers would pick up on the issues that emerged from the public debate and find the best possible solution. As we emphasise in this chapter, this idea has long been overcome by a complex, more empirically based, multifaceted and less-than-perfect understanding of policy and decision-making. The role of uncertainty, ambiguity and the impact of competition between actors and interests must be acknowledged.[106] This complex understanding has made it much easier for policy analysts to take account of the many processes that can be identified in policy-making, although it is daunting to gathering empirical data on the phenomena that are involved in policy-making, whether in general or in specific areas such as surveillance.

[106] See, for example, Lindblom, Charles E. and Edward J. Woodhouse, *The Policy-Making Process*. Prentice Hall, Englewood, NJ, 1993 (3rd edition).

There are a number of ways of conceiving what is meant by the very term "policy-making", and academic literature in political science and public policy has brought forward a number of approaches and models that are intended to help understand the public policy-making process. Useful approaches include the "policy cycles",[107] "policy networks",[108] and "policy streams"[109] approaches, as well as models that focus on the processes of decision-making.[110] Policy-making can also be conceived as a "practice": the art of policy-making,[111] or as an activity that is closely related to, and not distinct from, service delivery and strategy. Implicit in policy-oriented approaches are ideas that policy-making involves the making of decisions or the setting of a direction, especially in relation to public services and/or regulation. Policy-making is therefore also closely aligned to the legitimacy of the political and democratic systems and the rationality of individual policies.

Policy-making, in whatever field of activity and under whatever definition, is inherently complex. It involves a wide range of actors, organisations and institutions, as well as relationships and discourses. Moreover, this constellation moves through time, often in recursive loops and with a kaleidoscopically shifting array of participants, ideas and outputs. Policy-making, for example in relation to surveillance, can best be understood from two key perspectives, first as the *processes* that lead to emergence of surveillance policy, and second as the *content* of policy relating to surveillance. Although these two perspectives are interrelated, they are recognised in general policy studies as distinctive schools of research.[112] Together, they underline the importance of understanding what constitutes a surveillance policy, who is formally responsible for determining it, how the policy emerges, which actors, institutions and discourses influence and shape the policy-making process, and what relationships and vested interests are central to the development of the policy. They also involve an investigation of policy rationales, substance, and effects. Therefore, they analyse and evaluate a policy as well as comment upon its procedural aspects, including the extent to which a policy conforms to democratic values and processes. In the case of surveillance, many processes are covert – perhaps necessarily – and emerge from within relatively closed circles of actors and institutions, and not always

[107] See, for example, Lasswell, Harold D., *The Decision Process: Seven Categories of Functional Analysis,* University of Maryland Press, College Park MD, 1956; Lasswell, Harold D., *The Future of Political Science,* Atherton, New York, NY, 1963; Mack, Ruth P., *Planning on Uncertainty,* John Wiley, New York NY, 1971; Rose, Richard, "Comparing public policy: an overview", *European Journal of Political Research,* Vol. 1, No. 1, 1973, pp. 67-94; and Jenkins, W. I., *Policy Analysis: A Political and Organisational Perspective,* Martin Robertson, London, 1978.

[108] See, for example, Marsh, David and Roderick Rhodes, (eds.), *Policy Networks in British Government,* Clarendon, Oxford, 1992; Marsh, David and Roderick Rhodes, (eds.), *Implementing Thatcherite Policies,* Open University Press, Buckingham, 1992; Rhodes, Roderick, A. W., "Power dependence, policy communities and intergovernmental networks", *Public Administration Bulletin*, 49, 1985, pp. 4-31; Rhodes, Roderick A. W., *The National World of Local Government,* Allen and Unwin, London, 1986; Rhodes, Roderick A. W., *Beyond Westminster and Whitehall,* Unwin Hyman, London, 1988; and Smith, Martin, *Pressure, Power and Policy,* Harvester Wheatsheaf, Hemel Hempstead, 1993.

[109] See, for example, Kingdon, John, *Agendas, Alternatives and Public Policies,* Little Brown, Boston MA, 1984.

[110] Se, for example, Triantaphyllou, Evangelos, *Multi-criteria decision making methods: a comparative study,* Kluwer Academic Publishers (now Springer), Dordrecht, 2000; and Kepner, Charles H. and Benjamin B. Tregoe, *The Rational Manager: A Systematic Approach to Problem Solving and Decision-Making,* McGraw-Hill, New York NY,1965.

[111] Vickers, Geoffrey, *The Art of Judgement: A Study of Policymaking,* Chapman Hall, London, 1965

[112] John, Peter, *Analysing Public Policy,* Pinter, London, 1998.

specifically endorsed through democratic, representative bodies. This makes it difficult to study surveillance policy thoroughly in terms of process, and to evaluate it in terms of content and effect.

2.1.1 Policy-making processes

A *process* perspective on policy-making uses a number of theories and approaches. It identifies and considers all the actors and organisations in a policy system and how the system turns policy inputs into policy activity and outcomes.[113] Within the overall system, policy theorists often point to a number of "stages" within a policy "cycle", starting with policy formation and ending with policy implementation and evaluation.[114] This is a useful set of analytical concepts, although the assumption of a linear or temporal sequence is arguable not often warranted. Nevertheless, by breaking the process down into a number of conceptual stages it is possible to organise empirical data about the actors and institutions that are active and influential at which stage in the policy cycle. In this way it becomes possible to identify organisations formally involved in developing public policy, such as governments, parliaments and other public agencies, and also the emergence of interests, groups and networks, which may seek to shape the policy-making process to their advantage.[115] Policy-making in this perspective is less about the content of policy and more about the negotiated processes by which policy content emerges.

Policy-oriented approaches to understanding policy-making emphasise the significance of the *processes* by which policies emerge and are implemented. The "policy process" is usually understood to mean the methods, strategies, techniques and (non-) decisions taken by actors or a group of actors to develop and implant a policy.[116] The policy process incorporates a range of complex relationships between actors, actions, institutions and discourses that combine to create policy output. For Ham and Hill, the focus on policy process necessarily emphasises "the stages through which issues pass… (and where)…attempts are made to assess the influence of different factors on the development of the issues. Studies of the policy process invariably show concern with policy content, but in the main they are interested in uncovering the main influences on policy formation".[117] Studies of the policy process

[113] Easton, David, *A Systems Analysis of Political Life*, John Wiley, New York, NY, 1965; Ham, Christopher, and Michael Hill, *The Policy Process in the Modern Capitalist State*, Brighton, Harvester Wheatsheaf, Brighton, 1993, p. 9.
[114] Hogwood, Brian W., and Lewis A. Gunn, *Policy Analysis for the Real World*, Oxford University Press, Oxford, 1984; Hogwood, Brian W., *Trends in British Public Policy*, Open University Press, Buckingham, 1992; Hogwood, Brian W., *From Crisis to Complacency: Shaping Public Policy in Britain*, Oxford University Press, Oxford, 1987.
[115] Richardson, Jeremy J., and A. Grant Jordan, *Governing Under Pressure*, Martin Robertson, Oxford, 1979; Sabatier, Paul A., and Hank C. Jenkins-Smith, (eds.), *Policy Change and Learning*, Westview, Boulder CO, 1993. For a discussion of th actors in privacy-protection policy systems, see Raab, Charles and Bert-Jaap Koops, "Privacy Actors, Performances and the Future of Privacy Protection", in Gutwirth, Serge, Yves Poullet, Paul De Hert, Cecile de Terwangne and Sjaak Nouwt (eds.), *Reinventing Data Protection?*, Springer, Dordrecht, 2009, pp. 207-221; and Bennett, Colin J. and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge MA, 2006, chapter 8.
[116] John, Peter, *Analysing Public Policy*, Pinter, London, 1998.
[117] Ham, Christopher, and Michael Hill, *The Policy Process in the Modern Capitalist State*, Brighton, Harvester Wheatsheaf, Brighton, 1993, p. 9.

are therefore largely concerned with the way policy emerges and advances over time, and with trying to understand the various forces and influences that shape policy advancement. A policy-process perspective is useful because it can help explain why one policy emerges and another does not. It also illuminates power structures, institutional processes, vested interests and influential actors in a process that is messy, complex and sometimes apparently irrational.

The most sophisticated process accounts of policy-making suggest that policy processes are not autonomous phenomena but are inextricably linked to pre-existing political, social and economic arrangements in which policy-makers operate. In this perspective, 'social structure' influences and constrains the development of policy[118] and policy emerges as a result of wider socio-economic forces in society. Similarly, 'ideas' or 'discourse' approaches to policy-making emphasise the importance of the creation and sharing of knowledge in and around policy processes,[119] and that policy-making takes place in the context of discourse, debate, dispute and discussion about different ideas and beliefs. Ideas influence policy development by acting as 'road maps' to help actors determine their own preferences, by alleviating policy problems by providing acceptable policy solutions and by encouraging habitual, routine behaviour.[120]

The focus on ideas and discourse highlights the role played by the media in contemporary policy-making processes. Henschel argues that the media plays a crucial role in defining problems and in constructing political and policy agendas.[121] As was suggested earlier in Task 2.2, this is because the media often sensationalises and amplifies certain issues and uses language that shapes our perception of an issue.[122] In this respect, representations of surveillance in the media play an important role in the policy process,[123] for example in the importance of realising national security. A number of authors have argued that whilst the media undoubtedly has a role in shaping policy agendas and hence policy outcomes, policy-makers and politicians use the media themselves to shape public opinion and consequentially mediate the development of a preferred policy.[124]

In relation to surveillance, the policy-process approach alerts us to consider the roles played by various actors in the public policy-making process, including those

---

[118] Marinetto, Mike, *Studies of the Policy Process: A Case Analysis*, Prentice Hall, Hemel Hempstead, 1999.

[119] Habermas, Jurgen, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, Polity Press, London, 1989.

[120] Goldstein, Judith, and Robert O. Keohane, (eds.) *Ideas and Foreign Policy: Beliefs Institutions and Political Change*, Ithaca, Cornell University Press, 1993.

[121] Henschel, Richard R. *Thinking About Social Problems*, Harcourt Brace Jovanovich, New York, 1990.

[122] See Cohen, Stanley, *Folk Devils and Moral Panics*, Paladin, London, 1972; and Edelman, Murray J., *Constructing the Political Spectacle*, Chicago University Press, Chicago IL, 1988.

[123] Kammerer, Dietmar, "Surveillance in literature, film and television", in Ball, Kirstie, Kevin D. Haggerty and David Lyon, (eds.), *Routledge Handbook of Surveillance Studies*, London, 2012, pp. 99-106.

[124] See, for example, O'Shaughnessy, Nicholas J., *The Phenomenon of Political Marketing*, Macmillan, London, 1990; Franklin, Bob, *Packaging Politics: Political Communications in Britain's Media Democracy*, Edward Arnold, London, 1994; and Cook, Fay Lomax, and Wesley G. Skogan, "Convergent and divergent voice models of the rise and fall of policy issues", in Protess, David and Maxwell E. McCombs (eds.) *Agenda Setting: Readings on Media Public Opinion and Policymaking*, Lawrence Erlbaum Associates, New Jersey, 1991.

formally charged with determining policy content, but significantly also those involved in shaping the process and those who have a vested interest in the development of policy. This would include official government and public agencies, politicians, the media, and also companies that manufacture, supply and maintain surveillance systems, the latter including the military and large multinational defence companies. The combination of these vested interests has been referred to as the "surveillance industrial complex",[125] the "political economy of surveillance",[126] and organisations contributing to "surveillant assemblages".[127] Additionally, the process approach encourages us to consider the roles played by language, discourse and those who seek to shape public opinion and understanding. In this respect, representations of surveillance in the media play an important role in the policy process, for example in the importance of realising national security.

2.1.2 Surveillance policy

In terms of the *content* of policy, despite the prevalence of technologically mediated surveillance practices in everyday life,[128] it is very rare for an explicit "surveillance policy" to exist, although we can identify decisions to put surveillance into practice and to use specific technologies. This is not to imply that surveillance is never a discrete policy area; rather, that it is the subject of policy in a range of different policy areas or settings, from national defence to transport and community safety, and at different jurisdictional levels from the local to the global. Later on, we focus upon data retention as an illustration of recent policy-making in the field of surveillance.

Within the policy studies literature, it is recognised that there does not necessarily have to be a written policy for a policy to exist. Instead a policy can be "course of action" arising from a series of intended activities or even as the unintended outcome of activities that are nonetheless carried out in the administration and implementation of services.[129] In this respect, the development of surveillance policy is subtle and multi-layered, possibly through the aggregation of individual decisions without an overarching and deliberate "policy". In the absence of a dedicated, overall surveillance policy, a key issue to consider is which policy environments are relevant to the development of surveillance and how the aim of surveillance varies across them. Typically, it is assumed that policy relating to surveillance would include national and local security, where surveillance technologies and systems are developed and deployed as part of explicit defence, intelligence and security

[125] Ball, Kirstie, Kevin D. Haggerty, and David Lyon, (eds.), "Introducing surveillance studies", in Ball, Kirstie, Kevin D. Haggerty and David Lyon, (eds.), *Routledge Handbook of Surveillance Studies*, London, 2012.
[126] Lyon, David, "Airports as data filters: Converging data systems after September 11th", *Journal of Information, Communication and Ethics in Society*, Vol. 1, No. 1, 2003, pp. 13-20.
[127] Haggerty, Kevin. D. and Richard V. Ericson, "The surveillant assemblage" *British Journal of Sociology* Vol. 51, No. 4, 2000, pp. 605-622.
[128] Murakami Wood, David, and C. William R. Webster, "Living in Surveillance Societies: The normalisation of surveillance in Europe and the threat of Britain's bad example", *Journal of Contemporary European Research*, Vol. 5, No.2, 2009, pp. 259-273.
[129] Parsons, Wayne, *Public Policy: An Introduction to the Theory and Practice of Policy Analysis*, Edward Elgar, Aldershot, 1995, p. 13; see also Hogwood, Brian W., and Lewis A. Gunn, *Policy Analysis for the Real World*, Oxford University Press, Oxford, 1984 for the various meanings of the term 'policy'.

policies.[130] This takes place at international, national and local policy-making making levels. For example, in the Stockholm Programme,[131] surveillance is explicitly part of the policy area and the implementation of European security systems. Surveillance as a policy area can also be assumed to be part of national defence and security in that it forms part of the arsenal of techniques used for counter terrorism, intelligence gathering and national security, and as a central feature in the development of technologies and policy that involve explicit surveillance technologies, such as the UK national CCTV strategy.[132] At the local level, surveillance may form part of local strategies for service delivery, especially in relation to community safety and the deterrence of criminal and undesirable behaviour.[133] At any level, eyes, ears and brains still remain useful "technologies" of surveillance.

Beyond the domain of security and safety, surveillance technologies and practices have entered a range of other policy arenas and service environments. Explicit surveillance systems are evident in transport[134] and education[135] settings, as well as at large-scale events,[136] such as the quadrennial Olympic Games. This is especially the case in relation to video surveillance cameras, which have diffused into a wide range of public-service settings.[137] A more nuanced understanding of surveillance would include a range of technological database systems used in the provision of "eGovernment", where surveillance practices are implicit and relate more specifically to the exchange of personal information required for service delivery.[138] In that understanding, surveillance is embedded as part of the processes involved in the use of new technologies for service provision, and as such is part of many policy areas. The point emerging from these considerations is that the involvement of these systems and practices can be taken as evidence of the kind of deliberate activity, including the allocation of resources, that is usually comprehended within the scope of studies of policy-making. As such, questions of accountability, transparency, and

[130] Council of the EU, *Interim Report on the Evaluation of National Anti-Terrorist Arrangements*, 14306/0/04, Brussels, 23 November, 2004.
[131] Wright, David, Michael Friedewald, Serge Gutwirth, Marc Langheinrich, Emilio Mordini, Rocco Bellanova, Paul De Hert, Kush Wadhwa and Didier Bigo, "Sorting out smart surveillance", *Computer Law and Security Review*, Vol. 26, No. 4, July 2010.
[132] Gerrard, Graeme, Garry Parkins, Ian Cunningham, Wayne Jones, Samantha Hill and Sarah Douglas, *National CCTV Strategy*, London, Home Office, 2007.
[133] Armitage, Rachel, *To CCTV or not to CCTV? A Review of Current Research into the Effectiveness of CCTV Systems in Reducing Crime*, NACRO Community Safety Practice Briefing, NACRO, London, 2002.
[134] Svenonius, Ola, "The Stockholm Security Project: Plural policing, security and surveillance", *Information Polity*, Vol. 17, No.1, 2012, pp. 35-43.
[135] Taylor, Emmeline, "I spy with my little eye: the use of CCTV in schools and the impact on privacy", T*he Sociological Review*, Vol. 58, No. 3, 2010.
[136] Boyle, Philip, Kevin D. Haggerty, Spectacular Security: Mega Events and the Security Complex, *International Political Sociology*, Vol. 3, No. 3, 2009, pp. 257-274.
[137] See Webster, C. William R., "Closed circuit television and governance: the eve of a surveillance age", *Information Infrastructure and Policy*, Vol. 5, No. 4, 1996, pp. 253-263; Webster, C. William R., "The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK", *Surveillance and Society*, CCTV Special (eds. Norris, McCahill and Wood), Vol. 2, Nos. 2-3, 2004, pp. 230-250; Webster, C. William R., "CCTV policy in the UK: reconsidering the evidence base", *Surveillance and Society* , Vol. 6, No. 1, 2009, pp.10-22; and Webster, C. William R., Eric Töpfer, Francisco R. Klauser and Charles D. Raab (eds.), *Video Surveillance Practices and Policies in Europe*, IOS Press, Amsterdam, 2012.
[138] Webster, C. William R., "Public Administration as Surveillance", in Ball, Kirstie, Kevin D. Haggerty and David Lyon, (eds.), *Routledge Handbook of Surveillance Studies*, London, 2012, pp. 313-320.

legitimacy apply to surveillance policy just as much as in other policy areas, even if these evaluative criteria yield different answers in the case of surveillance. In democratic regimes, there is therefore a tension between surveillance and the values in terms of which such political systems typically like to be measured.

This perspective on surveillance, which incorporates those practices and technologies that collect and process personal information, makes data protection and privacy key surveillance policy-making areas. Policy-making in these areas is well established, and within Europe, takes place at the EU and national levels.[139] At the EU level, this includes the Article 29 Working Party,[140] the institutions of the European Union, and pieces of legislation such as the 1995 European Directive on Data Protection. At the national level, policy-making content includes the development of national legislation and regulation (for example, the Data Protection Act 1998 (DPA) in the UK) and the creation of an agency responsible for data protection policy and regulation (for example, in the UK, the Information Commissioner's Office (ICO)). In the UK, under the DPA and other legislation including the Regulation of Investigatory Powers Act (RIPA) 2000, there is a cluster of regulators in the surveillance field besides the ICO: an Interim CCTV Regulator, and Interception of Communications Commissioner, and a Chief Surveillance Commissioner. This somewhat confused bundle of activity and responsibility for has been called into question,[141] and there are moves afoot to create a "strategy for a more joined up approach to the regulation of surveillance which impacts on personal privacy".[142] In the area of surveillance, organisational profusion at the level of policy-implementation and enforcement has implications for the transparency and accountability of surveillance practices in democratic regimes.

2.1.3 Surveillance policy: data retention

We now move from the general to the particular in focusing on a specific recent example of policy-making content and process: data-retention policy in the EU.

2.1.3.1 *Data retention as a form of surveillance*

Deliverable 1.1 outlined several types of surveillance and the technologies they involve; these types include watching, listening, locating, detecting, and personal data monitoring ("dataveillance"). It was pointed out that some types are targeted on particular individuals, groups, or social categories of persons, while others operate generically. There is, however, a further practice that is defined in terms of *time* rather than in terms of a particular technology, a direction of attention, or a specific purpose, and that involves practices further downstream from the collection of data by whatever means. This practice – data retention – involves the storage of information, whether personally identifiable or not, for specified or unspecified periods of time.

---

[139] Bennett, Colin J., and Charles D. Raab, *The governance of Privacy: Policy Instruments in Global Perspective*, The MIT Press, Cambridge, MA, 2006.

[140] Article 29 Working Party: http://ec.europa.eu/justice/policies/privacy/workinggroup/wpdocs/index_en.htm.

[141] Raab, Charles and Benjamin Goold, *Protecting Information Privacy*, Research Report 69, Equality and Human Rights Commission, London, 2011; House of Lords, Select Committee on the Constitution, 2nd Report of Session 2008-09, *Surveillance: Citizens and the State*, HL Paper 18-I, The Stationery Office, London, 2009.

[142] http://www.ico.gov.uk/about_us/boards_committees_and_minutes/~/media/documents/library/Corporate/Notices/20120123_mb_meeting_Information_Rights_Report.ashx.

Data retention is part of a specific form of surveillance even if it does not come to mind immediately as a surveillance method. The reason that data retention is not closely associated with surveillance in the public mind might be the fact that data retention is a non-visual, non-real time, empirically unnoticeable form of observation of citizens that people normally may "face" only in statutory provisions or media narratives. Yet data retention is intrinsically involved with surveillance, more precisely to dataveillance, since it enables states to collect data related to their citizens' activities and to use these data to understand and control or assist the subjects of monitoring.[143] The retention of traffic and location data perfectly meets the definition of surveillance as presented by David Lyon: "a focused, systematic, and routine attention to personal details in the end to individuals for the purposes of influencing and protecting those whose data have been garnered".[144]

Owing to its *quantitative* and *qualitative* characteristics, data retention facilitates *mass* and *pervasive* surveillance. As social interactions are conducted today mostly via electronic communication networks, a huge amount of information that is inevitably produced in citizens' everyday lives is subject to data retention. In particular, the observation of Internet activities represents a uniquely powerful form of surveillance, since the web provides multiple spaces for individuals to be engaged in personal activities: contacting each other, sharing personal ideas, engaging in business transactions, shopping, etc.[145] European data retention law does not allow the retention of the content of communications,[146] and "only" location records and traffic data are to be stored;[147] these can be used for creating clear tracking profiles of targeted persons.[148] It is widely held that these "footprints" may give a very rich, comprehensive picture of individuals' personal habits, preferences, interactions, associations, etc.[149] Findings of a study from the Massachusetts Institute for

[143] Roberts, Hal and John Palfrey, "The EU Data Retention Directive in an Era of Internet Surveillance", in Deibert Ronald J., John Palfrey, Rahal Rohozinski and Jonathan Zittrain (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, MIT Press, Cambridge, MA: 2010, p. 35.

[144] Lyon, David, *Surveillance Studies, An Overview*, Polity Press, Cambridge, 2007, p. 14.

[145] Mitrou, Lilian, "The impact of communications data retention on fundamental rights and democracy – the case of EU Data Retention Directive", in Haggerty, Kevin D. and Minas Samatas (eds.), *Surveillance and Democracy* Routledge, Abingdon, 2010, p. 129. See also Huey, Laura and Richard S. Rosenberg, "Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention" *Canadian Journal of Criminology and Criminal Justice*, Vol. 46, No. 5, 2004, p. 603.

[146] However, one can reasonably assume that the increasing storage and computing capacity and its decreasing costs will lead to demands for retaining the content of the communication as well.

[147] For detailed discussion of these categories of data, see Rauhofer, Judith, "Just because you're paranoid, doesn't mean they're not after you: legislative developments in relation to the mandatory retention of communications data in the European Union" *SCRIPT-ed*, Vol. 3, No. 4, 2006, pp. 323-324.

[148] To see the extent to which telecommunications data enable individuals to be followed, see the website of the German daily *Die Zeit* (http://www.zeit.de/datenschutz/malte-spitz-vorratsdaten). An interactive map shows the information that the combination of geographical location and Internet traffic data tracked within a six-month period provides for the surveillors. The infograph was prepared from personal data related to the German Green politician, Malte Spitz, who went to court to obtain six-months' worth of data from his Internet and mobile phone service provider, Deutsche Telekom. By pushing the play button, viewers can begin a detailed journey through six months of his life.

[149] For instance, Farrell, Maria, "Communications data retention in the UK", *E-commerce Law and Policy*, Vol. 3, 2001, p. 11. See also Rauhofer, Judith, "Just because you're paranoid, doesn't mean they're not after you: legislative developments in relation to the mandatory retention of communications data in the European Union" *SCRIPT*ed, Vol. 3, No. 4, 2006, pp. 323-324.

Technology showed that traffic data allow the revelation of a user's circle of colleagues, friends, and acquaintances with 90 per cent accuracy. They also allow a prediction whether one will meet a person in the next 12 hours also in 90% of cases. Moreover, traffic and location data only of the previous month allows a prediction of one's location in the next 12 hours in 95% of cases, and they also tell one's general activities in the next 12 hours with 80% accuracy.[150]

The pervasiveness of data retention is associated not only with the range of the data being kept but also with the involvement of private sector entities in law enforcement. Drawing upon communication service providers' (CSPs') knowledge, expertise, human resources, and technical support for law enforcement purposes greatly expands the state's surveillance capacities, and in sense shifts the police presence beyond the state into the private sphere.[151] The obligation of CSPs to assist law enforcement agencies in gathering and analysing data on individuals does not only result in a massive growth of the role of the state in social control but also blurs the boundaries of responsibility for posing dangers to privacy between the government and private actors.

2.1.3.2 *The emergence of data retention on the EU policy agenda*

Among the relatively wide scale of dataveillance tools existing today in the EU surveillance regime, the Data Retention Directive of 2006[152] has given rise to the most intense controversy. Until 2004 the issue of a common approach for countering organised crime and terrorism did not gain prominence on the EU policy agenda.[153] This is not surprising when considering that the inherent and primary aim of the establishment of the EU was the economic and monetary integration of Member States. Attempts to counter global security threats fall far beyond the scope of this aspiration. True enough, political deliberations on data retention had already taken place in Europe in the early 2000s, especially after the 9/11 terrorist attack of 2001 in New York, when President George W. Bush asked the EU to assist the US in its international effort against terrorism. The long list of proposed actions for EU-US counter-terrorism co-operation included the implementation of data retention, but in a restricted form that would have pertained only to certain critical information requested for law enforcement authorities (data preservation).[154] Although a number of Member States had already adopted data retention statutes at that time, the EU was reluctant to harmonise the diverging data retention regimes until 2004 despite external pressure. The radical change was triggered by the terrorist bombing attacks in Madrid and London that directed lawmakers' attention to EU mechanisms for the

[150] http://reality.media.mit.edu/dyads.php and http://reality.media.mit.edu/user.php.

[151] For an analysis on the state efforts at redistributing and expanding policy functions with private sector and its impact on surveillance see Huey, Laura and Richard S. Rosenberg, "Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention" *Canadian Journal of Criminology and Criminal Justice*, Vol. 46, No. 5, 2004, pp. 599-603.

[152] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC*, L 105/54, 13.4.2006.

[153] Flynn, Cathal, "Data Retention, the Separation of Power in the EU and the Right to Privacy: A Critical Analysis of the Legal Validity of the 2006 Directive on the Retention of Data", *University College Dublin Law Review* Vol. 8, No. 1, 2008, p. 1.

[154] See the letter of Mr James J. Foster, Deputy Chief of the United States Mission to the former President of the European Commission, Mr Romano Prodi: http://www.statewatch.org/news/2001/nov/06Ausalet.htm.

intensification of the collection, storage and exchange of personal data.[155] Adopting the Directive in 2006 was a direct legal manifestation of this attempt. The main point of its adoption was the standardisation of national regulations of the way in which traffic data are stored by CSPs. By choosing the form of a Directive from the range of possible legally binding instruments, lawmakers provided considerable leeway for Member States in implementing the mandatory data retention requirements. The Directive obliges telephony suppliers and internet service providers (ISPs) to retain, for up to 2 years, communication traffic and location data, and information about subscribers, for the purposes of investigating, detecting and prosecuting serious crime.

2.1.3.3 *Criticisms of data retention: output and outcome*

Data retention policy in general, and in EU's Data Retention Directive in particular, have been facing heavy criticism from many societal and policy actors, and from many perspectives. No one questions, however, the legitimacy of purpose, i.e., that a democratic regime must be engaged in fighting crime. However, a wide range of regulatory or non-regulatory instruments are available, according to surveys among victims and criminals, official pronouncements, media narratives, and academic articles. Among these, only one possible response is the storage of all individuals' communications data. Therefore, the main criticisms focus on the rationality, efficiency, necessity and proportionality of data retention surveillance in the light of both the *output* of data retention (i.e., the extent to which the goal of combating crime has been achieved) and the *outcome* of storing telecommunications data (i.e., the overall social, economic, political, legal and other costs), with special emphasis on the encroachment upon the right to privacy of individuals. Evaluations of these illustrative aspects of policy *content* are important parts of the *process* of policy-making.

2.1.3.3.1 *The output of data retention policy: effectiveness*

As explained above, the output of data retention policy raises the questions of the rationality and effectiveness of data retention, i.e., the question concerning the extent to which the goal of combating crime and terrorism can be achieved with the mandatory storage of communications data.

In theory, traffic and location records might be quite important in law enforcement procedures by providing key information both for detecting organised crime activities and for granting evidences of guilt (or even innocence) before the courts. Indeed, it is without doubt that these records might play an especially important role in identifying criminals, especially those who use screen names or pseudonyms on the Internet.[156] Nevertheless, serious doubts have been raised about the reliability of the retained data. As Caspar Bowden, the former Director of the Foundation for Information Policy Research (FIPR) argues, "traffic data cannot prove the identity of the author of an e-mail or the person who actually made a particular call. … No amount of traffic

[155] See the Declaration on Combating Terrorism adopted by the European Council on March 25, 2004 (http://www.consilium.europa.eu/uedocs/cmsUpload/DECL-25.3.pdf), and the EU's Plan of Action on Combating Terrorism (http://ue.eu.int/uedocs/cmsUpload/EUplan16090.pdf). See Konstandinides, Theodore, "Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem", *European Law Review* Vol. 35, No. 5, 2011, pp. 722-724.

[156] Solove, Daniel. J, "Reconstructing the electronic surveillance law", *George Washington Law Review*, Vol. 72, 2003-2004, p. 1284.

data by itself can prove an alibi, because while it may be persuasive circumstantially, it does not eliminate the possibility that a bogus trail has been carefully laid by an accomplice".[157] A study prepared by the US Center for Democracy and Technology also argues that, as a result of the same trend in address allocation, IP address data may no longer reliably identify individual end-user devices, thus reducing the effectiveness of data retention mandates.[158]

In addition to these points, the available quantitative and qualitative information based upon the practical experiences of the implementation of the Directive failed to prove that data retention is a necessary instrument to fight serious crime. Here it should be noted that Member States have scarcely fulfilled their legal obligation to provide statistics on the use of data retained under the Directive,[159] thus limiting the ability to assess precisely the usefulness of data retention requirements. Although Member States have generally reported data retention valuable and in some cases indispensable, as revealed in the evaluation report of the European Commission on the Directive,[160] the available statistical information is unable to provide relevant evidence for its effectiveness. No Member State has provided evidence that could establish that data retention is useful for fighting crimes. Therefore, Member States' general evaluations can be deemed political, rather than evidence-based statements.[161]

Indeed, the existing statistics that can be relied on even underpin the opposite: that indiscriminate and blanket telecommunications data retention has had no statistically significant effect on crime or crime-solving trends. For instance, according to the official German policy crime statistics of 2011,[162] with the Data Retention Directive in force, more serious criminal acts were registered than before (1,359,102 in 2007, and 1,422,968 in 2009) and a smaller proportion, even, were cleared up (77.6% in 2007, and 76.3% in 2009). Several other studies conducted by independent organisations demonstrate that blanket data retention has proven to be superfluous

---

[157] Bowden, Caspar, "Closed Circuit Television for Inside Your Head: Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation, *Computer and Telecommunications Law Review*, Vol. 8, 2002; Rauhofer, Judith, "Just because you're paranoid, doesn't mean they're not after you: legislative developments in relation to the mandatory retention of communications data in the European Union", *SCRIPT-ed*, Vol. 3, No. 4, 2006.

[158] This study accurately explains that many IP addresses no longer uniquely identify users and end-user devices. "Data Retention Mandates: Changes in Internet Addressing Technology Affect Cost, Effectiveness, and Proportionality", Center for Democracy & Technology, Sept. 2011, www.cdt.org%2Ffiles%2FCDT_Data_Retention-NAT_Paper.doc&ei=jO56UNyjHI7KtAbH3IH4Ag&usg=AFQjCNGbC1adj9md4LOchqzrOYzAeUZ93g>

[159] Article 10 of the Data Retention Directive stipulates that Member States shall ensure that the Commission is provided on a yearly basis with statistics on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or a public communications network.

[160] According to the Evaluation Report from the European Commission to the Council and the European Parliament on the Data Retention Directive, the Czech Republic considered data retention "completely indispensable in a large number of cases"; Hungary said it was "indispensable in [law enforcement agencies'] regular activities"; Slovenia stated that the absence of retained data would "paralyze the law enforcement agencies' operation"; a United Kingdom police agency described the availability of traffic data as "absolutely crucial (…) to investigating the threat of terrorism and serious crime". See COM(2011)225, 18.4.2011 < http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52011DC0225:EN:HTML>, p. 23.

[161] See the EDRI's Shadow report on the Data Retention Directive, 17.4.2011 <http://www.edri.org/files/shadow_drd_report_110417.pdf>, p. 9.

[162] Created by the German Federal Crime Agency (BKA), available at http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf.

since the large number of requests for retained data had virtually no effect on the detection of crimes. This picture is confirmed by the findings of the Max Planck Institute for Foreign and International Criminal Law, which concluded that blanket data retention in Germany might only bring a difference to 0.002% of criminal investigations at most.[163] Research conducted at Erasmus University Rotterdam, studying 65 criminal cases in terms of the usefulness of data retention for law enforcement purposes, found that that requests for traffic data could "nearly always" be served even in the absence of blanket data retention.[164]

2.1.3.3.2 *The outcome of data retention policy: overall costs*

The outcome of the introduction of data retention rules in terms of their intended and unintended costs has led to widespread European criticism from many different groups and for many different reasons. Central to these criticisms lie the questions of necessity and proportionality of the mandatory storage of all traffic and location data relating to all EU individuals in the European Union especially for such a long time that is prescribed by the Directive (6-24 months).

Under the flag of the protection of fundamental rights and freedoms, political actors, worldwide co-ordinated public protests, as well as academics have repeatedly argued that data retention undermines democratic practises and free society by undermining the right to privacy, the right to remain anonymous, the presumption of innocence, and social confidence. Several surveys conducted by independent organisations suggest that the pervasive surveillance performed by data retention changes individuals' social behaviour, jeopardises their autonomous decision-making, discourages their participating in public debate, and chills their personal activities. Data retention may result in all the potential harms that are associated with privacy invasive tools in general in the academic literature.[165] The practical experience of the implementation of the Directive led even the European Data Protection Supervisor itself to conclude that the Directive is "the most privacy invasive instrument ever adopted by the European Union." [166]

As for the social effects, a poll of 1002 Germans in 2008 found that indiscriminate data retention has a strong chilling effect on the use of mobile phones, e-mail and other Internet activities. The findings show that more than half the respondents (52%)

---

[163] Forschungsbericht des Max-Planck-Instituts für ausländisches und internationales Strafrecht <http://dip21.bundestag.de/dip21/btd/16/084/1608434.pdf>. For an interpretative summery of the findings see the EDRI's Shadow report on the Data Retention Directive, ibid, p. 14.

[164] Erasmus University Rotterdam, "Wie wat bewaart heeft wat" ("Who retains something has something"), 2005, <http://www.erfgoedinspectie.nl/uploads/publications/Wie%20wat%20bewaart.pdf>, p. 43.

[165] For detailed analyses on potential harms of data retention in the academic literature, see e.g., Mitrou, Lilian, "Communications Data Retention: A Pandora's Box for Rights and Liberties?", in Acquisti, Alessandro, Stefanos Gritzalis, Costas Lambrinoudakis and Sabrina De Capitani di Vimercati (eds.), *Digital Privacy: Theory, Technologies, and Practices*, Auerbach Publications, Boca Raton, FL, 2007, p. 429-430; Munir, Abu Bakar and Siti Hajar Mohd Yasin, "Retention of communications data: a bumpy road ahead", *The John Marshall Journal of Computer and Information Law*, Vol. 22, No. 4, 2004, pp. 757-758. See also Newland, Erica and Cynthia Wong, "Data Retention Mandates: A Threat to Privacy, Free Expression, and Business Development", Center for Democracy & Technology, Washington, DC,Oct. 2011, <http://cdt.org/files/pdfs/CDT_Data_Retention_Paper.pdf>.

[166] See Peter Hustinx' presentation, "The moment of truth for the Data Retention Directive", delivered at the conference on "Taking on the Data Retention Directive" Brussels, 3 December 2010. <http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-12-03_Data_retention_speech_PH_EN.pdf>

would refrain from confidential contacts if they needed help: for example, from contacting a marriage counsellor, a psychotherapist, or a drug-misuse counsellor by phone or e-mail. Moreover, 11% of the respondents said that they had already abstained from using a telephone, mobile phone or e-mail on certain occasions, and 6% believe they receive less communication since the beginning of data retention.[167] However, the poll also revealed that 48% still think that data retention is a necessary step for crime prevention.

Possible negative impacts of data retention on freedoms of expression and the press are also suggested. Traffic data can easily be misused to spy on journalists and to expose their sources and whistleblowers. What makes matters worse from this perspective is the lack of guarantees of high data security in order to guard against misuses. Cases such as the widely known abuse of T-Mobile, whose staff sold millions of records from thousands of customers on the black market,[168] do not enhance trust in CSPs who are responsible for taking adequate safety measures in order to protect personal data.

Acting as guardians of their constitutional system, the highest judicial authorities of several Member States have ruled that the implementation of the Directive in domestic law was unconstitutional.[169] So did the Constitutional Court of Romania, Germany, the Czech Republic, as well as the Irish High Court, but a number of cases are pending before other national courts.[170] These courts had to act under enormous pressure to uphold constitutional values. In Germany, for instance, due to the tireless campaign of the German Working Group on Data Retention, 34,451 citizens took part as plaintiffs in the constitutional complaint procedure before the Federal Constitutional Court. All these courts concluded that the relevant national laws did not ensure adequate safeguards in order to balance between the serious infringement of the right to privacy and other freedoms affected, on the one hand, and the legitimate purpose of combating crime, on the other.

Apart from the legal and societal risks, underlying cost-benefit analyses have also raised serious concerns. Such existing analyses question whether data retention represents a more efficient allocation of resources (on a cost-benefit basis) than if such resources were put to alternative use. Maria-Helen Maras concludes that the economic advantages of pursuing EU-wide data retention are more than outweighed by its economic disadvantages. She shows that the Directive may negatively impact upon competition and other economic policies in the EU by leading consumers to use international webmail services (that is, non-EU providers), and new (and even existing) market participants to take their businesses elsewhere. In all, she found the Directive a disproportionate measure.[171]

---

[167] *Opinions of citizens on data retention*. Forsa Institute, 2 June, 2008., p. 3. Available at http://www.vorratsdatenspeicherung.de/content/view/228/79/.

[168] BBC News: http://news.bbc.co.uk/2/hi/uk_news/8364421.stm.

[169] For a detailed analyses of judicial challenges, see: Konstandinides, Theodore, "Destroying democracy on the ground of defending it?: The Data Retention Directive, the surveillance state and our constitutional ecosystem", *European Law Review*, Vol. 35, No. 5, 2011, pp. 727-733.

[170] The actions of some Member States' national courts are described in Task 2.3.

[171] Maras, Maria-Helen, "The economic costs and consequences of mass communications data retention: is the Data Retention Directive a proportionate measure?" *European Journal of Law and Economics*, Vol. 33, No. 2, 2012, pp. 447-472.

2.1.3.4 Data retention policy: concluding remarks

The case study above has provided a brief description of the policy of data retention as an example of surveillance and a brief analysis of evaluative criticisms. Putting these criticisms together (and not putting them aside, as policy-makers tend to do), they points to the conclusion that data retention has minimal effects within, but significant effects beyond its explicit scope, and that these unintended consequences have been shown to be costly in several dimensions. In Deliverable 2.3, we describe the response that has occurred in several Member States over the constitutionality and legality of the Directive's implementation and other measures of data retention, in the context of fundamental rights. The recent interest in the "right to be forgotten" as part of the proposed reform of EU data protection law is not unrelated to the question of the retention of data insofar as this right would enable citizens further to realise their existing rights to challenge the collection of personal data and obtain its erasure. It would strengthen the well-established requirement, stated in Article 6(e) of the Data Protection Directive 95/46/EC, that personally identifiable data be held "for no longer than is necessary" unless stored for longer periods for historical, statistical or scientific use. In order to give better effect to this statutory right, writing deletion more strongly into law and possibly designing expiration dates into information systems have been proposed and discussed, although the rhetoric of the proposed new "right" has aroused scepticism. Koops, for example, argues that "there is no consensus what exactly a right to be forgotten means, and its status – as a right, interest, or value; in need of reinforcement or to be created from scratch – is unclear." [172] Whether the "right to be forgotten" will remain largely as an inspirational mantra without effective legal embodiment is not certain. Nonetheless, it is a countervailing force against the prevailing trend underlined by the Chairman of Google, Eric Schmidt: "Pretty soon, in a year or two, with the phones many of you have already and the tablets, you will never forget anything. Starting soon it will be possible to remember the hotels you went to, the pictures you took, the friends you met, because computer memories last forever."[173]

2.1.4 POLICY-MAKING AND SURVEILLANCE: CONCLUSION

The brief discussion of surveillance policy-making has pointed up several salient issues for a political perspective on surveillance. These include not only the way policies are made, implemented and evaluated, but also their impact upon society, the

[172] Koops, Bert-Jaap "Forgetting Footprints, Shunning Shadows, a Critical Analysis of the 'Right to be Forgotten' in Big Data Practice'', *Script*ed, Vol. 8., No. 3, December 2011, p. 230. Among the scholarly literature, see Mayer-Schönberger, Viktor, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, Princeton NJ, 2009; Rouvroy, Antoinette, "Réinventer l'art d'oublier et de se faire oublier dans la société de l'information?", at: http://works.bepress.com/cgi/viewcontent.cgi?article=1004&context=antoinette_rouvroy, accessed 19/12/12. Widening the scope of deletion through 'objective and automated' means has been proposed as part of the right to be forgotten by the European Data Protection Supervisor: see "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'", OJ 2011/C, 22.6.11, paras. 88-89, at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2011:181:0001:0023:EN:PDF, accessed 19/12/12.

[173] Quoted in *The Guardian*, 16 February 2011, p. 24.

political system, rights and freedoms. The accountability and transparency of policy and practice are integral to these considerations, as is the rule of law. The next sections examine these crucial dimensions of the political perspective.

2.2 ACCOUNTABILITY

We continue with a discussion of accountability. As the thrust of our argument in Chapter 2 makes clear, good policy-making requires debate, accountability and an evidence-based link between problems and solutions. In the case of surveillance technologies, security theatre, and the need for fast, visible policy responses to events and fears, public debate and policy deliberation are being short-circuited, raising questions about the democratic accountability of our political systems.
The accountability of rulers to their publics is a central pillar of the modern democratic state, manifested in elections and other forms of relationship through which office-holders justify their claim to continue in office by subjecting their record of performance to the scrutiny and approval of the electorate. Although perhaps less exemplified in practice, the principle of accountability is also prominent in the corporate economy, in which managers and executives periodically put their case for the continued support of shareholders. In the world of surveillance, which involves the performance of those who collect, process, and communicate information relating to persons, the question of accountability is less straightforward and accountability practices are far less developed. Yet there is a growing mood that holds that surveillance users ought to be accountable to those whose information they handle and to others who may be affected by surveillance practices. How this drive for accountability will relate to other forms of surveillance scrutiny and regulation is yet to be determined.

"Accountability", however, is an elusive concept.[174] It is a familiar term in English, but may lead to misinterpretation because it may differ in other languages and under different legal jurisdictions, as the EU's Article 29 Working Party, established under the EU Data Protection Directive 95/46/EC[175], pointed out. They note that other terms could be "reinforced responsibility", "assurance", "reliability", "trustworthiness" and "obligation de rendre des comptes".[176] Mulgan distinguishes between *internal* and *external* aspects of accountability.[177] He argues that in the governmental world, *internal* accountability or responsibility has to do with the professionalism and personal morality or conscience of public servants and others in the exercise of their functions, and especially of their discretion. But within an organisation, it also involves accountability to hierarchical superiors, and therefore there is, in a sense, an element of externality for the individual official, beyond her own personal morality. On the other hand, *external* accountability more conventionally involves some agent,

[174] Bovens, Mark, "Analysing and Assessing Accountability: A Conceptual Framework", *European Law Journal*, Vol. 13, No. 4, 2007, pp. 447-468.
[175] European Parliament and the Council, *Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281, 23.11.1995
[176] Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, Adopted on 13 July 2010. WP 173, paras. 21-23.
[177] Mulgan, Richard, '"Accountability": An Ever-Expanding Concept?', *Public Administration*, Vol. 78, No. 3, 2000, pp. 555-573.

external to the organisation, in assessing and investigating actions or failures to act, and in imposing sanctions, but these processes will also touch on professional and personal factors that explain the action. The internal and external aspects are therefore connected in complex ways, but the conceptual distinction between having and not having to account to someone else for one's actions remains. In any case, the crucial question identified by Bennett is "[a]ccountability for what and to whom?"[178] It is especially the external form of accountability that appears relevant in the case of privacy protection, because it corresponds more closely to the relationship of data controllers to data subjects, as well as to regulators and the general public. On the other hand, there is an important current trend to develop internal accountability within data-controlling organisations, including codified elements of ethical conduct for individuals to practice within a regime of information governance, as will be explained below.

The 14th Guideline – the "Accountability Principle" – of the prominent 1981 OECD data protection Guidelines says that data controllers should be accountable for measures that give effect to data protection principles. The 62nd explanatory paragraph of the Guidelines says that 'accountability' refers to legal sanctions as well as the requirements set out in codes of conduct.[179] Most of the existing strategies of surveillance regulation, including instruments for data protection, have emphasised legal and technical arrangements for limiting surveillance and for sanctioning excesses in the activities that comprise surveillance. Laws and mechanisms to enforce legal compliance, self-regulatory instruments including codes of practice, and technological tools and design have attracted the most attention from policy-makers and commentators;[180] this repertory is discussed in further detail later on, where we focus upon the governance of surveillance. But as will be discussed, some recent developments in this field are concerned more directly with foregrounding accountability requirements themselves.

If they are crafted properly and accompanied by sufficient oversight and enforcement powers, the existing array of types of regulatory measure can exert a powerful influence to limit surveillance in the interests of liberty and democracy. For laws and self-regulation to have this effect, they should be couched in organisational environments and cultures in which information governance is taken seriously. The definition of "information governance" espoused by Gartner, the IT research and advisory group, is "the specification of decision rights and an accountability framework to encourage desirable behaviour in the valuation, creation, storage, use, archival and deletion of information".[181] In this context, the organisational practices, including processes of accountability in which those who gather and control personal data engage, have received increasing attention in more recent years. A further element is the need for organisations to take seriously the requirement imposed upon

[178] Bennett, Colin., 'International privacy standards: Can accountability ever be adequate?', *Privacy Laws & Business International Newsletter*, Issue 106, August 2010, p.22.
[179] Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris: OECD, 1981.
[180] Bennett, Colin J. and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge, MA, 2006.
[181] Logan, Debra, 'What is Information Governance? And Why is it So Hard?', Gartner Blog, January 11, 2010, http://blogs.gartner.com/debra_logan/2010/01/11/what-is-information-governance-and-why-is-it-so-hard/, accessed 07/07/12).

data controllers by the EU Data Protection Directive 95/46/EC[182] in terms of the security of data processing, which involves not only technical measures such as encryption, passwords, and other tools, but also "appropriate … organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, … and against all other unlawful forms of processing".

Increasing attention can also be attributed in part to the proliferation of data breaches in many countries in the 2000s, violating laws and principles of data protection and reducing the trust in which the public holds private and public sector users of surveillance. The spotlight has turned to the scrutiny of organisational procedures that arbitrate the extent to which data controllers and other surveillance operators are equipped to apply the criteria of privacy protection and the safeguarding of other human values to their information practices when they are the custodians of individuals' personal information. The promotion of better processes of data handling has been one important result. In the UK, for example, following a host of central-government breaches, the Cabinet Office Data Handling Report laid down many mandatory requirements aimed to strengthen accountability, particularly at senior organisational levels in government departments. It did this by establishing new roles, by ensuring that information risks are considered early on, and by seeking to "foster a culture of individual accountability throughout the organisation, with targeted, relevant, role-based training to ensure that employees have a clear understanding of how to use and share information securely".[183] A further report charted progress in implementing these measures in the context of managing information risk, and renewed the emphasis on accountability and clarifying lines of responsibility.[184] A major review on data sharing in government also subscribed to the view of accountability, as well as transparency and responsibility, as being a prime requirement in information governance.[185]

All these developments beneficially promote accountability, but they appear to reproduce a common and misleading understanding of accountability by eliding this concept with 'responsibility' for undertaking certain actions, for example, in regard to surveillance or data processing. Thus a 2002 Canadian Treasury Board document on privacy impact assessment (PIA) includes a section on "Accountability" in which it states that that senior officials in public organisations and others are 'responsible for' carrying out and ensuring the implementation of the PIA policy through the performance of specific activities: in other words, what they must *do*.[186] We can thereby only understand who is supposed to do what – a form of role description that may be useful in bringing sanctions or rewards to bear, depending on the quality of the performance, but that goes no further in describing any process of accountability for this performance.

[182] European Parliament and the Council, Directive 95/46/EC of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, Article 17(1).
[183] UK Cabinet Office, *Data Handling Procedures in Government: Final Report, June 2008*, pp 9, 13.
[184] UK Cabinet Office, *Protecting Information in Government*, January 2010.
[185] Thomas, Richard and Mark Walport, *Data Sharing Review Report*, 11 July 2008.
[186] Government of Canada, Treasury Board of Canada Secretariat, *Privacy Impact Assessment Policy*, section on accountability, 2 May 2002.

But accountability is not easily achieved because, as a UK Parliamentary report observed, the trend towards data sharing in the public sector has shown the difficulty of tracing the flow of personal data and of maintaining clarity about who is responsible for it and how they can be held accountable.[187] A leading UK legal expert has argued that the constitutional convention that government ministers are accountable to Parliament could mean that surveillance activities undertaken under ministerial authorisation should be subjected to parliamentary scrutiny.[188] This indicates that the question of who should be held accountable can be asked at all levels of surveillance systems, and does not only pertain to back-room or street-level operatives, or to systems managers and controllers at higher levels or organisational hierarchies. Parliamentary or other forms of external scrutiny help to cast light on practices and to increase the amount of public information about surveillance that is available in a democracy. Thus the principle of accountability is interdependent with the principle of transparency in the effort to retain public confidence, as the UK Information Commissioner implied in insisting that "public authorities must remain transparent and accountable if they are to retain the trust of the public they serve".[189] Transparency is discussed later, but its relationship to accountability needs to be articulated more precisely, in terms of a better understanding of the meaning of accountability, which is explored shortly.

Accountability moved centre-stage in 2012 in the current phase that is expected to lead to the adoption of a new EU Regulation to replace Directive 95/46/EC. New ways of ensuring accountability have attracted the attention of those drafting the new Regulation as well as of influential official commentators on this legislative change. Yet there is some lack of clarity: the proposed Regulation explains that "Article 22 takes account of the debate on a 'principle of accountability' and describes in detail the obligation of responsibility of the controller to comply with this Regulation and to demonstrate this compliance, including by way of adoption of internal policies and mechanisms for ensuring such compliance".[190] But Article 22 itself nowhere mentions accountability, although it does specify that the data controller must "ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation", and "ensure the verification of the effectiveness of the [compliance] measures". A form of external or internal accountability is provided for "[i]f proportionate", whereupon "this verification shall be carried out by independent internal or external auditors".

[187] House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State, Volume I: Report*, 2nd Report of Session 2008-09, HL Paper 18-I, The Stationery Office Limited, London, 2009, p. 19.

[188] House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State, Volume II: Evidence*, 2nd Report of Session 2008-09, HL Paper 18-II, The Stationery Office Limited, London, 2009, Oral evidence of Professor David Feldman, Q 518.

[189] UK Information Commissioner's Office, News Release 5 July 2012, 'ICO shows its teeth, as the public's concern with illegal marketing calls grows', http://www.ico.gov.uk/news/latest_news/2012/ico-shows-its-teeth-as-the-public-concern-over-illegal-marketing-calls-grows-05072012.aspx, accessed 5 July 2012.

[190] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, Brussels, 25.1.2012, p.10 (3.4.4.1).

These provisions follow closely the proposal for a general accountability principle put forward by the 2010 Opinion of the Article 29 Working Party.[191] This proposal mainly describes the actions that data controllers must undertake in order to comply with the law and the principles of data protection, and requires them to "demonstrate on request" to regulatory authorities the compliance measures they have taken and their effectiveness.[192] It is very short on what this "demonstration" should consist of, in terms of the information conveyed externally, but the European Data Protection Supervisor's welcoming comment on the draft Regulation inches closer to this accountability requirement by suggesting that the data controller produce, whether voluntarily or under a legal obligation, a regular report on its activities that would include the measures taken and their effectiveness.[193]

This discourse around the proposed Regulation shows considerable affinity with an industry-led development project aimed at inserting accountability at the centre of self-regulation. The "Accountability Project" has apparently been influential over the thinking and drafting of the Regulation, although it too is particularly weak on the concept of accountability itself as something distinguishable from responsibility and as something that could require more than a requested demonstration of compliance and effectiveness. Much the same can be said for the accountability principle incorporated into the 2009 Madrid Resolution, adopted by the international conference of data protection and privacy commissioners.[194] As with all the documents mentioned here, the language of "demonstration" of accountability is prolifically used, especially in the Accountability Project.[195] There is no explanation of what a demonstration would entail apart from the actions or phenomena to which the demonstration is supposed to testify: the organisation's capacity and willingness to be accountable and to achieve privacy objectives; its possession of an infrastructure for responsibility; its commitment; its adoption of responsible policies; and the like. The demonstration will involve external, independent third parties and regulators, and internal monitoring.

Indeed, as Raab argues,[196] it is the communicative dimension of accountability, related to transparency, that needs to be developed if accountability is to be a more robust requirement in the environment of surveillance and data protection. This requires an understanding of accountability as involving the giving, receiving, and

---

[191] Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, Adopted on 13 July 2010. WP 173. Commentary on this can be found in Guagnin, Daniel, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland and Hector Postigo (eds.), *Managing Privacy through Accountability*, Palgrave Macmillan, London, 2012, Introduction.

[192] Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, Adopted on 13 July 2010. WP 173, paras. 27-28.

[193] European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the data protection reform package*, 7 March 2012, para. 176.

[194] *International Standards on the Protection of Personal Data and Privacy – The Madrid Resolution*, Madrid: International Conference of Data Protection and Privacy Commissioners, 2009.

[195] Hunton & Williams LLP, The Centre for Information Policy Leadership, "Global Discussion on the Commonly-accepted Elements of Privacy Accountability – Galway, Ireland, April 29, 2009"; Hunton & Williams LLP, The Centre for Information Policy Leadership, "Data Protection Accountability: The Essential Elements – a Document for Discussion, October 2009"; Hunton & Williams LLP, The Centre for Information Policy Leadership, "Demonstrating and Measuring Accountability – A Discussion Document, Accountability Phase II – The Paris Project, October 2010".

[196] Raab, Charles D., "The Meaning of 'Accountability' in the Information Privacy Context'" in Guagnin, Daniel, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland and Hector Postigo (eds.), *Managing Privacy through Accountability*, Palgrave Macmillan, London, 2012.

scrutiny of an "account" as a *narrative* about the surveillance, about the compliance or other measures taken to safeguard privacy, and about their effectiveness. Merely to require a user of surveillance to demonstrate, or to be prepared to demonstrate on request, how responsibly they are behaving, says nothing about what that demonstration must consist of, how it is to be communicated, and what its dialogic afterlife might be in any forensic forum through which it could be debated. More work needs to be done to develop the accountability codes and frames within which a company reports its activities, specifying the kinds of information needed by the external reviewers of these accounts.

If an account is a story, what it looks like is critically important, but so too is the way in which it is questioned, challenged, verified or denied by the receiver of the account.[197] To "give an account" – *rendre des comptes* – is to tell a story, and three levels can be distinguished. First, on a weak definition, it means the obligation of an organisation to report back, to "give an account of its actions". Second, on a stronger definition, it means that, plus the implication that the audience can interrogate the account and produce other accounts "on their own account". Third, on the strongest definition, it means the previous two, plus the implication that sanctions can be brought to bear where there is a general agreement that the organisation has "given a bad account of itself", either (a) through its inactions, or (b) through its own unsatisfactory production of an account. The audience, which may be the public, can thus "hold the organisation to account", and that might have real consequences.

Current discourse and practical development of accountability in surveillance limitation and data protection do not explore these avenues, and remain mainly at the first level indicated above. It is hard to identify in current developments the material or conceptual culture of accountability demonstrations, apart from the very worthy materials and concepts regarding the organisation's information-governance action that the demonstration might re-present, or any clear indication that these elements of the communication and dialogue of accountability would need to be developed in successive iterations of the Accountability Project, or in the implementation of the new EU Regulation.

2.3 TRANSPARENCY

2.3.1 Introduction

Among the wide range of democratic values, transparency is not one that is closely associated with surveillance in the public mind.[198] In public policy discourse,

[197] McPherson, Andrew, Charles Raab and David Raffe, "Social Explanation and Political Accountability: Two Related Problems with a Single Solution" paper presented to the Symposium on Accountability at the Annual Conference of the British Educational Research Association, Leeds, September 1978. See the similar analysis in Bovens, Mark, "Analysing and Assessing Accountability: A Conceptual Framework", *European Law Journal*, Vol. 13, No. 4, 2007, pp. 447-468.

[198] For terminological clarity, it is noted that there is a parallel and divergent development in the meaning of the word 'transparency' in recent years: in contemporary literature on political philosophy and constitutional matters, 'transparency' generally designates the democratic value of open government and the free flow of the information related to the public sphere. On the other hand, in the surveillance context 'transparency' is increasingly used in terms of the visibility of the citizen. In this connotation, transparency is basically considered as a harmful phenomenon to be avoided and feared, but it is not without precedent in the literature that citizens' transparency is deemed a good scenario to

transparency is mainly discussed in terms of a key factor in ensuring governmental accountability – discussed earlier – and fighting corruption. Perhaps less frequently emphasised, a commonly agreed approach to transparency is also the description of this value as a necessary vehicle for participation in public debates through exercising certain political fundamental rights such as the ones reflected in the freedoms of expression and the press. However, as a core attribute of democracy, transparency has a much deeper and more comprehensive meaning than these traditional contexts obviously assign to it. Focusing on the essential function that transparency is supposed to fulfil in a liberal democracy allows us to contemplate and explore what implications the commitment to this value might, and even should, have specifically for surveillance societies. This functional approach helps us not only to establish the relevance of transparency to surveillance, but also to get closer to answering the question of who should be transparent, why, and with what costs, in a democratic society that features more and more pervasive surveillance.

2.3.2 The intrinsic function of transparency: scrutinising power

Liberal democracies rest on the principles that individuals are equally free, and that, in the interest of this liberty, the power of the state is strictly limited. Transparency is an indispensable condition for the realisation of these fundamental principles.[199] To stand any realistic chance to make knowledgeable individual choices, and to hold institutional power in check, citizens, as autonomous beings, must be able to possess adequate, accurate, and detailed information about the political, economic, and social forces exerting influence on their fundamental rights. In short, transparency is a guarantee of greater legitimacy of the exercise of power affecting people's autonomy and freedoms. It is a vital tool for counterbalancing the strength of powerful actors by ensuring that power is wielded in a responsible and accountable manner. Departing from the axiom that surveillance produces knowledge, and knowledge produces power – which needs to be plausibly justified and put under public scrutiny – it may be simply stated that where surveillance is performed, there must be some degree of transparency.

2.3.3 The mutual dependence of privacy and transparency

Ever since surveillance issues entered policy and academic discourse, privacy has always been in the focus of attention. The same cannot be said for transparency.

---

achieve. For the latter see the concept of 'transparent society', 'reciprocal transparency' in Brin, David, *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?*, Addison-Wesley, New York, NY, 1998. Since one of the cornerstones of modern democracy has been the dichotomy of the transparent state and the opaque citizen, when writing about transparency *as a democratic value* in this section, we use the traditional meaning of the term.

[199] The majority of political theorists, even though on different grounds, broadly agree with this statement. See Mill, John Stuart, *Considerations on Representative Government* (1861) pp. 30-33), Kant, Immanuel (see Rosen, Allen D., *Kant's Theory of Justice*, Cornell University Press, Ithaca, NY, 1993 pp. 174-186), Rawls, John, *Political Liberalism*, Columbia University Press, New York, NY, 1993, pp. 35; 66-71), and even the minimalist Hayek, Friedrich A., *The Road to Serfdom*, Chicago University Press, Chicago, IL, 1944, pp. 75-76. For a brief contemporary analysis of transparency advocates in political philosophy see Fenster, Mark, "The Opacity of Transparency", *Iowa Law Review*, Vol. 91, 2005-2006, pp. 885-949, at pp. 895-897.

Nevertheless, thinking about transparency from a functional angle encourages us to recognise that the protection of personal liberty depends not only on how people can control access to their personal information, but also how citizens' access to the information on the operation of power can be promoted.[200] The relationship between these two basic components of so-called "informational autonomy", namely between the values of privacy and transparency, is not only complementary but also interdependent. The meaning and the meaningfulness of this mutual dependence are, however, not revealed in the conventional competitive concept of these values, according to which privacy and transparency conflict and cancel each other out. On the contrary, in what follows, it will be argued, although unusually,[201] that privacy and transparency mutually presuppose each other's realisation. Theorising this interdependence might suggest to policy framers and lawmakers that, for the sake of good government protecting autonomy and freedoms, both values must be assured at a high level.

2.3.3.1 *Privacy with and without transparency*

Historical totalitarian regimes that sought to design a totalised form of surveillance clearly illustrate the mutually shaping relationship between privacy and transparency. It was not by accident that totalitarian regimes put serious effort into the systematic suppression of people's authentic knowledge, and carried out surveillance secretly. As Maria Los says in her analysis of the totalitarian potential, "[t]he masses need to acquire a Kafkaesque sense that the true power structure does not lie in the visible maze of offices, but is deeply hidden and profoundly secret." [202] Negating transparency by depriving individuals of information about when, by whom, for what purpose, etc. their behaviour *can be* surveilled was a perfectly satisfactory means of taking away individual privacy, and with it, liberty. The totalitarian arrangement of surveillance taught us that the extent of the invasion of privacy depends strongly on the extent of the confidence of being and acting one's self, discussing matters in private, etc. This connection was drawn in Lawrence Lessig's criticism of the perfection of the totalitarianism of Oceania in Orwell's impressive novel. Lessig argues that the telescreen, the central device for surveillance in Oceania, was inefficient to build perfect totalitarianism because the location and the perspective of the telescreen were transparent, and thus Winston knew where to do things he did not want Big Brother to see.[203] Bentham's Panopticon was also based on the assumption that human autonomy and further aspects of identity are much more vulnerable to surveillance practices being performed in a non-transparent way. The great strength of the arrangement of the Panopticon lies not only in its maximising the visibility of inmates by allowing them no place to hide from the watchers but also, more seriously,

[200] Szekely, Ivan, "Freedom of Information versus Privacy: Friends or Foes?", in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds.), *Reinventing Data Protection?*, Springer, Dordrecht, 2009, pp. 293-316. See also: Schachter, Harvey, *Crossing Boundaries: Privacy, Policy, and Information Technology*, Institute of Public Administration of Canada, 1999, p. 11.

[201] See Szekely, Ivan, "Freedom of Information versus Privacy: Friends or Foes?", in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds.), *Reinventing Data Protection?*, Springer, Dordrecht, 2009, pp. 293-316.

[202] Los, Maria, "Looking into the future: surveillance, globalization and the totalitarian potential", in Lyon, David (ed.), *Theorizing Surveillance. The Panopticon and Beyond*, Willan Publishing, Cullompton, Devon, 2006, p. 72.

[203] Lessig, Lawrence, *Code: And Other Laws of Cyberspace, Version 2.0*. Basic Books, New York, NY, 2006. p. 208.

in the structure which let the guards observe inmates while remaining unseen.[204] As Bentham explains, "[t]he essence of it consists … in the *centrality of* the Inspector's situation, combined with the well-known and most effectual contrivances *for seeing without being seen.*"[205]

The interwoven relationship of privacy and transparency equally applies to rule-of-law regimes, even though undoubtedly under different conditions. It can be maintained that the subjective right to informational self-determination – the very core of the modern concept of informational privacy, as mentioned in Task 1.5 – remains only an illusion without the disclosure of reliable information on the interference of individuals' privacy rights. To have a feasible opportunity to give informed consent to the collection and use of one's personal information, as well as to possess the ability to follow the fate of one's own data, an awareness and understanding of the policies and detailed parameters of the particular data management – including both the beneficial and jeopardising consequences of consent – are of an importance which can hardly be exaggerated.[206] In addition, transparency plays a pivotal role in the enforcement of the legal requirements imposed on data processors. Any normative standard regarding privacy rights – such as the need for an underlying legal basis, necessity, and proportionality – only makes sense if one can recognise and adequately determine when and how his or her right is supposed to have been infringed, and if competent authorities are also capable of following the implementation of norms. The importance of the role of transparency in legal privacy matters is also reflected in the case law developed by the European Court of Human Rights (ECtHR) on state surveillance, which is basically centred upon the requirements of creating transparent frameworks for, and providing public scrutiny of, surveillance practices.[207]

---

[204] Foucault, Michael, "Panopticism", in Kaplan, David M., *Readings in the Philosophy of Technology*, Rowman and Littlefield, Lanham, MD, 2009, p. 265.

[205] Emphasis in original. It is also important to emphasise a more complicated (path-dependent) interplay between surveillance and transparency in former communist countries of Central and Eastern Europe (CEE). In its most powerful manifestation, this interplay served as a basis for the political legitimacy of a reunified Germany after the fall of the Berlin wall in 1989. "Germany's new-found moral legitimacy came to rest on portraying East Germany as an immoral state; the former socialist state became an object that needed to be made fully transparent. The East German secret police (Stasi) and its vast surveillance apparatus became a natural target of transparency, as it inverted the logic of transparency by which the West German state claimed to function. As one form of transparency became key to legitimacy in Germany, its inversion – surveillance – became a marker of illegitimacy." See Sperling, Stefan: "The Politics of Transparency and Surveillance in Post-Reunification Germany". *Surveillance & Society* Vol. 8, No. 4, 2011, pp. 396-412.

[206] This discussion is even more complex in postcommunist societies that simultaneously built rule-of-law regimes and had to come to terms with their own communist past. As a significant part of transitional justice, many CEE countries established 'memory institutes' (ÚPN in Slovakia, IPN in Poland, ÁBTL in Hungary, and ÚSTR in Czech Republic, all established after 2000). Their role was to serve as a means to redress legacies of the former regimes' abuses by allowing individuals access to information that ŠTB, SB or AVO compiled on them and by making files publicly available. At the same time, these countries faced dilemmas of how to satisfy the need for justice, i.e., transparency about the past, and demands by recently introduced data protection laws.

[207] See for instance, *Shimovolos v. Russia* (Application no. 30194/09); *Copland vs. United Kingdom* (Application no. 62617/00); *Amann v. Switzerland* (Application no. 27798/95). For the case law regarding particularly visual surveillance, see Taylor, Nick: "A Conceptual Legal Framework for Privacy. Accountability and Transparency in Visual Surveillance Systems", *Surveillance & Society* Vol. 8, No. 4, 2011, pp. 455-470.

2.3.3.2 *Transparency with and without privacy*

Recognising the interdependence of privacy and transparency suggests that the enforcement of transparency also calls for the implementation of privacy, and not only is the opposite true. The argument for this direction of interdependence rests upon two premises. The first is that transparency does not become a reality, at least in moral sense, by merely enabling free access to an amount of public information. The core value of a transparent society is manifested not in the revealed information itself but in the *knowledge* and in the certain *behavioural liberties* that public data put into citizens' hands. The second premise is that mere access to public information does not *mechanically* produce the knowledge and certain actions that transparency is supposed to promote. The success of transparency mechanisms equally depends upon the cognitive, social, and legal status of the recipient "audience" for the available information.[208] Hence the question is: Can members of the political community be expected to exploit the multiple benefits of free access to public data while being under constant, overt surveillance?

As explored above, the free flow of public information allows people to participate knowledgeably in democratic deliberation and control, to learn from and disseminate of public information, to express their views on, and to make individual choices with regard to what the government and other stakeholders are doing. Transparency, as a bridge between the public and the private, the powerful and the powerless, enables also the sharing of inputs and feedbacks (ideas, concerns, criticisms) among these actors, and thereby can further increase the legitimacy and quality of authorities' actions. As can be seen, the realisation of transparency, if it qualifies as a substantial value, is based upon citizens' ability to deliberate autonomously and upon their capacity and willingness for sovereign action. Privacy, as several advocates maintain – especially those who examine privacy's functions in socio-political and psychological dimensions – is at the core of this capacity, as was seen in Deliverable 1.1. At the socio-political level, the loss of privacy deprives persons of the chance of discussing public matters privately, remaining *incognito* when expressing their opinions, reviewing and criticising the powers opaquely, etc. [209] Even if such a person willingly appeared to participate in public life under such circumstances, his acting would not be an independent voice; he would censor himself. As Edward Bloustein declared, "[s]uch an individual would merge with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man."[210] When such conditions apply, the great political, social, and individual potential lying in public information vanishes, and transparency simultaneously becomes functionally "dead".

[208] See Fenster, Mark, "The Opacity of Transparency", *Iowa Law Review*, Vol. 91, 2005-2006, pp. 895-897, at p. 930; Solove, Daniel J., *The Digital Person*, New York University Press, New York, NY, 2004, pp. 73-74.

[209] Westin, Alan. F., *Privacy and Freedom*, Atheneum, New York, NY, 1967; See also Margulis, Stephen T. "Privacy as a Social Issue and Behavioral Concept", *Journal of Social Issues* Vol. 59, No. 2, 2003, pp. 243-261.

[210] Bloustein, Edward, "Privacy as an aspect of human dignity: an answer to Dean Prosser", *New York University Law Review*, Vol. 39, 1964, pp. 962-1007, at p. 1003. For a very similar argumentation see the dissent of Justice William O. Douglas in *Osborn v. United States*. 385 U.S. 323, 353-54 (1966).

2.4 THE NEED FOR TRANSPARENCY IN TODAY'S SURVEILLANCE SOCIETY

Considering transparency's function and its interlocked relationship with privacy leads to the conclusion that transparency should be seen in the centre when seeking mechanisms to address privacy and other particular concerns imposed by contemporary surveillance practices. Transparency can, to a certain extent, counterbalance the power of stakeholders obtained through surveillance by mitigating the informational asymmetry between the surveiller and the surveilled. By enhancing the ability of people to review and understand the operation of the surveillance systems surrounding them, transparency, from functional perspective, virtually works in the same way as surveillance does, but the other way around: as surveillance provides a method of control over citizens for surveillers, so does transparency for citizens over their surveillers.

2.4.1 Transparency-decreasing factors

A key attribute of contemporary surveillance is that it is everywhere, but is hardly observable. There are at least two factors that profoundly inhibit the realisation of transparency in today's surveillance societies. First, recent technological developments, most notably in the field of ICT, tend to remove surveillance from the face-to-face to the background.[211] Surveillance methods running at a distance may easily sneak into the private sphere in an unobtrusive or even undetected way. In addition, increasingly sophisticated technological solutions enable more and more complex and extensive surveillance, while the processes of data handling are becoming less and less obvious and transparent.[212] Consider the devices and applications of ubiquitous computing, for example: the rapid spread of popularity of well-designed smart phones, PDAs, GPS, etc. has been remarkable, but only a few who use such devices are likely to be aware of their surveillance capacities. The fact is that those who do not put serious effort into acquiring knowledge about the operation and impacts of today's, as well as the emerging, surveillance technologies, but are subject to them, may lose control over the roles they are playing in various contexts based on classification, stereotyping, mistaken identity, etc. Nevertheless, one should not forget that technology can also facilitate transparency when private actors exploit their information advantage over surveillers.

Besides the technological shift, the ability of citizens to oversee surveillance practices is also hindered by the recent shift in power relations.[213] With, and largely due to, the development of new technologies that have fragmented the informational power inherently possessed by the government, the bipolar structure of power has been replaced by a multipolar one. The government is no longer a single actor in control of

[211] Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2007, p. 192. Haggerty, Kevin D. and Ericson, Richard, *The New Politics of Surveillance and Visibility*, University of Toronto Press, Toronto, 2007, p. 13. Schermer, Bart W., "Surveillance and Privacy in the Ubiquitous Network Society", *Amsterdam Law Forum*, Vol. 1, No. 4, 2009, pp. 68-69.

[212] Székely, Iván, Máté Dániel Szabó and Beatrix Vissy, "Regulating the future? Law, ethics, and emerging technologies" *Journal of Information, Communication and Ethics in Society*, Vol. 9, No. 3, 2011, p. 188.

[213] Koops, Bert-Jaap, "Law, Technology, and Shifting Power Relations", *Berkeley Technology and Law Journal*, Vol. 25, 2010, p. 973.

surveillance systems: a wide range of private actors is also involved. In order to maintain democratic control over power, constitutional states must look beyond the governmental-related concept of transparency, and adjust transparency requirements to these new conditions. This is all the more so because transparency is not promoted by the fact that surveillance practices do not exclusively belong to one actor: in other words, because of the practice of "surveillant assemblage".[214] Since these disparate but closely integrated entities using and sharing personal data have created, as Lyon notes, "a complex matrix of power",[215] it has become less possible for citizens to know who is in a position that should be feared. Moreover, from the perspectives of democratic control and accountability, it is also of importance that the decentralisation of the informational power on the stronger side – the state and other stakeholders – has necessarily led to the fragmentation of attentions on the weaker side – citizens – both at the individual and the social level.

The significance of this consideration is to point up that the implementation of transparency is prevented in different ways. The conclusion that can be drawn by policy framers is that as much as the guaranteeing of transparency is hampered by technology and surveillant assemblage (or other factors), so much the more is it necessary to be protected and promoted.

2.4.2 A new voice for enhancing transparency

The meagre but growing literature on the role of transparency vis-à-vis surveillance suggests that the current social reality of surveillance has prompted a new voice calling for transparency in the area of privacy policy. An increasing number of privacy advocates tend to support the view that the dominant privacy paradigm, which focuses predominantly on the limitation of the flow of personal data, cannot be maintained.[216] They argue that the existing data protection frameworks aimed at limiting data processing are not very effective,[217] since the extensive manifestation of today's constant and pervasive surveillance, pushed by technological and social developments in a process of mutual shaping,[218] does not allow citizens to hide from the gaze. Hence, when data mining is inevitable, privacy policy should look for plausible solutions to privacy concerns "outside the data flow box".[219] The majority of those few who have been deliberating on mechanisms for resistance outside this box suppose that certain forms of transparency hold the key to minimising the risk of data mining.

---

[214] Haggerty, Kevin D. and Ericson, Richard, "The Surveillant Assemblage", *British Journal of Sociology*, Vol. 51, No. 4, 2000.

[215] Lyon, David, *Surveillance Studies: An Overvie*w, Polity Press, Cambridge, 2007, p. 95.

[216] This paradigm is outlined in Bennett, Colin J. and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Persective*, The MIT Pre3ss, Cambridge, MA, 2006, chapter 1.

[217] Koops, Bert-Jaap, "Law, Technology, and Shifting Power Relations", *Berkeley Technology and Law Journal*, Vol. 25, 2010, p. 1031.

[218] Lyon, David, *Surveillance Society. Monitoring everyday life*, Open University Press, 2001, pp. 23-27. See also Koops, Bert-Jaap, "Law, Technology, and Shifting Power Relations", *Berkeley Technology and Law Journal*, Vol. 25, 2010, p. 979.

[219] Zarsky, Tal, "Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society", *58 University of Miami Law Review*, Vol. 58, 2003-2004, p. 991.

2.4.3 Transparency-based privacy solutions – with question-marks

Transparency-based privacy solutions offered in the literature rest on the notions of "synoptic surveillance", "sousveillance", "countersurveillance", "watching the watchers". The common feature of these solutions is the attempt to enhance the ability of people to collect data about the operation of their surveillance, and thus mitigate the inequality between the surveiller and the weaker actors. Apart from this, however, these mechanisms differ considerably from each other in character.

The most radical form of this type of surveillance (if it can be regarded as such) is presented by David Brin, who envisages a completely "transparent society" that is based not on hiding personal information but on the concept that anyone can be surveilled by anyone at any time.[220] According to Brin, "reciprocal transparency", as he calls it, is "the best hope to preserve a little privacy in the next century",[221] since it is able to create a proper system of checks and balances for surveillance powers within the whole society.[222] What Brin actually proposes is to stipulate the equality of surveillance powers by letting them "fight" each other through totalising transparency (visibility). The aim of reciprocal transparency, namely to equalise and to hold to account informational power, is highly desirable but not as an ultimate goal that might be achieved at the cost of the complete destruction of individual privacy. However, entitling anybody, indeed everybody, to penetrate one's most intrinsic private sphere, is not to preserve privacy but completely to give it up by legitimising otherwise morally questionable surveillance practices. Consequently and paradoxically, what Brin suggests is destroying privacy for the sake of protecting it, which seems to be confusing and, not least, frightening. In addition, as William Schermer notes, when envisaging the equal distribution of power, Brin seems to take into account neither pre-existing social inequalities (i.e., money, knowledge, etc.) that might profoundly distort relations, nor the fact that totalising surveillance might easily turn into a tyranny of the majority over the few.[223] All in all, Brin's extreme scenario can hardly be an *output* of democratic deliberations on feasible solutions to privacy concerns,[224] but it has provoked fruitful debates over countersurveillance strategies and their constitutional boundaries.[225]

---

[220] Brin, David, *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?*, Addison-Wesley, New York, NY, 1998.

[221] Brin, David, *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?*, Addison-Wesley, New York, NY, 1998, p. 55.

[222] Brin, David, *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?*, Addison-Wesley, New York, NY, 1998, pp. 258-260.

[223] Schermer, Bert William, *Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance*, Leiden University Press, Leiden, 2007, p.

[224] For a counterargument see Koops, Bert-Jaap, "Law, Technology, and Shifting Power Relations", *Berkeley Technology and Law Journal*, Vol. 25, 2010, p. 1034.

[225] See Zarsky, Tal, "Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society", *University of Miami Law Review*, Vol. 58, 2003-2004, pp. 995-1003; Koops, Bert-Jaap, "Law, Technology, and Shifting Power Relations", *Berkeley Technology and Law Journal*, Vol. 25, 2010, pp. 1033-1035., Solove, Daniel J., *The Digital Person*, New York University Press, New York, NY, 2004, pp. 73-74.

Less drastic but also contradictory forms of synoptic surveillance are the various forms of *sousveillance* ("watching from below") developed by Steve Mann.[226] Sousveillance relies on the potential of wearable computing devices used by individuals when encountering organisations. It is not a normatively desired form of privacy[227] but an impressive form of political performance art,[228] aimed at problematising surveillance, and as such it is valuable. However, sousveillance is also a source of concern from many perspectives. It has to be taken into consideration that the surveillant assemblage can use sousveillance for its own purposes,[229] and can take advantage of disadvantage. More importantly, there is no guarantee that wearable computing will never get on the wrong side and will never be used against individuals (neighbours, wives, husbands, lovers, co-workers, etc.).

Naturally, there are more consolidated solutions, too, which do not demand the abandonment of the existing privacy paradigm and the giving up of the search for tools of hiding from the gaze, but see great prospects in transparency mechanisms. Those who represent this view have recognised that both privacy and transparency policies have their own limits but that both values should persist despite difficulties. They also seem to accept that the chance of either one profoundly depends on the fate of the other.

Advocates of consolidated mechanisms demand both legal (institutional) and non-legal (non-institutional) solutions. Regarding legal instruments, Lyon highlights the importance of the enforceability of transparency that may be achieved through implementing a set of policies and Freedom of Information laws, including penalties that may be imposed on those who break the rules.[230] Lyon also emphasises that a much broader coalition of affected actors is needed if transparency is really to occur in a routine way.[231] However, it should be kept in mind that maintaining opacity might be in the interest of stakeholders from many perspectives (business interests, informational property rights holders, etc.). As Gandy points out, "[i]t seems unreasonable to expect that those who use these techniques will be the best sources of public awareness of the consequences of their use." This underpins the responsibility of journalism, the academic sphere, and advocates to communicate tirelessly to individuals the capacities of surveillance practices.[232] The extent to which

[226] Mann, Steve, Jason Nolan and Barry Welllman, "Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments", *Surveillance & Society* Vol. 1, No. 3, 2003, pp. 331-355.
[227] Mann, Steve, Jason Nolan and Barry Welllman, "Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments", *Surveillance & Society* Vol. 1, No. 3, 2003,p. 333.
[228] Cohen, Julie E., "Privacy, Visibility, Transparency, Exposure", *University of Chicago Law Review*, Vol. 75, 2008, p. 199.
[229] Möller, Frank: "Celebration and Concern", in Corinne Martin and Thilo von Pape (eds.), *Images in Mobile Communication: New Content, New Uses, New Perspectives*, VS Verlag für Sozialwissenschaften, 2012. pp. 75-76; Berendt, Bettina, "Data Mining for Information Literacy", in Dawn, E. Holmes and Lakhmi, C. Jain. (eds.), *Data Mining: Foundations and Intelligent Paradigms.* Springer, 2011, p. 291.
[230] Lyon, David, *Surveillance Studies: An Overvie*w, Polity Press, Cambridge, 2007, p. 194.
[231] Lyon, David, *Surveillance Studies: An Overvie*w, Polity Press, Cambridge, 2007, p. 194.
[232] Gandy, Oscar, Jr., "Data mining, Surveillance, and Discrimination in the Post 9-11 Environment", in Haggerty, Kevin D. and Ericson, Richard, *The New Politics of Surveillance and Visibility*, University of Toronto Press, Toronto, 2007, p. 379.

transparency prevails in the future will be crucial. As far as it does, according to Foucault, surveillance should not be feared "to degenerate into tyranny".[233]

2.5 RIGHTS, FREEDOMS, AND THE RULE OF LAW

2.5.1 Rights and freedoms

Fundamental rights are normative moral requirements that democratic states are engaged with and give effect to under any circumstances. Hence, every democratic political regime is responsible to protect its citizens adequately against emerging threats to fundamental rights. In the digital age, democratic states are witnessing a major transformation in power relations that has a profound impact on citizens' rights and freedoms, and thus poses serious challenges to these rights and freedoms. Existing concepts and laws developed for protecting fundamental rights do not always provide ready answers to these developments. In order to be able properly to meet the social needs of the information society and to provide adequate safeguards against new dangers threatening the equality and freedom of individuals, the system of protection of fundamental rights has had to be renewed over and over again. The extension of the catalogue of fundamental rights through legislative or judicial development in order to protect the information autonomy of the person is a progressive manifestation of such renewal.

However, even if law is expected to provide adequate guarantees and tools to solve such problems, one should be aware that the realisation of fundamental rights as normative moral requirements does not necessarily presuppose the use of legal means; nor can legal instruments alone always guarantee the realisation of the moral requirements. In addition, using legal instruments in the area of fundamental rights poses serious risks, since law is always double-faced: even if it serves as a guarantee of freedom, the rule itself is a restriction at the same time. Expanding the range of legal instruments may be useful in situations where these moral requirements cannot otherwise be guaranteed to prevail. The form and extent of such uses of legal instruments, and their effectiveness, depend on the political and constitutional culture and traditions.

From the range of information rights, it is the right to privacy – or its sister right of narrower scope, data protection – which is often the one that most conflicts with surveillance practices. The right to privacy is recognised both in the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the EU; however, the level of protection of this right is not equivalent in the different legal systems existing within the EU. The different levels of protection and the variety of legal instruments applied reflect the cultural diversity and differences in legal traditions in countries of the EU.[234] The ECHR therefore provides only a minimum legal standard to be met by all Members States of the EU, within which national jurisdictions have a relatively wide room for manoeuvre. As a clear attempt to legitimise and standardise the framework of manoeuvring, the so-called doctrine of

[233] Foucault, Michael, "Panopticism", in Kaplan, David M., *Readings in the Philosophy of Technology*, Rowman and Littlefield, Lanham, MD, 2009. p. 268.
[234] Aolain, Fionnuala, "Emergence of Diversity: Differences in Human Rights Jurisprudence", *Fordham International Law Journal*, Vol. 19, 1995-1996, p. 115-117.

"margin of appreciation" has been developed as a response to concerns of national governments that warned that international obligations could threaten the interests of national security. This doctrine has been frequently applied in the jurisdiction of the European Court of Human Rights (ECtHR) in cases involving the violation of the right to private life by state surveillance practices.[235] Some important ECtHR cases are discussed in some depth in a later section. But jurisprudential development is also relevant from another aspect: courts have developed new fundamental rights responding to the needs of information (surveillance) societies, such as the "confidentiality of information systems and the fundamental right to ensure their integrity" (by the German Federal Constitutional Court) or the "right to anonymous speech" (by the US Supreme Court).

2.5.2 The rule of law

We have discussed the rule of law in Deliverable 1.1, but here we give a more general and succinct treatment of its importance. The rule of law is one of the pillars of democratic constitutional states and societies. Having its roots in classical Greek though and springing from ancient Greek philosophers,[236] this principle has a broad meaning and wide-ranging implications in democratic systems. Though Western democracies tend to take the rule of law for granted within their democratic constitutional framework, the meaning and practical enforcement of this principle are changing as a result of the rise of surveillance technologies.

Although an analysis of the origins of the rule of law would be outside the scope of this contribution, it is necessary to define the broad burdens of this principle. The meaning of the rule of law can be sourced to two main theoretical formulations, each coming in three distinct forms.[237] They are alternative and complementary expressions that both contribute to describe the content of the principle. The rule of law has a *formal* and a *substantive* meaning. From a *formal* perspective, the rule of law has the connotations of (I) rule *by* law (law as an instrument of government action); (II) formal legality (legislative process); and (III) democracy (consent determines the content of law) (III). In *substantive* terms, the rule of law consists in (I) individual rights; (II) justice/right to dignity; and (III) social welfare (substantive equality/welfare). Therefore, formal conceptions of the rule of law focus on how law is adopted and on the nature of rules, whereas substantive theories also include requirements about the content and practical enforcement of the law (thus implying justice and moral requirements).

Although the meaning of the rule of law can be referred to unambiguous theoretical categories, the role of the rule of law in democratic legal systems might be misleading. In fact, there are two main paradoxes related to the rule of law within

[235] Yourow, Howard C., *The Margin of Appreciation Doctrine in the Dynamics of European Human Rights Jurisprudence*, Martinus Nijhoff Publisher, Dordrecht,1996, pp. 4-6.
[236] Plato and Aristotle depicted exemplary models of democracy in which the rule of law was considered as the main pillar in the framework of the constitutional state. Klosko, George, *The Development of Plato's Political Theory*, Cambridge University Press, Cambridge, 1986, pp. 225-226. Aristotle, *The Politics of Aristotle*, W.L. Newman (ed.), Arno Press, New York, 1973.
[237] Tamanaha, Brian Z., *On the Rule of Law. History, Politics, Theory*, Cambridge University Press, Cambridge, 2004, p. 91.

democratic systems. First, governments are called to propose and pass legislation which limit the very same state power. Nevertheless, they are bound to comply with those pieces of legislation that impose restrictions on state powers. Second, the state gives its authority to judges who are called to contest the way the state uses its powers. The paradox of the state's limiting its own powers is called the *Rechtsstaat* paradox.[238] These two paradoxes are typical of all democratic systems.[239]

2.5.3 The rule of law, democracy and surveillance

As has been pointed out,[240] like "liberty" or "equality", the principle of the rule of law is a contestable concept on which an overwhelming consensus is lacking. It is the highest expression of the "checks and balances" principle endorsed by the various and different constitutional traditions of democratic states.[241] The rule of law is one of the cornerstones of constitutionalism and democracy. It frames the delicate balance between authoritative powers and civil society in democratic contexts in which citizens entrust governments in exchange for their accountability, which was discussed earlier. As mentioned before, democracy is a fundamental component of the rule of law and this latter, in turn, is one of the fundamental premises of democracy. Thus, a sustainable democracy presumes and maintains the rule of law.[242] Authoritative powers find their way to democracy by recognising human rights and liberties. This recognition implies that democratic governments exercise their legitimate powers through opacity and transparency tools[243] and the safeguarding of citizens' negative and positive liberty.[244]

Conducting surveillance is a legitimate activity conducted by the state to protect itself and its citizens; for example, in crime prevention and in combating anti-democratic terrorist threats. The issue is how to keep such practices in check, ensuring that they

[238] Kaarlo Tuori identifies two paradoxes in the analysis of the role of positive law in modern democratic states, namely the paradox of the *Rechtsstaat* and the paradox of fundamental rights. Tuori, Kaarlo, "Fundamental Rights Principles: Disciplining the Instrumentalism of Policies", in Agustín J. Menéndez and Erik O. Eriksen (eds.), *Arguing Fundamental Rights*, Springer, New York NY, 2006, pp. 33-52, p. 33.

[239] Several authors have provided explanations for the *Rechtsstaat* paradox. In the 18th century Montesquieu solved it through the *trias politica*. In Montesquieu's words, "When the legislative and executive powers are united in the same person, or in the same body of magistrates, there can be no liberty. Again, there is no liberty, if the judiciary power be not separated from the legislative and executive". De Montesquieu, Charles-Louis, *The Spirit of the Laws*, 1748, (translated by Thomas Nugent), Batoche Books, Kitchener, Ontario, Canada, 2001, p. 173.

[240] Fallon, Richard H. Jr., "'The Rule of Law' as a Concept in Constitutional Discourse", *Columbia Law Review*, Vol. 97, No. 1, 1997.

[241] For a detailed analysis of the transposition of the rule of law in the different European and Anglo-Saxon legal traditions, see Rosenfeld, Michel, "The Rule of Law and the Legitimacy of Constitutional Democracy", *Southern California Law Review*, Vol. 74, 1307, 2001, pp. 1037-1352.

[242] Hildebrandt, Mireille, "Profiling and the Rule of Law", *Identity in the Information Society*, Vol. 1, No. 1, 2008, p. 7.

[243] Opacity tools are intended to safeguard the individual's freedom and autonomy with respect to state authorities, whereas transparency tools are aimed to make the state accountable and responsible before its citizens. Gutwirth, Serge and Paul De Hert, "Regulating Profiling in a Democratic Constitutional State" in Mireille Hildebrandt and Serge Gutwirth (eds.) *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Springer, 2008, pp. 271-293.

[244] Berlin, Isaiah, "Two Concepts of Liberty", in Anthony Quinton (ed.), *Political Philosophy*, Oxford University Press, Oxford, 1967, pp. 141-152.

are "proportionate" and "necessary". This points to the central role played by privacy and data protection in the discourse on the rule of law, democracy and surveillance, as two human values and fundamental human rights.[245] De Hert and Gutwirth emphasise the constitutional nature of privacy and data protection, considering privacy as a tool of opacity and data protection as a tool of transparency.[246] In fact, these do not only serve as regulators and controllers of state powers, but do also represent a safeguard against the indiscriminate and pervasive use of surveillance technologies. Privacy and data protection do not simply consist in a set of rules and in legislative provisions, but are instrumental values that contribute to the achievement of fundamental constitutional rights and to the development of a democratic society.[247]

The close and delicate relationship between the rule of law, democracy and surveillance is not a novelty, whether in surveillance studies or in the jurisprudence of the ECtHR. In fact, the ECtHR case law on the use of surveillance technologies is greatly devoted to the search for a balance between surveillance and democracy and finds its main legal basis in Article 8 of the ECHR.[248] In *Klass*,[249] the Court, being aware of the danger secret surveillance poses of "undermining or even destroying democracy on the ground of defending it",[250] underlined the need to establish legal safeguards to the arbitrary use of surveillance in order to ensure democracy. It stated that "any individual measure of surveillance has to comply with the strict conditions and procedures laid down in the legislation",[251] and that "powers of secret

[245] The constitutional nature of the right of data protection is still a matter of discussion. González Fuster, Gloria and Raphaël Gellert, "The Fundamental Right of Data Protection in the European Union: in Search of an Uncharted Right", *International Review of Law, Computers & Technology*, Vol. 26, No. 1, 2012, pp. 73-82.

[246] Gutwirth Serge and Paul De Hert, "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of the Power", in Erik Claes, Anthony Duff and Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Intersentia, Antwerp, 2006, pp. 61-104, and Gutwirth Serge, and Paul De Hert, "Regulating Profiling in a Democratic Constitutional State", in Mireille Hildebrandt and Serge Gutwirth (eds.) *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Springer, 2008, pp. 271-293.

[247] In fact, privacy and data protection are considered as "intermediate" values and notably as tools through which "more fundamental values are pursued"; see Rouvroy, Antoinette and Yves Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy and Democracy", in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds.), *Reinventing Data Protection?*, Springer, Dordrecht, 2009, pp. 45-76, p. 53.

[248] Article 8 of the ECHR provides 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 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.

[249] ECtHR, *Klass and Others v. Germany*, judgement of 6 December 1978, Series A no. 28. In this case the applicants (G. Klass, P. Lubberger, J. Nussbruch, H.J. Pohl and D. Selb) claimed that two German laws passed in 1968 (an amendment to Article 10 §2 of the Basic Law and Act of 13 August) that restricted the right to secrecy of email, post and telecommunications breached the ECHR, notably art. 6, 8 and 13. In this case, the ECtHR found no breach of the Convention had occurred.

[250] ECtHR, *Klass and Others v. Germany*, judgement of 6 December 1978, Series A no. 28, para. 49.

[251] ECtHR, *Klass and Others v. Germany*, judgement of 6 December 1978, Series A no. 28, para. 40.

surveillance of citizens are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions".[252]

The ECtHR has long been considering the rule of law as one of the crucial legal requirements to ascertain the boundaries between surveillance and democracy. Referring to the expression "in accordance with the law" (Article 8.2 ECHR), the ECtHR recognises that any interference by public authorities with the right to respect for private life and correspondence "must have some basis in domestic law",[253] where the word "law" covers both written (or statute) and unwritten law.[254] Secondly, any law which derogates to Article 8 ECHR must be "adequately accessible" (the citizen must be able to have an adequate indication of the legal rules applicable to a given case), sufficiently precise and foreseeable ("its consequences need to be foreseeable with absolute certainty").[255] Nevertheless, in *Malone*,[256] the ECtHR stated that any law that interferes with the right guaranteed by Article 8.1 ECHR "must indicate the scope of any discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard of the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference".[257] The ECtHR recalled this jurisprudence in *Kruslin* and *Huvig*,[258] and more recently in *Khan*[259] by saying that exceptions to Article 8.1 ECHR are legitimate if surveillance measures (such as tapping and interception of telephone conversations) are foreseen by national laws which must be "particularly precise",[260] clear and detailed in order to prevent abuses from national authorities and comply with the rule of law.[261]

[252] ECtHR, *Klass and Others v. Germany*, judgement of 6 December 1978, Series A no. 28, para. 42.
[253] ECtHR, *Silver and Others v. the United Kingdom*, judgement of 25 March 1983, Series A no. 61, para. 86.
[254] ECtHR, *The Sunday Times v. the United Kingdom*, judgement of 26 April 1979, Series A no. 30, para. 47.
[255] ECtHR, *The Sunday Times v. the United Kingdom*, judgement of 26 April 1979, Series A no. 30, para. 49 and ECtHR, *Silver and Others v. the United Kingdom*, judgement of 25 March 1983, Series A no. 61, paras. 87-88.
[256] ECtHR, *Malone v. the United Kingdom*, judgement of 2 August 1984, Series A no. 82. Mr. Malone claimed that his correspondence had been intercepted, his telephone lines tapped and his telephone metered unlawfully by the British Post Office (on behalf of the police) within the general context of a criminal investigation. The ECtHR found that an infringement to art. 8 ECHR had occurred as the law of England and Wales did not indicate "with reasonable clarity the scope and matter of the relevant discretion conferred on the public authorities". ECtHR, *Malone v. the United Kindgdom*, para. 79.
[257] ECtHR, *Malone v. the United Kingdom*, judgement of 2 August 1984, Series A no. 82, para. 68.
[258] ECtHR, *Kruslin v. France*, judgement of 24 April 1990, Series A no. 176-A and *Huvig v. France*, judgement of 24 April 1990, Series A no. 176-B. In both cases the applicants (convicted for murder and tax evasion, respectively) contested the decision of French police authorities that had tapped their telephone conversations. In this case, the Court found that the interception of conversations infringed art. 8 ECHR and the applicants' right to respect for their correspondence and private life given that French legislation on interception of telephone conversations did not '*afford adequate safeguards against various possible abuses'* of national authorities. ECtHR, *Kruslin v. France*, para. 35.
[259] ECtHR, *Khan v. the United Kidgdom*, judgement of 12 May 2000, Series A no. 290.
[260] ECtHR, *Kruslin v. France*, judgement of 24 April 1990, Series A no. 176-A, para. 33.
[261] ECtHR, par. 32-36 of the *Kruslin* judgment and point 1 of its operative provisions and paras. 31-35 of the *Huvig* judgment.

2.6 CONCLUSION

As shown above, there is a significant ECtHR jurisprudence on the rule of law that provides several interpretative guidelines on the content and meaning of this principle, particularly as regards the implementation of surveillance measures. It concerns not only the rule of law in its formal meaning but also its qualitative and content-related facets. The importance given to the rule of law by the ECtHR is deliberate and appropriate, given the widespread use of surveillance technologies in today's societies and the potential threat they pose to individual rights and freedoms, and so to democracy. As the Court recognised in *Malone*, surveillance implies the exercise of a power that, "because of its inherent secrecy, carries with it a danger of abuse of a kind that is potentially easy in individual cases and could have harmful consequences for democratic society as a whole".[262] As the ECtHR highlights, the rule of law represents a legal guarantee against the indiscriminate and pervasive power of national authorities in the exercise of surveillance measures and a bulwark of democracy and the constitutional state.

2.7 THE GOVERNANCE OF SURVEILLANCE

More than any specific law or body of laws, the rule of law and a strong determination to defend and promote rights and freedoms are central to the formation of regimes that are able to keep the forces of surveillance in check. Political scientists have gone beyond a traditional focus on government and legislation as the main subject of the study of state power and decision-making. Government, in the sense of executive, legislative and judicial institutions of the state – although themselves testifying somewhat to a plurality of decision-makers, especially if sub-national levels are considered as well – now tends to be seen as one of a number of sites of power or agents of control, albeit it remains the one that is vested with legal or constitutional authority to act in the name of the state. "Governance" draws attention to a pattern of relations or networks embracing the state and society that may span different jurisdictional levels, through which functions are jointly performed.[263] It denotes that rules and decisions cannot be attributed only to government in each legal jurisdiction or country. These interrelationships exacerbate the problem of accountability in a democratic system, because policy decisions and their implementation through administrative action and the use of resources are not confined to single organisations with hierarchical lines of bureaucratic accountability, as Rhodes has argued.[264]
The governance of surveillance denotes that there are many dispersed agencies and mechanisms that aim to apply legal, ethical and practical constraints upon surveillance to keep it within bounds and therefore consistent with the values of

[262] ECtHR, *Malone v. the United Kingdom*, judgement of 2 August 1984, Series A no. 82, para. 81.
[263] Various approaches to the study of governance are given in Kooiman, Jan (ed.), *Modern Governance: New Government-Society Interactions*, Sage, London, 1993; Kooiman, Jan, *Governing as Governance*, Sage, London, 2003; Rhodes, Rod, *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability*, Open University Press, Buckingham, 1997; and Pierre, Jon (ed.), *Debating Governance: Authority, Steering, and Democracy*, Oxford University Press, Oxford, 2000.
[264] Rhodes, Rod, *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability*, Open University Press, Buckingham, 1997, pp. 21-22, 58-59.

democratic societies founded on the rule of law.[265] In terms of the online environment, this constellation has been colourfully portrayed by Westin in terms of the Wild West of cyberspace: "As in the earliest frontier days in America, the Internet abounds with modern-day cattlemen, sheep-herders, farmers, saloon keepers, whores, and hacker-gunmen, with the influences of the schoolmarm, minister, sheriff, and judge also struggling to be heard and felt".[266] Insofar as the internet is an important site of surveillance, its governance is "multifaceted, complex, and far from transparent".[267] This not only serves as a portrait of the Internet, but of other domains in which surveillance is practiced.

Moreover, surveillance itself is used by myriad organisations in the private and public sectors for a variety of purposes, and may involve the creation of an "assemblage" of mechanisms provided by different Wild West agents. Whether these cohere in ways that pose greater threats to privacy and liberties than they might otherwise do is an empirical question. Haggerty and Ericson believe they do,[268] but this seems contingent on the efforts and capabilities of actors in 'powerful institutions' to harness, "integrate, combine, and coordinate" these separate and partly disconnected surveillance technologies and practices; however, the evidence of achievement is mixed, and surveillance is prone to error and resistance.[269]

There are multiple organisational sources and practices of surveillance. They are often invisible and covert, and their practices subject to the elusive dynamics of "function creep", and – where they form an assemblage – interactive, making it difficult to pin down who is engaging in what surveillance practices and to apply a regulatory array of legal and other controls upon the behaviour of individuals or organisations.[270] Accountability problems exist both in surveillance and in the efforts to govern it. The regulatory landscape itself is fragmented across multiple regulatory instruments,

---

[265] Fuller discussion can be found in Bennett, Colin J. and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge, MA, 2006; Ball, Kirstie, David Murakami Wood, David Lyon, Clive Norris and Charles Raab, *A Report on the Surveillance Society*, Office of the Information Commissioner, Wilmslow, September 2006, Part D.

[266] Privacy and American Business, *Commerce, Communication, and Privacy Online: A National Survey of Computer Users*, conducted for Privacy & American Business by Louis Harris & Associates and Dr. Alan F. Westin, Hackensack, NJ, Privacy & American Business, 1997, p. xvi.

[267] Bygrave, Lee A., "Introduction", in Bygrave, Lee A. and Jon Bing (eds.), *Internet Governance: Infrastructure and Institutions*, Oxford University Press, Oxford, 2009, p. 1. Regulatory complexity is further explored in Murray, Andrew D., *The Regulation of Cyberspace: Control in the Online Environment*, Routledge-Cavendish, Abingdon, 2007.

[268] Haggerty, Kevin D. and Richard V. Ericson, "The surveillant assemblage", *British Journal of Sociology*, Vol. 51, No. 4, December 2000, pp. 605-622, at p. 610: '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 now 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."

[269] Haggerty, Kevin D. and Richard V. Ericson, 'The New Politics of Surveillance and Visibility", in Haggerty, Kevin D. and Richard V. Ericson (eds.), *The New Politics of Surveillance and Visibility*, University of Toronto Press, Toronto, 2006, pp. 3-25.

[270] Lyon, David, Kevin D. Haggerty and Kirstie Ball, "Introducing surveillance studies", in Ball, Kirstie, Kevin D. Haggerty and David Lyon (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, London, 2012, p. 9.

levels, jurisdictions, institutions, and domains. Governance is emphatically not an exercise of top-down authority to govern surveillance, whether within states or globally. In certain fields, such as law enforcement and counter-terrorism, it might be a question whether the forces promoting integrated surveillance are more potent and follow a faster trajectory than those who promote integrated governance or regulation.[271] The latter are further weakened by the necessary reliance for crucial elements of regulation upon those who are themselves engaged in surveillance, whether as private companies or as governmental actors, and who therefore do not advocate strong controls.

Although the impacts of surveillance are felt in ways that go beyond the individual's right to privacy, the governance of surveillance has empirically been largely a matter concerning the safeguarding of privacy and the protection of personal data. As mentioned in the earlier discussion of accountability, most of the existing strategies of surveillance regulation, in terms of data protection, have emphasised legal and technical arrangements for limiting surveillance and for sanctioning excesses in the activities that comprise surveillance; legal instruments were first in the field. These strategies have typically been articulated for *data protection* or the safeguarding of *information* privacy, and have largely left other areas of privacy on one side. Thus only some of Finn *et al.*'s seven types of privacy[272] come directly into the compass of the governance of surveillance as conventionally and narrowly conceived in terms of information privacy, except insofar as privacy invasion involves one or more of the phases of processing of personal data. Within the narrower focus, a sometimes bewildering and patchy array of sectoral and general laws and institutional mechanisms to enforce legal compliance, self-regulatory instruments including codes of practice, and technological tools and design have attracted the most attention from policy-makers and commentators. However, both within these and additionally, mechanisms of accountability and information governance are now receiving greater attention, as we have shown, along with processes of public awareness-raising and individuals' control over their own data.

The governance of surveillance can be seen in terms of policy instruments and policy actors, whether in one or several jurisdictions and at one or more levels from the local to the global. In the world of data protection, instruments and actors form a regime of governance that work towards limiting surveillance and protecting individuals' rights and societal values regarding privacy and a range of associated human values. Bennett and Raab[273] have analysed the repertory of transnational policy instruments arising in several arenas, including the European Union, the Council of Europe, the Organisation for Economic Co-operation and Development, the Asia-Pacific arena, and international standardisation bodies. Law is one of the principle means of

[271] Raab, Charles D., "Joined-up Surveillance: The Challenge to Privacy", in Ball, Kirstie and Frank Webster (eds.), *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*, Pluto Press, London, 2003.

[272] Finn, Rachel, David Wright and Michael Friedewald, "Seven Types of Privacy", 2013 (forthcoming). Their seven types are privacy of the person; of behaviour and action; of communications; of data and image; of thought and feelings; of location and space; and of association.

[273] Bennett, Colin J. and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge, MA, 2006, chapters 4-8. See also Bennett, Colin J., *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Cornell University Press, Ithaca, NY, 1992, especially chapter 5.

governing surveillance,[274] although it perhaps legitimises it more than preventing or remedying its excesses.[275] There has been a proliferation of legal measures at national and sub-national levels, including privacy and data protection laws in at least 76 national jurisdictions[276] and many others in component parts of these states. Other laws operate with regard to specific forms of activity in which surveillance is practiced, such as telecommunications, health, policing, finance, and child protection, and many of these laws are not specific only to the protection of personal data or to the private or public sectors. National and sub-national laws tend to create regulatory agencies, such as the data protection authorities (DPAs) legislated by statute or by international instruments; these authorities, in turn, operate in elaborate international, regional and other networks of regulation to control information processing practices that have implications for privacy.[277] In the EU, the European Data Protection Supervisor and the Article 29 Working Party comprising the DPAs of the 27 Member States have been the most prominent institutions of regulatory governance.

Other instruments are of a more self-regulatory nature, adopted by single organisations or trade bodies as codes of practice, commitments, standards, and seals (in the online environment). Codes of practice may also be mandated by law in certain countries, or else strongly encouraged and shaped by legal instruments and regulatory authorities. The accountability movement, discussed earlier, is the latest effort at self-regulation, generally speaking, with the possibility of being inscribed in the proposed EU Regulation as an international instrument. Then there is a range of technological instruments, aimed at designing or harnessing controls inherent in the technical means of surveillance in order to reduce or eliminate the threats they might pose to privacy and other values.[278] "Privacy-enhancing Technologies" (PETs) and more recently, "Privacy by Design" are the general labels under which these instruments exist, [279] although their practical implementation lags far behind the promise their promoters hold for them. The wide variety of technological tools also includes data encryption, identity assurance systems for anonymity and pseudonymity, and filtering technologies against internet monitoring. Beyond all these instruments, but serving to support them, is the creation of greater public awareness of surveillance and its

[274] Bygrave, Lee A., *Data Protection Law: Approaching its Rationale, Logic and Limits*, Kluwer Law International, New York, 2002.

[275] Flaherty, David H., *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*, University of North Carolina Press, Chapel Hill, NC, 1989, p. 384"

[276] Greenleaf, Graham, "76 Global Data Privacy Laws', *Privacy Laws & Business Special Report*, Privacy Laws & Business, London, September 2011. For USA legislation on computerised databases, wiretapping and polygraph testing, see Regan, Priscilla M., *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, Chapel Hill, NC, 1995.

[277] Flaherty, David H., *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*, University of North Carolina Press, Chapel Hill, NC, 1989; Raab, Charles D., "Networks for Regulation: Privacy Commissioners in a Changing World", *Journal of Comparative Policy Analysis: Research and Practice*, Vol. 13, No. 2**,** 2011, pp. 195-213; Raab, Charles D., "Information Privacy: Networks of Regulation at the Subglobal Level", *Global Policy*, Vol. 1, No. 3, 2010, pp. 291-302.

[278] Lessig, Lawrence, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999; Reidenberg, Joel R., "Lex Informatica: The Formulation of Information Policy Rules Through Technology", *Texas Law Review*, Vol. 76, pp. 552-593.

[279] Burkert. Herbert, "Privacy Enhancing Technologies: Typology, Critique, Vision", in Philip E. Agre and Marc Rotenberg (eds.), *Technology and Privacy: The New Landscape*, The MIT Press, Cambridge, MA, 1997, pp. 125-143; Cavoukian, Ann, *Privacy by Design…Take the Challenge*, Information and Privacy Commissioner of Ontario, Canada, Toronto, 2009.

implications for everyday life. This role is one of many that are performed by regulatory bodies, privacy advocates[280], the media, and legislatures.[281]

At this point, it is important to shift the discussion to the policy actors who wield the various instruments of governance. Even within one jurisdiction, there are many players. Raab and Koops identify a non-exhaustive list that may include constitution-makers, legislatures, DPAs, courts, government departments, private companies, activist organisations, academics, journalists, consumers, citizens, and technology developers.[282] There are many potential and actual connections among them. Empirical studies would highlight these, showing the extent to which they are present in any specific governance activity on any issue. They would also see whether they constitute either a coherent and integrated regime of surveillance governance or a disparate collection of players each wielding a different policy instrument but with no overall strategy or leadership to develop synergies and reduce conflicts within the constellation of governance actors. But the fact that many forms of surveillance involve flows of information and practices that go beyond jurisdictional boundaries means that the cast of characters involved in governance likewise crosses these borders and comprises an even more complex network of regulatory contributors, one that is still in the early stage of formation but with doubtful prospects of rapid further development.

3. CONCLUSIONS ABOUT THE POLITICAL PERSPECTIVE

The political perspective on surveillance given here complements the social and legal perspectives. It also overlaps with them in the sense that, with regard to the social perspective, it sees political and governance processes as embedded within social processes, values, demands and resilience potential, taking their strength and sense of surveillance limits from society, and giving back surveillance policies as well as controls on that surveillance itself. With regard to the legal perspective, the political perspective overlaps in the sense that it understands democracy as embedded in the rule of law and in an appreciation of rights and freedoms that may be at stake in whatever surveillance policies the political system creates, but also in whatever surveillance-limiting measures it undertakes as well. In particular, this Deliverable precedes the discussion of the legal perspective, which has its own emphases and priorities, although those do not necessarily cut across or take issue with either the political or social perspectives.

The chapters of Deliverable 2.2 have tried to capture something of this confluence while at the same time seeing the tensions between competing factors and forces. In a

[280] Bennett, Colin J., *The Privacy Advocates: Resisting the Spread of Surveillance*, The MIT Press, Cambridge, MA, 2008.

[281] For example, House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State, Volume I: Report*, 2nd Report of Session 2008-09, HL Paper 18-I, The Stationery Office Limited, London, 2009.

[282] Raab, Charles and Bert-Jaap Koops, "Privacy Actors, Performances and the Future of Privacy Protection", in Gutwirth, Serge, Yves Poullet, Paul De Hert, Cecile de Terwangne and Sjaak Nouwt (eds.), *Reinventing Data Protection?*, Springer, Dordrecht, 2009, pp. 207-221, at p. 215; see also the chapters in Part II. The list of policy actors draws upon the discussion in Bennett, Colin J. and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge, MA, 2006, chapter 8.

short piece of descriptive and analytical; writing such as this, it has not been possible to explore the political perspective to a fuller extent, whether in terms of different areas of surveillance, geography or jurisdiction, or in terms of comparisons across these dimensions, although broad distinctions have been drawn between established democracies and ones with a recent a history of repressive rule and intensive surveillance. Much less has it been able to find the basis for specific hypotheses to be tested by further systematic research. However, given the patchy nature of the evidence, these chapters have aimed shy of endorsing particular conclusions based on insubstantial empirical findings, much as those conclusions may be plausible and attractive: for example, that the media are (or are not) responsible for inventing fears; that the state of public opinion is (or is not) what certain surveys conclude it to be; or that the law and public policy processes are sufficient (or insufficient) to keep surveillance in bounds.

That said, a few main themes emerge from the political perspective. These are as follows:

1. Surveillance practices of all kinds impinge on a large range of rights, freedoms, liberties, and social and political relationships and processes that affect the nature and texture of life in democratic societies and political systems.

2. Public attitudes, perceptions, fears, expectations and demands are shaped by many forces, among which the mass media are one of the most powerful, tending towards a particular appreciation of surveillance, its technologies, and its role in reducing threats and the level of fear.

3. Social insecurity feeds policy demands for surveillance that tend to limit genuine debate and to ignore the disadvantages and externalities of making life safer and more secure through surveillance; and the resilience of society or, on the other hand, the precautionary anticipation of threats, are in part arbitrated by these demands and by the nature of deliberative processes.

4. The accountability and transparency of surveillance, and the rule of law, are essential in a democratic society, and need to be improved and made potent in order to limit surveillance.

5. The governance of surveillance, and surveillance policy-making, are highly complex and sometimes ephemeral processes that need to be comprehended and rationalised if surveillance is to be regulated in accordance with democratic values.

4. REFERENCES

Acquisti, Alessandro, Stefanos Gritzalis, Costas Lambrinoudakis and Sabrina De Capitani di Vimercati (eds.), *Digital Privacy: Theory, Technologies, and Practices*, Auerbach Publications, Boca Raton, FL, 2007.

Agre, Philip E. and Marc Rotenberg (eds.), *Technology and Privacy: The New Landscape*, The MIT Press, Cambridge, MA, 1997.

Altheide, David, "The News Media, the Problem Frame, and the Production of Fear", *The Sociological Quarterly*, Vol. 38 No. 4, 1997.

Aolain, Fionnuala, "Emergence of Diversity: Differences in Human Rights Jurisprudence", *Fordham International Law Journal*, Vol. 19, 1995-1996.

Aristotle, *The Politics of Aristotle*, W.L. Newman (ed.), Arno Press, New York, 1973.

Armitage, Rachel, *To CCTV or not to CCTV? A Review of Current Research into the Effectiveness of CCTV Systems in Reducing Crime*, NACRO Community Safety Practice Briefing, NACRO, London, 2002.

Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, Adopted on 13 July 2010.

Ball, Kirstie and Frank Webster (eds.), *The Intensification of Surveillance: Crime, Terrorism and Warfare in the Information Age*, Pluto Press, London, 2003.

Ball, Kirstie, Kevin D. Haggerty and David Lyon (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, London, 2012.

Banks, Mark, "Spaces of (in)security: Media and fear of crime in a local context", *Crime Media Culture*, Vol. 1, 2005, pp.169-187.

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

Bennett, Colin J. and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge MA, 2006.

Bennett, Colin J. and Priscilla M. Regan, "Editorial: Surveillance and mobilities", *Surveillance & Society*, Vol. 1, No. 4.

Bennett, Colin J., *The Privacy Advocates: Resisting the Spread of Surveillance*, The MIT Press, Cambridge, MA, 2008.

Bennett, Colin., 'International privacy standards: Can accountability ever be adequate?', *Privacy Laws & Business International Newsletter*, Issue 106, August 2010.

Berendt, Bettina, "Data Mining for Information Literacy", in Dawn, E. Holmes and Lakhmi, C. Jain. (eds.), *Data Mining: Foundations and Intelligent Paradigms.* Springer, 2011.

Berlin, Isaiah, "Two Concepts of Liberty", in Anthony Quinton (ed.), *Political Philosophy*, Oxford University Press, Oxford, 1967.

Bidlo, Oliver, "Ins elektronische Panoptikum der sozialen Kontrolle oder: Das Bild hat immer recht", in Nils Zurawski (ed.), *Überwachungspraxen – Praktiken der Überwachung*, Budrich UniPress, Opladen, 2011.

Black, Edwin, *IBM and the Holocaust*, Little Brown, Boston, MA, 2001.

Bloss, William, "Escalating U.S. Police Surveillance after 9/11: an Examination of Causes and Effects", *Surveillance & Society*, Vol. 4, No. 3, 2007.

Bloustein, Edward, "Privacy as an aspect of human dignity: an answer to Dean Prosser", *New York University Law Review*, Vol. 39, 1964.

Boin, Arjen, Paul 't Hart, Eric Stern and Bengt Sundelius, *The Politics of Crisis Management: Public Leadership under Pressure*. Cambridge University Press, New York, 2005.

Bovens, Mark, "Analysing and Assessing Accountability: A Conceptual Framework", *European Law Journal*, Vol. 13, No. 4, 2007.
Bowden, Caspar, "Closed Circuit Television for Inside Your Head: Blanket Traffic Data Retention and the Emergency Anti-Terrorism Legislation, *Computer and Telecommunications Law Review*, Vol. 8, 2002.
Boyle, Philip, Kevin D. Haggerty, Spectacular Security: Mega Events and the Security Complex, *International Political Sociology*, Vol. 3, No. 3, 2009.
Brin, David, *The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom?*, Addison-Wesley, New York, NY, 1998.
Bygrave, Lee A. and Jon Bing (eds.), *Internet Governance: Infrastructure and Institutions*, Oxford University Press, Oxford, 2009.
Bygrave, Lee A., *Data Protection Law: Approaching its Rationale, Logic and Limits*, Kluwer Law International, New York, 2002.
Cavoukian, Ann, *Privacy by Design…Take the Challenge*, Information and Privacy Commissioner of Ontario, Canada, Toronto, 2009.
Chaddee, Dick and Jason Ditton, "Fear of crime and the media: Assessing the lack of relationship", *Crime Media Culture*, Vol. 1, 2005.
Chan, J., "Dangerous art and suspicious packages", *Law Text Culture*, Vol. 11, No. 1, 2007.
Chibnall, Steve, *Law and Order News*, London, Tavistock, 1977.
Chiricos, Ted, Sarah Eschholz and Marc Gertz, "Crime, News and Fear of Crime: Toward an Identification of Audience Effects", *Social Problems*, Vol. 44, No. 3, 1997.
Clarke, Juanne N., Everest, Michelle M. (2006): "Cancer in the Mass Media: Fear, uncertainty and the medical model", in: *Social Science and Medicine*, Vol. 62, 2006.
Cohen, Julie E., "Privacy, Visibility, Transparency, Exposure", *University of Chicago Law Review*, Vol. 75, 2008.
Cohen, Stanley, *Folk Devils and Moral Panics*, Paladin, London, 1972.
Cook, Fay Lomax, and Wesley G. Skogan, "Convergent and divergent voice models of the rise and fall of policy issues", in Protess, David and Maxwell E. McCombs (eds.) *Agenda Setting: Readings on Media Public Opinion and Policymaking*, Lawrence Erlbaum Associates, New Jersey, 1991.
Council of the EU, *Interim Report on the Evaluation of National Anti-Terrorist Arrangements*, 14306/0/04, Brussels, 23 November, 2004.
De Montesquieu, Charles-Louis, *The Spirit of the Laws*, 1748, (translated by Thomas Nugent), Batoche Books, Kitchener, Ontario, Canada, 2001.
Easton, David, *A Systems Analysis of Political Life*, John Wiley, New York, NY, 1965.
Edelman, Murray J., *Constructing the Political Spectacle*, Chicago University Press, Chicago IL, 1988.
Elin, Nan, *Postmodern Urbanism*, Princeton University Press, New York, 1999.
Ericson, Richard V., and Kevin D. Haggerty, *Policing the Risk Society*, Oxford University Press, Oxford, 1997.
Ericson, Richard V., *Crime in an Insecure World*, Polity Press, Cambridge, 2007.
European Data Protection Supervisor (EDPS), *Opinion of the European Data Protection Supervisor on the data protection reform package*, 7 March 2012.
Fallon, Richard H. Jr., "'The Rule of Law' as a Concept in Constitutional Discourse", *Columbia Law Review*, Vol. 97, No. 1, 1997.
Farrell, Maria, "Communications data retention in the UK", *E-commerce Law and*

Policy, Vol. 3, 2001.
Federrath, Hannes, Marit Hansen and Michael Waidner, "Andreas Pfitzmann 1958-2010: Pioneeer of Technical Privacy Protection in the Information Society", in Fischer-Hübner, Simone, Penny Duquenoy, Marit Hansen, Ronald Leenes and Ge Zhang (eds.), *Privacy and Identity Management for Life*, Springer, 2011.
FEMA, "Crisis Response and Disaster Resilience 2030: Forging Strategic Action in an Age of Uncertainty", January 2012: http://www.fema.gov/library/viewRecord.do?id=4995 (last accessed 31 October 2012).
Fenster, Mark, "The Opacity of Transparency", *Iowa Law Review*, Vol. 91, 2005-2006.
Flaherty, David H., *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States*, University of North Carolina Press, Chapel Hill, NC, 1989.
Flynn, Cathal, "Data Retention, the Separation of Power in the EU and the Right to Privacy: A Critical Analysis of the Legal Validity of the 2006 Directive on the Retention of Data", *University College Dublin Law Review* Vol. 8, No. 1, 2008.
Flynn, Stephen E., "America the Resilient", *Foreign Affairs*, Volume 87, No. 2, 2008.
Foucault, Michael, "Panopticism", in Kaplan, David M., *Readings in the Philosophy of Technology*, Rowman and Littlefield, Lanham, MD, 2009.
Franklin, Bob, *Packaging Politics: Political Communications in Britain's Media Democracy*, Edward Arnold, London, 1994.
Furedi, Frank, "The only thing we have to fear is the culture of fear' itself", 2007, available on: http://www.spiked-online.com/index.php?/site/article/3053/ (last accessed 31 October 2012).
Furedi, Frank, *Culture of Fear. Risk-Taking and the Morality of Low Expectation, Cassell*, London, 2006.
Furedi, Frank, *Politics of Fear*, Continuum Press, New York, 2005.
Galtung, Johan and Mari Holmboe Ruge, "Structuring and selecting the news", in Stanley Cohen and Jock Young (eds.), *The Manufacture of News*, Constable, London, 1973.
Gandy, Oscar, Jr., "Data mining, Surveillance, and Discrimination in the Post 9-11 Environment", in Haggerty, Kevin D. and Ericson, Richard, *The New Politics of Surveillance and Visibility*, University of Toronto Press, Toronto, 2007.
Garton Ash, Timothy, *The File: A Personal History*, HarperCollins, London, 1997.
Gerrard, Graeme, Garry Parkins, Ian Cunningham, Wayne Jones, Samantha Hill and Sarah Douglas, *National CCTV Strategy*, London, Home Office, 2007.
Goldstein, Judith, and Robert O. Keohane, (eds.) *Ideas and Foreign Policy: Beliefs Institutions and Political Change,* Ithaca, Cornell University Press, 1993.
González Fuster, Gloria and Raphaël Gellert, "The Fundamental Right of Data Protection in the European Union: in Search of an Uncharted Right", *International Review of Law, Computers & Technology*, Vol. 26, No. 1, 2012.
Greenleaf, Graham, "76 Global Data Privacy Laws', *Privacy Laws & Business Special Report*, Privacy Laws & Business, London, September 2011.
Grupp, Stefanie, "Political Implications of a Discourse of Fear: The Mass Mediated Discourse of Fear in the Aftermath of 9/11", unpublished paper, Berlin.
Guagnin, Daniel, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland and Hector Postigo (eds.), *Managing Privacy through Accountability*, Palgrave Macmillan, London, 2012, Introduction.

Gutwirth, Serge, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds.), *Reinventing Data Protection?*, Springer, Dordrecht, 2009.
Gutwirth Serge and Paul De Hert, "Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of the Power", in Erik Claes, Anthony Duff and Serge Gutwirth (eds.), *Privacy and the Criminal Law*, Intersentia, Antwerp, 2006.
Gutwirth Serge, and Paul De Hert, "Regulating Profiling in a Democratic Constitutional State", in Mireille Hildebrandt and Serge Gutwirth (eds.) *Profiling the European Citizen. Cross-Disciplinary Perspectives*, Springer, 2008.
Habermas, Jurgen, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, Polity Press, London, 1989.
Haggerty, Kevin D. and Ericson, Richard, "The Surveillant Assemblage", *British Journal of Sociology*, Vol. 51, No. 4, 2000.
Haggerty, Kevin D. and Ericson, Richard, *The New Politics of Surveillance and Visibility*, University of Toronto Press, Toronto, 2007.
Haggerty, Kevin D. and Minas Samatas, "Surveillance and democracy: an unsettled relationship", in Haggerty, Kevin D. and Minas Samatas (eds.), *Surveillance and democracy*, Routledge, London, 2010.
Haggerty, Kevin D. and Richard V. Ericson (eds.), *The New Politics of Surveillance and Visibility*, University of Toronto Press, Toronto, 2006.
Hall, Steve, *Theorizing Crime and Deviance: A New Perspective*. Sage, London, 2012.
Hall, Stuart, "The Determination of News Photographs" [1973], in Chris Greer (ed.), *Crime and Media: A Reader*, Routledge, London, 2010.
Ham, Christopher, and Michael Hill, *The Policy Process in the Modern Capitalist State*, Brighton, Harvester Wheatsheaf, Brighton, 1993.
Hankiss, Elemér,: *Fears And Symbols; An Introduction to the Study of Western Civilisation*, Central European Press, Budapest, 2001.
Hayek, Friedrich A., *The Road to Serfdom*, Chicago University Press, Chicago, IL, 1944.
Henschel, Richard R. *Thinking About Social Problems*, Harcourt Brace Jovanovich, New York, 1990.
Hildebrandt, Mireille, "Profiling and the Rule of Law", *Identity in the Information Society*, Vol. 1, No. 1, 2008.
Hochschild, Arlie R, "Emotion Work, Feeling Rules, and Social Structure", *American Journal of Sociology*, Vol. 85, No. 3, 1979.
Hogwood, Brian W., and Lewis A. Gunn, *Policy Analysis for the Real World*, Oxford University Press, Oxford, 1984.
Hogwood, Brian W., *From Crisis to Complacency: Shaping Public Policy in Britain*, Oxford University Press, Oxford, 1987.
Hogwood, Brian W., *Trends in British Public Policy*, Open University Press, Buckingham, 1992.
House of Lords Select Committee on the Constitution, *Surveillance: Citizens and the State*, *Volume I: Report*, 2nd Report of Session 2008-09, HL Paper 18-I, The Stationery Office Limited, London, 2009.
Huey, Laura and Richard S. Rosenberg, "Watching the Web: Thoughts on Expanding Police Surveillance Opportunities under the Cyber-Crime Convention" *Canadian Journal of Criminology and Criminal Justice*, Vol. 46, No. 5, 2004.

Jenkins, W. I., *Policy Analysis: A Political and Organisational Perspective,* Martin Robertson, London, 1978.
Jewkes, Yvonne, "The Construction of Crime News" [2004], in Chris. Greer (ed.), *Crime and Media: A Reader*, Routledge, London, 2010.
Jewkes, Yvonne, *Media and Crime*, Sage, Thousand Oaks, CA, 2004.
John, Peter, *Analysing Public Policy*, Pinter, London, 1998.
Kammerer, Dietmar, "Surveillance in literature, film and television", in Ball, Kirstie, Kevin D. Haggerty and David Lyon, (eds.), *Routledge Handbook of Surveillance Studies*, London, 2012.
Katz, Jack, "What makes crime 'news'?", *Media, Culture and Society*, Vol. 9, 1987.
Kepner, Charles H. and Benjamin B. Tregoe, *The Rational Manager: A Systematic Approach to Problem Solving and Decision-Making*, McGraw-Hill, New York NY,1965.
Kimmelman, Michael, "That Mushroom Cloud? They're Just Svejking Around", *The New York Times*, January 24, 2008.
Kingdon, John, *Agendas, Alternatives and Public Policies,* Little Brown, Boston MA, 1984.
Klosko, George, *The Development of Plato's Political Theory*, Cambridge University Press, Cambridge, 1986.
Konstandinides, Theodore, "Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem", *European Law Review* Vol. 35, No. 5, 2011.
Kooiman, Jan (ed.), *Modern Governance: New Government-Society Interactions*, Sage, London, 1993.
Kooiman, Jan, *Governing as Governance*, Sage, London, 2003.
Koops, Bert-Jaap "Forgetting Footprints, Shunning Shadows, a Critical Analysis of the 'Right to be Forgotten' in Big Data Practice'', *Script*ed, Vol. 8., No. 3, December 2011.
Koops, Bert-Jaap, "Law, Technology, and Shifting Power Relations", *Berkeley Technology and Law Journal*, Vol. 25, 2010.
Kraft, Michael E. and Scott R. Furlong. *Public Policy. Politics, Analysis, and Alternatives*, Sage/CQ Press, London, 2012 (4th edition).
Lasswell, Harold D., *The Decision Process: Seven Categories of Functional Analysis*, University of Maryland Press, College Park MD, 1956.
Lasswell, Harold D., *The Future of Political Science,* Atherton, New York, NY, 1963.
Lessig, Lawrence, *Code: And Other Laws of Cyberspace, Version 2.0.* Basic Books, New York, NY, 2006.
Lindblom, Charles E. and Edward J. Woodhouse, *The Policy-Making Process*. Prentice Hall, Englewood, NJ, 1993 (3rd edition).
Logan, Debra, 'What is Information Governance? And Why is it So Hard?', Gartner Blog, January 11, 2010: http://blogs.gartner.com/debra_logan/2010/01/11/what-is-information-governance-and-why-is-it-so-hard/, last accessed 07 July 2012).
Los, Maria, "A trans-systemic surveillance: The legacy of communist surveillance in the digital age", in Haggerty, Kevin D. and Minas Samatas (eds.), *Surveillance and Democracy*, Routledge, London, 2010.
Los, Maria, "Looking into the future: surveillance, globalization and the totalitarian potential", in Lyon, David (ed.), *Theorizing surveillance: the panopticon and beyond*, Willan Publishing, Cullompton, 2006.

Los, Maria, "Post-communist fear of crime and the commercialization of security", *Theoretical Criminology*, Vol. 6, No. 2, 2002.
Lyon, David, "Airports as data filters: Converging data systems after September 11th", *Journal of Information, Communication and Ethics in Society*, Vol. 1, No. 1, 2003.
Lyon, David, *Identifying Citizens: ID Cards as Surveillance*, Polity Press, Cambridge, 2009.
Lyon, David, *Surveillance Society. Monitoring everyday life,* Open University Press, 2001.
Lyon, David, *Surveillance Studies, An Overview*, Polity Press, Cambridge, 2007.
Mack, Ruth P., *Planning on Uncertainty*, John Wiley, New York NY, 1971.
Mann, Steve, Jason Nolan and Barry Welllman, "Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments", *Surveillance & Society* Vol. 1, No. 3, 2003.
Manyena, S. Bernard, "The concept of resilience revisited", *Disasters*, Vol. 30, 2006.
Maras, Maria-Helen, "The economic costs and consequences of mass communications data retention: is the Data Retention Directive a proportionate measure?" *European Journal of Law and Economics*, Vol. 33, No. 2, 2012.
Margulis, Stephen T. "Privacy as a Social Issue and Behavioral Concept", *Journal of Social Issues* Vol. 59, No. 2, 2003.
Marinetto, Mike, *Studies of the Policy Process: A Case Analysis*, Prentice Hall, Hemel Hempstead, 1999.
Marsh, David and Roderick Rhodes, (eds.), *Implementing Thatcherite Policies*, Open University Press, Buckingham, 1992.
Marsh, David and Roderick Rhodes, (eds.), *Policy Networks in British Government*, Clarendon, Oxford, 1992.
Marsh, Ian and Gaynor Melville, "Moral Panics and the British Media – A Look at Some Contemporary 'Folk Devils'", *Internet Journal of Criminology*, 2011 (online).Available: http://www.internetjournalofcriminology.com/Marsh_Melville_Moral_Panics_and_the_British_Media_March_2011.pdf (last accessed 23 October 2012).
May, Rollo, *The Meaning of Anxiety*, The Ronald Press Company, New York, NY, 1950.
Mayer-Schönberger, Viktor, *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press, Princeton NJ, 2009.
McPherson, Andrew, Charles Raab and David Raffe, "Social Explanation and Political Accountability: Two Related Problems with a Single Solution" paper presented to the Symposium on Accountability, Annual Conference of the British Educational Research Association, Leeds, September 1978.
McRobbie, Angela, and Sarah L. Thornton, "Rethinking 'Moral Panic' for Multi-Mediated Social Worlds", *British Journal of Sociology*, Vol. 46, No. 4, 1995.
Mill, John Stuart, *Considerations on Representative Government*, 1861.
Mitrou, Lilian, "The impact of communications data retention on fundamental rights and democracy – the case of EU Data Retention Directive", in Haggerty, Kevin D. and Minas Samatas (eds.), *Surveillance and Democracy* Routledge, Abingdon, 2010.
Möller, Frank: "Celebration and Concern", in Corinne Martin and Thilo von Pape (eds.), *Images in Mobile Communication: New Content, New Uses, New Perspectives,* VS Verlag für Sozialwissenschaften, 2012.
Monahan, Torin, *Surveillance in the Time of Insecurity*. Rutgers University Press,

New Brunswick, 2010.
Mulgan, Richard, '"Accountability": An Ever-Expanding Concept?', *Public Administration*, Vol. 78, No. 3, 2000.
Munir, Abu Bakar and Siti Hajar Mohd Yasin, "Retention of communications data: a bumpy road ahead", *The John Marshall Journal of Computer and Information Law*, Vol. 22, No. 4, 2004, pp. 757-758.
Murakami Wood, David, "Securing the Neurocity", *Criminal Justice Matters*, Vol. 68, No. 1, 2007.
Murakami Wood, David, and C. William R. Webster, "Living in Surveillance Societies: The normalisation of surveillance in Europe and the threat of Britain's bad example", *Journal of Contemporary European Research*, Vol. 5, No.2, 2009.
Murray, Andrew D., *The Regulation of Cyberspace: Control in the Online Environment*, Routledge-Cavendish, Abingdon, 2007.
Nellis, Mike, "Tracking offenders by satellite – progress or cost-cutting?", *Criminal Justice Matters*, Vol. 68, No. 1, 2007.
Newland, Erica and Cynthia Wong, "Data Retention Mandates: A Threat to Privacy, Free Expression, and Business Development", Center for Democracy & Technology, Washington, DC, Oct. 2011: <http://cdt.org/files/pdfs/CDT_Data_Retention_Paper.pdf>.
Norris, Clive, Michael McCahill and David Murakami Wood, "The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space", *Surveillance & Society*, Vol. 2, Nos. 2-3, 2004.
Norris, Fran H., Susan P. Stevens, Betty Pfefferbaum, Karen F. Wyche, and Rose L. Pfefferbaum, "Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness", *American Journal of Community Psychology*, Vol. 41, 2008.
O'Shaughnessy, Nicholas J., *The Phenomenon of Political Marketing*, Macmillan, London, 1990.
Organisation for Economic Co-operation and Development (OECD), *Emerging Systemic Risks in the 21st Century: An Agenda for Action*, 2003, http://www.oecd.org/sti/futures/globalprospects/37944611.pdf (last accessed 31 October 2012).
Organisation for Economic Co-operation and Development (OECD), *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, Paris: OECD, 1981.
Parsons, Wayne, *Public Policy: An Introduction to the Theory and Practice of Policy Analysis*, Edward Elgar, Aldershot, 1995.
Pierre, Jon (ed.), *Debating Governance: Authority, Steering, and Democracy*, Oxford University Press, Oxford, 2000.
Raab, Charles and Benjamin Goold, *Protecting Information Privacy*, Research Report 69, Equality and Human Rights Commission, London, 2011.
Raab, Charles and Bert-Jaap Koops, "Privacy Actors, Performances and the Future of Privacy Protection", in Gutwirth, Serge, Yves Poullet, Paul De Hert, Cecile de Terwangne and Sjaak Nouwt (eds.), *Reinventing Data Protection?*, Springer, Dordrecht, 2009.
Raab, Charles D., "Information Privacy: Networks of Regulation at the Subglobal Level", *Global Policy*, Vol. 1, No. 3, 2010.
Raab, Charles D., "Networks for Regulation: Privacy Commissioners in a Changing World", *Journal of Comparative Policy Analysis: Research and Practice*, Vol. 13, No. 2, 2011.

Raab, Charles D., "The Meaning of 'Accountability' in the Information Privacy Context'" in Guagnin, Daniel, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland and Hector Postigo (eds.), *Managing Privacy through Accountability*, Palgrave Macmillan, London, 2012.

Rauhofer, Judith, "Just because you're paranoid, doesn't mean they're not after you: legislative developments in relation to the mandatory retention of communications data in the European Union" *SCRIPTed*, Vol. 3, No. 4, 2006.

Rawls, John, *Political Liberalism*, Columbia University Press, New York, NY, 1993.

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

Rhodes, Roderick A. W., *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability*, Open University Press, Buckingham, 1997.

Rhodes, Roderick A. W., *Beyond Westminster and Whitehall*, Unwin Hyman, London, 1988.

Rhodes, Roderick A. W., *The National World of Local Government*, Allen and Unwin, London, 1986.

Rhodes, Roderick, A. W., "Power dependence, policy communities and intergovernmental networks", *Public Administration Bulletin*, 49, 1985.

Richardson, Jeremy J., and A. Grant Jordan, *Governing Under Pressure*, Martin Robertson, Oxford, 1979.

Roberts, Alasdair S.,"Building Resilience: Macrodynamic Constraints on Governmental Response to Crises", *Suffolk University Law School Research Paper* 09-23, March 16, 2009.

Roberts, Hal and John Palfrey, "The EU Data Retention Directive in an Era of Internet Surveillance", in Deibert, Ronald J., John Palfrey, Rahal Rohozinski and Jonathan Zittrain (eds), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, MIT Press, Cambridge, MA: 2010.

Rose, Richard, "Comparing public policy: an overview", *European Journal of Political Research*, Vol. 1, No. 1, 1973.

Rouvroy, Antoinette, "Réinventer l'art d'oublier et de se faire oublier dans la société de l'information?", available at: http://works.bepress.com/cgi/viewcontent.cgi?article=1004&context=antoinette_rouvroy, (last accessed 19 December 2012).

Sabatier, Paul A., and Hank C. Jenkins-Smith, (eds.), *Policy Change and Learning*, Westview, Boulder CO, 1993.

Samatas, Minas, Chiara Fonio, Catarina Frois and Gemma Galdon Clavell, "Authoritarian Surveillance and its Legacy in South-European Societies: Greece, Italy, Spain, Portugal", in Webster, William C., Doina Balahur, Nils Zurawski, Kees Boersma, Bence Ságvári and Christel Backman (eds.), *Living in Surveillance Societies: The Ghosts of Surveillance. Proceedings of LiSS Conference 2*, Editura Universităţii, Alexandru Ioan Cuza", Iasi, 2011.

Schachter, Harvey, *Crossing Boundaries: Privacy, Policy, and Information Technology*, Institute of Public Administration of Canada, 1999.

Schermer, Bart W., "Surveillance and Privacy in the Ubiquitous Network Society", *Amsterdam Law Forum*, Vol. 1, No. 4, 2009.

Schermer, Bert William, *Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance*, Leiden University Press, Leiden, 2007.

Schneier, Bruce. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. Copernicus Books, New York, 2003.

Szekely, Ivan, "Freedom of Information versus Privacy: Friends or Foes?", in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds.), *Reinventing Data Protection?*, Springer, Dordrecht, 2009.

Sims, Benjamin., "Resilience and Homeland Security: Patriotism, Anxiety, and Complex System Dynamics", http://limn.it/resilience-and-homeland-security-patriotism-anxiety-and-complex-system-dynamics/ (last accessed 31 October 2012).

Smith, Martin, *Pressure, Power and Policy*, Harvester Wheatsheaf, Hemel Hempstead, 1993.

Solove, Daniel J., *The Digital Person*, New York University Press, New York, NY, 2004.

Solove, Daniel. J, "Reconstructing the electronic surveillance law", *George Washington Law Review*, Vol. 72, 2003-2004.

Spalek, Basia and Bob Lambert, "Muslim communities under surveillance", *Criminal Justice Matters*, Vol. 68, No. 1, 2007.

Speckhard, Anne, "Modeling Psycho-Social Resilience to Terrorism", in NATO, *Psychosocial, Organizational and Cultural Aspects of Terrorism*, Final Report of the NATO Human Factors and Medicine Research Task Group 140, November 2011, http://www.cso.nato.int/pubs/rdp.asp?RDP=RTO-TR-HFM-140 (last accessed 31 October 2012).

Sperling, Stefan: "The Politics of Transparency and Surveillance in Post-Reunification Germany", *Surveillance & Society* Vol. 8, No. 4, 2011.

Sunstein, Cass R., *The Laws of Fear: Beyond the Precautionary Principle*, Cambridge University Press, Cambridge, 2005.

Svenonius, Ola, "The Stockholm Security Project: Plural policing, security and surveillance", *Information Polity*, Vol. 17, No.1, 2012.

Svenonius, Ola. *Sensitising Urban Transport Security: Surveillance and Policing in Berlin, Stockholm, and Warsaw*, PhD thesis, Södertörn University, Stockholm, 2011.

Székely, Iván, "Changing attitudes in a changing society? Information privacy in Hungary 1989–2006", in Elia Zureik, L. Lynda Harling Stalker, Emily Smith, David Lyon, and Yolande E. Chan (eds.), *Privacy, Surveillance and the Globalization of Personal Information: International Comparisons*, McGill-Queen's University Press, Montreal & Kingston, 2010.

Székely, Iván, "Freedom of Information versus Privacy: Friends or Foes?", in Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile de Terwangne and Sjaak Nouwt (eds.), *Reinventing Data Protection?*, Springer, Dordrecht, 2009.

Székely, Iván, "Hungary", in James B. Rule and Graham Greenleaf (eds.), *Global Privacy Protection: The First Generation*, Edward Elgar Publishing Ltd., 2008.

Székely, Iván, Máté Dániel Szabó and Beatrix Vissy, "Regulating the future? Law, ethics, and emerging technologies" *Journal of Information, Communication and Ethics in Society*, Vol. 9, No. 3, 2011.

Tamanaha, Brian Z., *On the Rule of Law. History, Politics, Theory*, Cambridge University Press, Cambridge, 2004.

Taylor, Emmeline, "I spy with my little eye: the use of CCTV in schools and the impact on privacy", T*he Sociological Review*, Vol. 58, No. 3, 2010.

Thomas, Richard and Mark Walport, *Data Sharing Review Report*, 11 July 2008: http://www.connectingforhealth.nhs.uk/systemsandservices/infogov/links/datasharingreview.pdf.

Triantaphyllou, Evangelos, *Multi-criteria decision making methods: a comparative study*, Kluwer Academic Publishers (now Springer), Dordrecht, 2000.

Tuori, Kaarlo, "Fundamental Rights Principles: Disciplining the Instrumentalism of Policies", in Agustín J. Menéndez and Erik O. Eriksen (eds.), *Arguing Fundamental Rights*, Springer, New York NY, 2006.

UK Cabinet Office, *Data Handling Procedures in Government: Final Report, June 2008*.

Vasu, Norman, "Grace in Times of Friction: The Complexity of Social Resilience", *RSIS Commentaries*, No. 72, 2007, pp. 1-3, at p.1, http://www.rsis.edu.sg/publications/Perspective/RSIS0722007.pdf (last accessed 31 October 2012).

Verdery, Katherine, "Anthropological adventures with Romania's Wizard of Oz, 1973-1989", *Focaal*, Vol. 43, 2004.

Verleye, Gino, Pieter Maeseele, Isabelle Stevens and Anne Speckhard, "Resilience in an Age of Terrorism: Psychology, Media and Communication", in M. Brooke Rogers, Christopher A. Lewis, Kate M. Loewenthal, R. Amlot and Marco Cinnirella, (eds.) *Aspects of Terrorism and Martyrdom: Dying for God, Dying for Good*. The Edwin Mellin Press, Lampeter, 2009.

Vickers, Geoffrey, *The Art of Judgement: A Study of Policymaking*, Chapman Hall, London, 1965.

Webster, C. William R., "CCTV policy in the UK: reconsidering the evidence base", *Surveillance & Society* , Vol. 6, No. 1, 2009.

Webster, C. William R., "Closed circuit television and governance: the eve of a surveillance age", *Information Infrastructure and Policy*, Vol. 5, No. 4, 1996.

Webster, C. William R., "Public Administration as Surveillance", in Ball, Kirstie, Kevin D. Haggerty and David Lyon, (eds.), *Routledge Handbook of Surveillance Studies*, London, 2012.

Webster, C. William R., "The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK", *Surveillance & Society*, CCTV Special (eds. Norris, McCahill and Wood), Vol. 2, Nos. 2-3, 2004.

Webster, C. William R., Eric Töpfer, Francisco R. Klauser and Charles D. Raab (eds.), *Video Surveillance Practices and Policies in Europe*, IOS Press, Amsterdam, 2012.

Westin, Alan. F., *Privacy and Freedom*, Atheneum, New York, NY, 1967.

Wright, David, Michael Friedewald, Serge Gutwirth, Marc Langheinrich, Emilio Mordini, Rocco Bellanova, Paul De Hert, Kush Wadhwa and Didier Bigo, "Sorting out smart surveillance", *Computer Law and Security Review*, Vol. 26, No. 4, July 2010.

Young, Jock, "The Myth of the Drug Taker in the Mass Media", in Stanley Cohen and Jock Young (eds.), *The Manufacture of News*, Constable, London, 1973.

Young, Jock, *The Inclusive Society*, Sage, London, 1999.

Yourow, Howard C., *The Margin of Appreciation Doctrine in the Dynamics of European Human Rights Jurisprudence*, Martinus Nijhoff Publisher, Dordrecht,1996.

Zarsky, Tal, "Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society", *University of Miami Law Review*, Vol. 58, 2003-2004.

List of cases – European Court of Human Rights (ECtHR)

ECtHR, *Klass and Others v. Germany*, judgement of 6 December 1978, Series A no. 28.
ECtHR, *Silver and Others v. the United Kingdom*, judgement of 25 March 1983, Series A no. 61.
ECtHR, *The Sunday Times v. the United Kingdom*, judgement of 26 April 1979, Series A no. 30.
ECtHR, *Malone v. the United Kingdom*, judgement of 2 August 1984, Series A no. 82.
ECtHR, *Kruslin v. France*, judgement of 24 April 1990, Series A no. 176-A.
ECtHR, *Huvig v. France*, judgement of 24 April 1990, Series A no. 176-B.
ECtHR, *Khan v. the United Kidgdom*, judgement of 12 May 2000, Series A no. 290.