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 D1.1: Surveillance, fighting crime and violence

A report addressing and analysing the factors underpinning the development and use of surveillance systems and technologies by both public authorities and private actors, and their implications in fighting crime and terrorism, social and economic costs, protection or infringement of civil liberties, fundamental rights and ethical aspects

Co-ordinator	Trilateral Research and Consulting LLP
Dissemination level:	PU
Deliverable type:	Report
Version:	1
Submission date:	17 December 2012

	Lead	Contributors
Executive summary and overall editor	David Wright, Trilateral Research and Consulting	Johann Čas, Oesterreichische Akademie der Wissenschaften (Institute of Technology Assessment)
Concepts and terms	Ivan Szekely, Eotvos Karoly Policy Institute	Beatrix Vissy, EKINT
The co-evolution of surveillance technologies and surveillance practices	Michael Friedewald, Fraunhofer Institute for Systems and Innovation Research ISI	Kerstin Goos, Dara Hallinan, Fraunhofer ISI, William Webster, Charles Leleux, University of Stirling
The surveillance industry in Europe	Rowena Rodrigues, Trilateral Research and Consulting LLP	Michael Friedewald, Fraunhofer, and Gemma Galdon Clavell, University of Barcelona
The effectiveness of surveillance in preventing and detecting crime and terrorism	Reinhard Kreissl, Institute for the Sociology of Law and Criminology (IRKS)	Clive Norris, Marija Krlic and Leroy Groves Sheffield University, Anthony Amicelle, PRIO
Social and economic costs of surveillance	Johan Čas, Oesterreichische Akademie der Wissenschaften (Institute of Technology Assessment)	Stefan Strauß, Oesterreichische Akademie der Wissenschaften (Institute of Technology Assessment), Anthony Amicelle, PRIO, Kirstie Ball, Open University, Dara Hallinan, Michael Friedewald, Fraunhofer ISI, Ivan Szekely, Beatrix Vissy, EKINT
Impacts of surveillance on civil liberties and fundamental rights	Charles Raab, University of Edinburgh	Dara Hallinan, Fraunhofer ISI, Anthony Amicelle, PRIO; Gemma Galdon Clavell, UB; Paul De Hert, VUB; Antonella Galetta, VUB, Richard Jones, University of Edinburgh
Findings and recommendations	David Wright, Trilateral Research and Consulting	

Contents

EXECUTIVE SUMMARY

This is an executive summary of a report addressing and analysing the factors underpinning the development and use of surveillance systems and technologies by both public authorities and private actors, and their implications in fighting crime and terrorism, social and economic costs, protection or infringement of civil liberties, fundamental rights and ethical aspects. The executive summary comprises five main parts corresponding to the outputs of the five main tasks in WP1.

THE CO-EVOLUTION OF SURVEILLANCE TECHNOLOGIES AND SURVEILLANCE PRACTICES

The aim of Task 1.1 was to explore the dynamics of the proliferation of surveillance practices by considering driving factors such as actors, policy initiatives and reactions, societal, economic and technological developments. Task 1.1 also focuses on the historical development of surveillance technologies (beginning in the middle of the 20th century). It specifically examines how technological development has changed surveillance practices and how changed practices have spawned novel surveillance technologies in a co-evolutional manner.

The investigation starts with the review of the development and establishment of databases and the ensuing rise of the computer – which bred quantitative and qualitative shifts in surveillance practices. Beginning with punch cards, continuing with affordable disk storage and finally progressing to ever smaller computers offering huge data storage capacity, governments and corporations have identified, step by step, increased surveillance opportunities. As IT capabilities increased and their development accelerated, the possibilities to store and process data in turn triggered the ubiquity, decentralisation, anonymity and self-reinforcement of surveillance. Motives for the eventual usage of those technologies can be found in the rise of the welfare state which required the collection of data about citizens in order to offer social services. Further internal and external threats to national security caused the application of dragnet investigations (e.g., of left-wing terrorism in Germany in the 1970s), the installation of governmental databases for criminal records, policing and intelligence gathering, and the development of new surveillance technologies such as satellites or wireless bugging. An especially dominant surveillance application that broke through in the 1990s is closed circuit television (CCTV). The UK set the pace in CCTV deployment – showing the highest number of public space CCTV systems – although other European countries have also experienced a sustained growth in CCTV.

An important technological turning point was the convergence of telecommunications and information technologies and the increasing digitization since the mid-1980s. This made it possible to integrate all kinds of input devices (and the data they collect) into complex information processing systems. Increasingly powerful algorithms for data analysis facilitated the recognition of persons, incidents and the processing of much more information of possible interest for surveilling authorities. These developments began to allow (semi-) automated decision-making.

In addition to the interest of the state in the control and collection of data, corporations and employers entered the field as players in various surveillance contexts. The proliferation of credit cards and loyalty cards, and new possibilities to store and analyse the consumption activities of individuals, led to the rise of direct and targeted marketing activities and early

forms of large-scale social sorting. Computerisation also created new opportunities for the electronic surveillance of the individual worker and the workplace.

With the beginning of the 21st century and the concurrent rise and ubiquitous use of the Internet, it became obvious that surveillance was a phenomenon inherent in everyday life. Surveillance and data collection were no longer restricted to specific sites, but myriad forms of watching, recording and analysing are applied. The political-economic context moved to consumer capitalism and the economic significance of personal data increased significantly. In globalised, highly connected knowledge and information societies, where new tokens of trust are constantly required, and where organisations (and individuals) must continually identify and assess risks and work out ways to avoid or minimise those risks, ICTs are the the means of co-ordination and exchange. Web-generated data, GPS, GSM and Wi-Fi based location determination, biometric identification and communications surveillance all play an important role in the collection of information, data mining and social sorting.

Meanwhile, contemporary discussions about surveillance are inevitably entangled with the terrorist attacks of 11 September 2001. Although the so-called "war on terror" is only one rationale for the use of surveillance systems, unquestionably terrorist attacks have reinforced already existing anti-terrorist monitoring regimes. Policy responses within the US and Europe contain several far-reaching measures comprising changes in wiretapping laws, search warrants and the rules on the exchange and storage of personal data within and between countries.

There is no one-way causal relationship between the development of technologies and their application for surveillance purposes – but instead complex, context-dependent, social, political, historical and technological dynamics which interact and shape surveillance practices. The development of technologies financed by state agencies has gradually shifted from military to civil use. Policy reactions to real or perceived internal or external threats, broader developments affecting society as a whole (such as increased risks in a globalised world and the proliferation of information and communication technologies), the rise of consumer capitalism and changes in the willingness of individuals to share personal information, all play a role in the co-evolutionary development of surveillance technologies and surveillance practices. Surveillance is, and has always been, an element of modern society, but dominant societal changes, increasing economic interests in the individual, influential policy responses to unexpected looming events and the normalisation of surveillance has made surveillance a dominant facet of contemporary societies indeed. Although surveillance may be labelled normal, huge issues arise, e.g., in terms of transparency and the lack of accountability connected with the unclear purposes and efficiency of surveillance measures; the inherent danger of function creep causes concern as the specter of totalitarianism rises in eroding democracies.

THE SURVEILLANCE INDUSTRY IN EUROPE

The main objective of this Task is to identify and characterise the surveillance industry in Europe. Here, the surveillance industry (in a broad manner) refers to all the actors involved in the commercial production, trade and/or offering of surveillance products and services (or products and services that satisfy surveillance needs).

Overview

First, this task discusses surveillance markets in key surveillance areas such as biometrics, deep packet inspection, smart cards, RFID, smart homes, unmanned aerial systems, x-ray security screening, video surveillance. It profiles surveillance customers and discusses the drivers and inhibitors of markets. Second, it surveys the security and allied industries and identifies companies engaged in the business of surveillance in Europe. Since it was impossible to examine all identified companies within the task's limited timeframe, we analysed a sample of 39 leading companies in depth to characterise the European surveillance industry. We highlights the motivations, main offerings, features of and controversies beleaguering the industry. Third, the task outlines the surveillance industry's future market prospects and discusses competition and challenges. Fourth, the task identifies and analyses the nature, role, activities and effect of industry associations. Fifth, we examine the impact of the surveillance industry on security policy and research. Sixth, the task focuses on the surveillance industry and fundamental rights – it considers the attitude of the industry to human rights concerns, and highlights actions and good practices. Finally, the task identifies the watchers of the surveillance industry – i.e., the entities monitoring the surveillance industry, their monitoring motivations, actions and effects upon industry.

Key themes and findings

The global and European surveillance industry is developing at a rapid pace. Supply is increasing demands in both the public and private sector, across a range of areas such as national defence and security, critical infrastructure, banking, employment, energy and utilities, entertainment, finance, government, healthcare, policing and justice, retail, telecommunications, travel and transport. Various factors drive the industry: pro-surveillance policy and legislation, research and innovation, financial support and funding, profits, positive media coverage and public demand. On the other hand, inhibitors such as policy shifts, restrictive legislation, inadequate research, the apparent need for development and innovation, lack of financing and funding, losses, negative media publicity and lack of public demand or rejection affect its growth.

The surveillance industry in Europe is characterised by a diversity of companies (based on organisational history, revenues, size, location, operation and organisational focus) that provide a variety of surveillance solutions. The industry is profit-motivated and driven. Investment in manufacture, integration, provision or sale of surveillance technologies generates high levels of income for companies fuelled in particular by the government or public sector demand and expenditure. To boost their position and influence, surveillance companies are collaborating, making acquisitions and forming strategic partnerships and alliances, and entering into joint ventures with other companies, academia and research institutions.

The surveillance industry in Europe is characterised by the presence of a large number of non-European companies, particularly from the USA. Conversely, European companies, driven by the economic downturn in Europe, the huge potential of foreign markets and their receptiveness to surveillance solutions, are investing heavily in non-European markets in North and South America, Asia and Africa.

Surveillance companies have courted controversies such as unethical and even illegal business practices, illegal government subsidies, privacy and security concerns, sale of

technologies to authoritarian and undemocratic regimes, human rights abuses, conflict zone profiteering, general surveillance-related profiteering and pro-surveillance thrusts, misleading consumers, and anti-competitive practices. Overall, this has affected the industry's reputation as a whole. The European surveillance industry (individual companies and industry associations) needs to take stock of this.

Conclusion

In sum, the future of surveillance is set. We predict an increasing demand for surveillance solutions (stand-alone and integrated), rapid growth for the industry and strong market prospects, specifically based on the following trends: (1) a substantial growth of public sector demand for surveillance bolstered by the adoption of identity schemes, and terrorist detection technologies and markets, (2) an increase in the demand for civil/commercial surveillance, (3) the development of a global surveillance industry, (4) an increase in integrated surveillance solutions, (5) a rise in "international surveillance wars", by which we mean not only surveillance and cyber espionage by governments,[1] but also that surveillance companies from Europe will face stiff competition from companies based outside the European Union.

Despite the positive outlook for the European surveillance industry, it faces the following challenges: a lack of security awareness and attitudes, resulting from a decreased demand for security and surveillance products and services; stricter government regulation which may stifle the development and growth of the industry; financial challenges such as higher duties and costs; public rejection of technologies due to privacy, ethical and other human rights concerns; non-EU based competition. The industry needs multi-level strategies to deal with these.

Surveillance industry associations play an important role in the industry and in interactions with other stakeholders They promote and increase the use of their members' products and services, facilitate collaboration, promote research and development, establish policy, guidelines and standards, engage with the public and raise awareness of concerns such as security, safety, crime prevention and prosecution that ultimately drive and boost the demand for the surveillance industry's products and services. These associations influence security policy at different levels – e.g., government, law, research. They organise events, provide information and training, conduct networking activities, fund research, develop best practices, lobby government and policy-makers, develop strategic partnerships, maintain public and media relations. In any societal resilience-building exercise that needs to have deep impact, it would be advisable to harness the power of these associations.

Surveillance companies exert a great amount of influence through participation in security policy-related bodies such as the European Defence Agency (EDA), the European Organisation for Security (EOS) and European Security. They increasingly intersect with the public sector in performing traditionally public sector-restricted activities and are involved in a number of European research projects on security, information and communication technologies.

Though some surveillance companies provide assurances that they act in conformity with legal and social obligations and values, mostly these are inadequately expressed and followed

[1] Quite a few stories have appeared in the news media recently on this issue. See, for example, Taylor, Paul, "Former US Spy Warns on Cybersecurity", *The Financial Times*, 2 Dec 2012.
http://www.ft.com/cms/s/0/ed7ff098-3c4d-11e2-a6b2-00144feabdc0.html#axzz2DtVealdH

through. A majority of companies neglect this aspect. Key concerns include issues of privacy, data protection, freedom of expression, and freedom of movement. While some good practices exist, these are not enough; they are inadequate in terms of the intrusive potential of some of the surveillance technologies the industry is developing and marketing.

No one entity (i.e., government, media, civil society, academia or individuals) can play a self-sufficient or exclusive role in watching over the surveillance industry. Individually, each watcher is limited by its personal motivations and activities. Given the nature of the industry and its escalating potential to infringe upon fundamental rights and liberties, we recommend the formation and development of multi-stakeholder platforms or forums to monitor the industry (greater collaboration between *all* stakeholders) for greater effect and for building the resilience of society to surveillance.

THE EFFECTIVENESS OF SURVEILLANCE IN PREVENTING AND DETECTING CRIME AND TERRORISM

The fight against crime and terrorism has been a major driver for the development and implementation of surveillance technologies for a long time. Police work provided a test bed for the development of new technologies. On the other hand, various technologies developed for other purposes outside law enforcement have been put to use for fighting crime. A prominent example is the use of information collected by mobile phone service providers for their own administrative purposes, which is now regularly shared with police for their investigative purposes. While there seems to be a close and obvious link between surveillance and law enforcement, a closer look reveals problems, including the following:

1. Crime is not a natural kind but a socially defined legal-bureaucratic category. All data about the volume of crime in a society are the product of complex administrative procedures. When assessing the effects of different surveillance technologies on preventing and detecting crime, the data have to be interpreted with great caution.

2. Surveillance technologies are not evenly applied to prevent and detect all sorts of crimes and not all technologies lend themselves to all types of crimes. This makes it difficult to produce an overall conclusive assessment of the effectiveness of surveillance in preventing and detecting crime and terrorism.

3. Systematic evaluation studies conducted by independent researchers about the use and effectiveness of surveillance technologies are rare. Technologies such as CCTV that have been evaluated show mixed results. Long-term effects may counter short-term effects; external effects, such as displacement of crime from one surveilled neighbourhood to another, less or not surveilled neighbourhood, have been reported in the literature.

4. The use of surveillance technologies in the field of law enforcement has to be understood as being embedded in the emergence of the modern bureaucratic state. Individuals and the social world have to become “machine readable” in order to apply certain technologies of surveillance (e.g., automated number plate recognition, ANPR).

5. An important aspect in the development of surveillance technologies is the introduction of electronically mediated digital forms of data processing. With the growth of data collected through surveillance (e.g., finger prints), the management and retrieval of information

becomes time consuming. When this information is available in a digitized format, and search procedures can be performed automatically, the use of the stored data in the context of fighting crime (e.g., comparing data from crime scenes with information stored in police data files) is easy.

6. Digitizing the processing of data from surveillance technologies also creates new assemblages, combining information from different sources to identify or describe an individual. These data can be communicated and made available wherever there is access to a computer.

7. The growth of modern surveillance technologies fosters a shift in the orientation of policing from a reactive form of "thief-taking" to a proactive approach, focussing on prevention and early identification of potentially suspicious individuals. This again promotes a shift from the focus on the "criminal" to the control of so-called "pre-criminal" but in itself legal behaviour.

8. Surveillance technologies also affect the working routines of law enforcement personnel. Doing police work in an "information-intensive" environment creates new forms of policing, with new tasks, requiring new capabilities and competences typically not available to the traditional street cop. The emerging new forms of "intelligence-led" policing require a new type of professional police officer.

9. Surveillance technologies used in preventing and fighting crime often create problems of legal regulation with regard to fundamental norms of data-protection and privacy. With the growth of encompassing preventive surveillance the presumption of innocence as an important legal safeguard is gradually hollowed out.

10. Surveillance technologies can be categorized based on functionalities: identifying, locating, tracking individuals; screening populations and flows (of data, money, etc.). Some technologies operate remotely (e.g., CCTV), others require some sort of physical contact with individuals (e.g., DNA-sampling). Combining technologies with different functionalities creates comprehensive data doubles of individuals that can be used for law enforcement purposes.

SOCIAL AND ECONOMIC COSTS OF SURVEILLANCE

Following a comprehensive literature review, we have identified and describe the main categories of social and economic costs of surveillance. Social costs include effects such as discrimination, social exclusion and the increasing pressure for conformity as a consequence of surveillance. Beyond the direct costs for implementation and operation of surveillance systems, economic costs include potential long-term economic consequences, e.g., reduced innovativeness and subsequent losses in competitiveness due to the chilling effects of surveillance. We have also developed a taxonomy of the social and economic costs related to surveillance, which enables a more systematic analysis of different cost categories associated with surveillance measures.

Overview

We have identified two important difficulties in determining the social and economic costs related to surveillance. The first arises from the fact that the actual and potential surveillance

contemporary societies are facing is a rather new phenomenon; only recent progress in information technologies has allowed for the introduction of new forms of mass surveillance, and rapid technical progress is still changing the face of surveillance. Accordingly, many categories of social and economic costs may neither have materialised nor been identified yet. Second, social and economic costs are in themselves far from being commonly understood, well accepted and easily applied concepts.

Hence, we have created a framework for a taxonomy of social and economic costs, based on a layered approach utilised in the context of privacy impact assessments (PIA). It distinguishes four different cost layers, differentiating the individual layer, the relational layer, the group layer and the social and political layer. These layers are exemplified by costs mainly belonging to the social category. Social and economic costs are related and partly overlapping categories; the associations between them are briefly illustrated on the basis of false positives and costs of errors.

We have identified two key types of social costs of surveillance, costs related to exclusion and discrimination and costs of conformity. Our discussion on exclusion and discrimination focuses on the preventive dimension of contemporary surveillance policies. From this starting point, we address the issues of false positives and social damage, categorical suspicion and discrimination, marginalising effects and social inequalities, inhibition and the relation of privacy, societal harm and erosion of trust. Our discussion of surveillance and conformity focuses on the relation between conformity and bureaucratic rationality, classification and panopticism from a theoretical perspective. Our analysis of the costs of conformity is based on the (scarce) empirical work on this topic; it embraces the social domains of the workplace, schools, medicine, social media, sports coaching and public housing.

We include two case studies on the economic costs of surveillance,which exemplify the notoriously difficult process of estimating costs comprehensively. The first case study concerns body scanners; we compare European and US evaluation approaches. The second case study concerns the European External Border Surveillance System (EUROSUR), wherein we compare , the cost assessment by the European Commission with alternative estimates. Both case studies show specific shortcomings of the individual assessment efforts and a more general lack of (reliable) data.

The last section of our chapter on social and economic costs addresses the relevance of social and economic costs of surveillance in the context of decision-making. It briefly summarises the different cost categories, which should, in an ideal situation, all be reflected and compared to the benefits in decision-making processes on surveillance measures. It also describes the importance of taking social and economic costs properly into account for the legitimisation and justification of surveillance in democratic societies.

We then draw our main conclusions, which address the need for broad and participatory evaluation of costs (and benefits) of surveillance in view of the many practical and theoretical difficulties in identifying and quantifying the social and economic costs of surveillance.

Key findings

- Identification of alternatives and consideration of costs and (not materialised) benefits should be included in cost estimates.
- More research on long-term societal impacts and costs of surveillance is needed.

- The unintended consequences of surveillance and its costs are presumably unacceptably high: e.g., effective preventive surveillance and profiling produce unacceptably high rates of false positives.
- Existing cost estimations suffer from a lack of reliable data and are only taking into consideration direct costs, ignoring (long-term) social and economic costs.
- Full consideration of social, economic and political costs would presumably result in decisions diverging from the current main focus on surveillance.
- Open and participatory debates can compensate for the fundamental difficulties of comprehensive estimations of social and economic costs of surveillance.

Conclusion

The increasing reliance on surveillance measures and technologies in contemporary security policies is based on an insufficient and incomplete knowledge and consideration of the social and economic costs of surveillance. In both categories, the real, long-term costs might be much higher than anticipated and erode the very basis of our liberal societies, economic well-being and democratic values.

The relevance, magnitude and importance of social and economic costs of surveillance and the difficulties of identifying, assessing and quantifying them lead us to make two recommendations: First, more research in methods of the analysis of social and economic aspects of surveillance is needed to improve the reliability and comparability of such assessments. Second, the complexity of the involved issues and the danger of domination by individual interests demand representation of different interests and perspectives in any decision-making process on surveillance.

IMPACTS OF SURVEILLANCE ON CIVIL LIBERTIES AND FUNDAMENTAL RIGHTS

This Task first examines the propensity of surveillance systems to infringe fundamental rights and values. Distinguishing between different forms of surveillance, it draws on the literature dealing with the impact of surveillance on a variety of specific but inter-related rights, freedoms and values that are considered to be at risk through the use of surveillance technologies and systems. The Task starts by commenting on the effects of surveillance on privacy, dignity, autonomy, and various rights and freedoms as well as values. Going beyond privacy, the effects of surveillance on different categories of people are examined. This is a neglected focus in many sources on privacy, which deal with “data subjects” as legal abstractions who have rights, but which rarely investigate the differentiated, and often systematically biased, effects of surveillance on various social categories. Scholars in the emerging field of surveillance studies as well as others, however, regard the social patterning of surveillance and the unevenly distributed ability of individuals and groups to have their privacy protected as an essential focus of analysis and policy. Turning the question around, the impacts of fundamental rights and values on surveillance systems are considered in terms of how they might affect the design, deployment and oversight of surveillance systems, in the light of the current emphasis being given by those who are involved in regulation and governance to ways of mitigating surveillance through technological and systemic measures. Some instances of best practice are mentioned, where surveillance systems have the least negative impact on fundamental rights while still being (seen as) relatively effective.

The main subject areas

The Task distinguishes among the variety of surveillance practices (e.g., watching, listening, locating, detecting, dataveillance) in use in different situations (e.g., transport, public space, private premises databases, communications facilities, online transactions). It is important to consider the visibility, legality and power implications of surveillance in assessing the impact of surveillance upon social, economic and individual benefits, and upon individual privacy and freedoms and the texture of social life and relationships.

Privacy is a complex term with no agreed meaning. It must be disaggregated in terms of overlapping subjects (e.g., privacy of the person, privacy of behaviour and action, privacy of personal communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space, privacy of association (including group privacy)). The literature also identifies several general and overlapping types of privacy (the right to be let alone, limited access to the self, secrecy, control over personal information, personhood, and intimacy). Another prominent classification concerns states of privacy: solitude, reserve, intimacy and anonymity. It is important to consider a variety of values associated with, or even incorporated within the meaning of, privacy (autonomy, dignity, liberty, personality, self-determination). In addition to its importance as an individual right, privacy is of value for society and the political system in terms of social integration, political democracy, the rule of law, and equality of treatment across individuals and groups. We endorse a growing trend in contemporary discussions of privacy and surveillance: emphasising the importance of *context* in any proper understanding of the way privacy works in myriad situations in which norms operate to shape relationships, interactions, and outlooks. An appreciation of context also serves to avoid deterministic and non-empirical suppositions about the implications of technology for society, individuals, rights and values.

We examine the effects of surveillance on privacy, autonomy and dignity, drawing upon the relevant philosophical and social-science literature on these values, and illustrating them in terms of particular technologies that often impinge upon them (e.g., electronic monitoring, phone tapping, CCTV, airport security routines including body scanning, the use of DNA). We then turn to the effects of surveillance of freedom of assembly and association, and on freedom of expression, discussing the theoretical and practical consequences of surveillance on the public sphere. We consider these in terms of the framework of rights laid down in the European Charter of Fundamental Rights and the European Convention on Human Rights, and in view of the developing case law of the European Court of Human Rights. We investigate surveillance online and surveillance and freedom of movement, discuss surveillance and discrimination, social integration, the rule of law, the presumption of innocence, due process of law, and equality of treatment. We highlight the technologies and practices of movement tracking and tracing in these discussions, as well as categorisation through data mining and profiling (including racial profiling), control of public space through video surveillance, and dataveillance. We also outline new trends in criminal law as part of our analysis of the effects of surveillance, showing the growing trend towards pre-emptive, predictive approaches to policing and crime detection.

We consider the effects of rights and freedoms on systems design, given the requirement that surveillance technologies and systems should comply with human rights and privacy protection. We discuss privacy by design (PbD) and privacy-enhancing technologies (PETs) as leading instruments in shaping technological systems, and give some examples of good practice (e.g., in online browser settings, identity verification, and body scanning). Finally, we

consider the effects of rights and values in the oversight of systems, highlighting the regulatory and oversight relevance of privacy impact assessment (PIA), of the work of data protection authorities, and of the Article 29 Working Party as institutions.

Key themes and emergent findings

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

a. Surveillance technologies and practices have an actual or potential impact (mainly negative, but sometimes positive) upon a wide range of individual and trans-individual rights, freedoms and values.
b. The effects of surveillance go beyond those that concern individual privacy, dignity, autonomy and the presumption of innocence, and can also be seen in terms of various dimensions of social and political life.
c. There are gaps and deficiencies in the law and in jurisprudence as they struggle to keep pace with technological development and institutional practice, perhaps especially in an online environment and in a climate of enhanced law enforcement and counter-terrorist policy.
d. More effective regulation requires that existing regulatory philosophies, practices, laws and enforcement incorporate better development of anticipatory regulatory strategies that include design-stage controls, governance and evaluative instruments.

Conclusion

Discussing the impact of surveillance on a host of rights and values, and the impact of rights and values on surveillance requires conceptual disaggregation and clarity, detailed and systematic analysis, and empirical evidence. The degree to which all these *desiderata* are currently available is uneven, but our report shows how they can be brought to bear on a subject that is sometimes ambiguous (e.g., the concepts of privacy and surveillance) and sometimes not easily amenable to reliable empirical research (e.g., social and psychological effects), but with reasonable prospects of making subsequent judgements about the resilience of societies in the context of surveillance.

1 INTRODUCTION TO CONCEPTS AND TERMS

Ivan Szekely, EKINT

In the course of the present research, the members of the research consortium had the ambition to define a core set of notions and concepts and to use them in a coherent way in the analyses throughout the whole project. Where possible, such notions and concepts should be generally accepted in professional literature and scientific discourse, and should be suitable for interpreting and explaining the research results for decision-makers and the general public. A further ambition of the research consortium was to take into consideration the practice and findings of other EU projects dealing with related research questions and working in similar areas. This has relevance in two aspects: first, this way the duplication of certain unnecessary basic research into terms and concepts can be avoided – that is also a precondition of the efficient use of research resources – and second, the common understanding of terminology can ensure the comparability and joint interpretation of various sister projects in the EU, thereby implicitly providing terminological guidance for future research work.

The aim of this brief introduction is to identify some core notions and concepts, which are relevant not only for the present deliverable, but for the whole research, too, and to outline their content as understood throughout the lifecycle of the project. This also means that if a project deliverable were to use a notion or concept with a meaning different from what has been outlined here, writing of specific notes and explanations would also be necessary. Naturally, we do not aspire to enlist and define all terms and concepts used in the course of the research; we are focusing on those notions which have multiple interpretations in professional literature or in public opinion, or their sphere of interpretation may vary according to the context.

Evidently, *surveillance* is a core notion in IRISS and has a central importance in the analyses. The basic content and criteria of this notion are widely known and commonly understood; however, this term is used in rather diverse contexts and connotations, a part of which has no relevance for the present research. The subject of surveillance can be events, locations, temporal changes, patients in health care, etc. – these manifestations of the generic notion of surveillance fall outside the scope of our research. In this project, we regard surveillance in a meaning narrowed down to human subjects. We basically accept David Lyon's definition, according to which "it is 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"; [2] however, at the same time we deem necessary to emphasise three fundamental criteria of surveillance: there is an information asymmetry between the partners (the surveilling party is in the stronger position)[3], surveillance is performed in a non-transparent way (or secretly), and there is a lack of choice on the part of the surveilled subject.[4]

[2] Lyon, David, *Surveillance Studies, An Overview*, Polity Press, 2007, p. 14.
[3] See for example, Gandy, Oscar H., *The Panoptic Sort: A Political Economy of Personal Information (Critical Studies in Communication and in the Cultural Industries)*, Westview, 1993.
[4] Because an employee or a child knows they are being surveilled does not make surveillance transparent. Even if the employee knows about it, or can see the CCTV cameras, she cannot fully oversee who can have access to her data or when The same is the case with children surveilled by parents.

We also regard the definition used in a sister FP7 project, the Ethical Issues of Emerging ICT Applications (ETICA),[5] which is comprehensive and at the same time specific enough:

> Monitoring of the physical, mental, economic, cultural, social or other activities of identified or identifiable individuals, irrespectively of the means and methods applied, whether automated or human interaction-based, mass or individually targeted, continuous, repetitive or ad hoc, perceptible or imperceptible, done physically or from a distance by means of electronic equipment, done in real-time or retrospectively, based on the activities of the individual him/herself or on the analysis of the personal data of the individuals concerned.

When defining an *identifiable person*, we rely on the definition used by the Data Protection Directive of the European Union: a natural person who can be identified, directly or indirectly, in particular by reference to an identification code or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[6] Similarly, we follow the general definition of the EU directive of *personal data*, namely as "any information relating to an identified or identifiable natural person (the data subject)".[7] The content, extent and limits of the concept of the relationship between the data and the person concerned, and those of "identifiedness" or "identifiability" are constantly changing and being disputed, mainly because of the developments in the application of emerging technologies. We deem the detailed interpretation of this notion prepared by the Article 29 Data Protection Working Party of the EU particularly useful.[8]

Personal profiles, the inherent results of surveillance of identifiable individuals, are more than just personal data. A personal profile is a set of personal data, typically collected and developed through registration of such data or monitoring the activities of the persons concerned, which describes a part of the personality of the individual and can serve as the basis for drawing (true or false) conclusions regarding the past activities of the individual, or predicting his or her future behaviour or activities. Decisions influencing the life of individuals in a modern society are based increasingly on these profiles, also called their information replica or data double. These profiles can represent different parts or cross-sections of the individual but can never cover the totality of the personality. Emerging information technologies such as ubiquitous computing or ambient intelligence multiply the capabilities of the controller of such personal profiles and hide this practice from the data subjects, making the traceability of one's own data and the exercisability of one's informational self-determination even more difficult.

Since we regard information asymmetry between the parties as a fundamental criterion of surveillance, *information power* is also a concept that needs to be recognised in the course of the research. Informational power is the capacity of exerting influence or control by one party over another party by possessing, or having the capacity to possess, significantly or persistently more information about the other party than the other party possesses, or has the capacity to possess, about the first party. Any informational relationship, even a momentary one, has a stronger and a weaker side. The stronger party always has more information about this relationship; typically, the weaker parties cannot even be sure what it is exactly that the

[5] http://ethics.ccsr.cse.dmu.ac.uk/etica

[6] European Parliament and the Council, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data, Official Journal of the European Communities, L 281, 23 November 1995, pp. 31-50, Article 2(a)

[7] Ibid., Article 2(a)

[8] Article 29 Data Protection Working Party, Opinion 4/2007 on the concept of personal data. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

stronger side knows about her. Such a situation may deprive the weaker parties of the possibility to make deliberate decisions, thus distorting the behaviour of the actors both at individual and societal levels. This reasoning was included in the cornerstone decision of the Federal Constitutional Court of Germany that lay the foundations of the concept of informational self-determination.[9]

Of similar importance for the whole project are the terms *privacy* and *security*. The interpretation of these terms has an extensive literature in which the reader often finds contradictory or partial approaches. Several EU research projects conducted in recent years have been focusing on research areas involving the use of these concepts; some of these projects regarded the clarification and interpretation of either or both of these terms as their explicit task. As it has been discussed extensively in the conceptual framework of a running sister FP7 project, the "PRIvacy and Security MirrorS: Towards a European framework for integrated decision making" (PRISMS),[10] several authors emphasise the elusive nature of these terms, especially that of privacy. The notion of privacy "remains out of the grasp of every academic chasing it";[11] it is "an unusually slippery concept",[12] and can be understood rather as contextual integrity where the core problem is sharing of information outside of socially agreed contextual boundaries.[13] This leads to the issue of the relationship between privacy in general and information privacy (or the corresponding European term data protection) in particular.

It is a common understanding of the research consortium that privacy is a broader concept than information privacy or data protection, and it is possible to infringe someone's privacy without processing personal data at all. Nevertheless, as noted in the ETICA project, during the evolution of the definition of privacy, irrespectively of the differing legal, sociological or philosophical approaches, two main trends can be observed: (a) the weight of the information elements has increased, and (b) the negative and passive approach has been shifted towards a positive and active approach.

For the purpose of categorising the various domains of privacy, we deem useful the taxonomy developed – on the basis of previous researches – in the framework of the FP7 project "Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment" (PRESCIENT).[14] The seven main types of privacy distilled from this taxonomy, as identified by Finn et al. (2013) are: privacy of the person, privacy of behaviour and action, privacy of communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space, and privacy of association (including group privacy).[15]

We also regard privacy as a vital element of democracy and contemporary Western society because "it affects individual self-determination; the autonomy of relationships; behavioural independence; existential choices and the development of one's self; spiritual peace of mind

[9] BVerfGE 65, 1 (15.12.1983).
[10] http://prismsproject.eu
[11] Gutwirth, Serge, *Privacy and the information age*, Rowman & Littlefield, Lanham, 2002, p. 30.
[12] Whitman, James Q., "The Two Western Cultures of Privacy: Dignity Versus Liberty", *The Yale Law Journal*, Vol. 113, 2004, pp. 1151-1221 [pp. 1153-54].
[13] Nissenbaum, Helen, *Privacy in Context: Technology, Policy and the Integrity of Social Life*, Stanford University Press, Stanford CA, 2010.
[14] http://www.prescient-project.eu/
[15] Finn, Rachel L., David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Yves Poullet et al. (eds.), *European Data Protection: Coming of Age*, Springer, Dordrecht, 2013[Ffrthcoming].

and the ability to resist power and behavioural manipulation."[16] In using the term privacy, we also take into consideration that it is at the same time a value, a demand and a codified right (which is broader than the right to data protection, although not separable from it, with special regard to the historical evolution of the concept in which the information element has become of fundamental importance in today's information society – this is especially true in the relationship between privacy and security).

We understand *data protection* as the complex of principles, norms, procedures, data processing devices, means and methods restricting the collection, processing and use of personal data, and protecting the persons concerned. This definition is more generic, or rather interdisciplinary, than the definitions used by either legal or IT professionals. Since in the area of emerging technologies the data processing devices, means and methods will expectedly have an inseparable and ubiquitous character, the use of such a broader definition can be justified. Data protection should be clearly distinguished from *data security*, i.e., from the physical, organisational and human measures aimed at guaranteeing the confidentiality, authenticity and availability of any data (not only personal data) in information systems.

In our approach, privacy – similarly to security – is not a static concept, not an ideal state that one should endeavour to reach, but a dynamic concept changing throughout historical evolution and depending on the context, which has basic principles and context-dependent elements alike.

According to the widely quoted and accepted general definition prepared by the working group BT WG 161 of the European Committee of Standardization (CEN) in 2005, *security* is "the condition (perceived or confirmed) of an individual, a community, and organisation, a societal institution, a state, and their assets (such as goods, infrastructure), to be protected against danger or threats such as criminal activity, terrorism or other deliberate or hostile acts, disasters (natural and man-made)".[17]

One can classify this broad definition into certain categories based on the *subjects* of the condition of security, for example, security of international organisations, security of the State, security of companies, security of the civil society and movements, and security of individuals and households. One can also classify each of these categories according to their premises, definitions, the potential threats, possible counter-measures and their limitations.[18]

The PRISMS project further refined the content of the possible matrix of security according to the *type* of security: physical, political, economic, cultural, environmental security, as well as radical uncertainty security and information security. From this wide range of aspects, the present research understands security as "human security" or "security of the citizens".

A fundamental approach of our research is that neither privacy nor security is part of a zero sum game in which we must take away the same amount from the implementation of one concept that we add to the implementation of the other, and it is entirely up to us where we actually draw the line: it is possible to create an environment where both concepts are implemented at a high level. Similarly, privacy is not the antagonist of public goods – on the

[16] Gutwirth, op. cit., 2002.
[17] See for example, Beyerer, Jürgen (ed.), *Future Security. 2nd Security Research Conference 2007, 12th - 14th September Karlsruhe, Germany*, Universitätsverlag Karlsruhe 2007, pp. 53-54.
[18] For more detail, see Zedner, Lucia, *Security: Key Ideas in Criminology*, Routledge, London, 2009.

contrary, privacy itself is a public good, as is security. In this regard, surveillance is a link representing the interrelatedness of privacy and security in practice.

We cannot leave out from this introduction to terms and concepts the definition of *law* and its related concepts, their value content and relationship to ethics. The fact that our research is focusing on the European Union, more precisely, the Member States of the EU, their legal systems and the common European legal framework, emphasises the need for clarifying these concepts at the European level, too. We understand law as general rules made by the legitimate lawmakers that apply equally to everybody. The law should especially not single out any specific persons or group of persons; the rules must apply to those who lay them down and those who apply – that is, to the government as well as the governed – and that nobody has the power to grant exceptions. Law has an intermediary role between ethical norms and reality.[19]

Not every legal system may be titled as "constitutional" even if the legal system has a formal constitution. *Constitutionality* is a set of requirements or principles, which characterise the substance and realisation of an ideal and democratic constitution. It is a system of norms, which is governed by the principles of popular sovereignty, division of powers, rule of law, legal egalitarianism and fundamental rights and freedoms. Their function is to guarantee that the provisions of the constitution do not remain only ceremonially declared items.

The concept of the *rule of law* has two main interpretations. According to the formal interpretation, the law must be prospective, well-known, and have characteristics of generality, equality and certainty – however, this interpretation does not contain any requirement regarding the *content* of the law. Therefore, we follow the substantive interpretation of this concept, according to which the law that intrinsically protects some or all individual rights is above everyone and it applies to everyone. This approach allows us to protect democracy and individual rights, but at the same time recognises the existence of the rule of law in countries that do not necessarily have laws protecting democracy or individual rights.[20]

One of the basic arguments intended to justify surveillance is the need to fight *crime* and *terrorism*. However, neither crime nor terrorism has a universal definition; a major challenge for criminology is to identify and apply appropriate definitions of crime and terrorism in its domains. Crime seems like a common sense category, and in public opinion it is usually associated with harm and violence. The various definitions of crime can be divided into two main categories: legal and sociological.[21]

According to the legalistic approach, crime is the breaking of rules of law for which a governing authority can prescribe a conviction. (In the US legal terminology, crime, as an offence against the public or the state, is distinguished from torts, as wrongdoings against private parties.) In the sociological approach, crime is a deviant behaviour that violates prevailing norms and cultural standards in society. Due to the formalised characteristics of law and the slow pace of lawmaking, the sociological approach is more suitable for

[19] See Hayek, Friedrich, *The Constitution of Liberty*, University of Chicago Press, 1960.
[20] For more details on the different interpretations of the rule of law, see Tamanaha, Brian Z., *On the Rule of Law. History, Politics, Theory*, Cambridge University Press, 2005.
[21] In criminological literature, there are various, more detailed taxonomies of crime. See, for example, Morrison, Wayne, "What is crime? Contrasting definitions and perspectives", in Hale, Chris et al. (eds.), *Criminology*, Oxford Univeristy Press, 2009.

understanding and considering the complex realities of society and the changing social, political, psychological and economic conditions which may affect our judgement of what constitutes a deviant behaviour and what kind of deviances should be regarded as crimes. According to radical critics of the legalistic approach, "Crime has no ontological reality. Crime is not the object but the product of criminal policy";[22] "Crime does not exist. Only acts exist, acts often given different meanings within various social frameworks."[23]

Terrorism is even more difficult to define. This term is used by various legal systems and government agencies with different, politically and emotionally charged meanings. Experts have counted more than 100 definitions[24] and concluded that "the only general characteristic generally agreed upon is that terrorism involves violence and the threat of violence."[25] Since terrorism is not the only enterprise involving violence and the threat of violence – so does war, coercive diplomacy and organised crime, too – others from the counted 22 different definitional elements of terrorism are also necessary in outlining the meaning of terrorism. Since 1994, the UN General Assembly has been using the following political description: "Criminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes are in any circumstance unjustifiable, whatever the considerations of a political, philosophical, ideological, racial, ethnic, religious or any other nature that may be invoked to justify them."[26] According to Hoffman's more analytical definition, terrorism is "ineluctably political in aims and motives; violent – or, equally important, threatens violence; designed to have far-reaching psychological repercussions beyond the immediate victim or target; conducted by an organization with an identifiable chain of command or conspiratorial cell structure (whose members wear no uniform or identifying insignia); and perpetrated by a subnational group or non-state entity".[27]

It is not the task of the IRISS project to analyse and explore in full detail the nature of crime and terrorism; these notions are relevant in our research only as possible moral and legal justifications for keeping identifiable persons under surveillance. However, there is a concept, which has special importance in understanding the ideologies of the "surveillance society" in the context of crime and deviance: the so-called *actuarial society.* Actuarial society is an instrumentalist social theory, which instead of identifying and controlling normality and deviance in society, tries to solve social problems, especially deviant and criminal behaviour, by preventative measures based on predicting people's future activities with the help of profiling and mass surveillance. The paradigm shift from dealing with the relationship between individuals and communities to statistically predicting and managing social behaviour was first described in the field of criminology and justice.[28] While in a traditional democratic society individual autonomy and privacy is the main rule and surveillance is the exception, in the vision of the actuarial society based on emerging information technologies,

[22] Hulsman, Louk, "Critical Criminology and the Concept of Crime", *Contemporary Crises*, Vol. 10, Nos.3-4, 1986, pp. 63-80.
[23] Christie, Nils, *A Suitable Amount of Crime*, Routledge, London, 2004, p. 3.
[24] See, for example, Schmid, Alex P., and Albert J. Jongman, *Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature*, Transaction Books, New Brunswick, New Jersey, 1988, pp. 5-6.
[25] Laqueur, Walter, *The New Terrorism: Fanaticism and the Arms of Mass Destruction*, Oxford University Press, 2000, p. 6.
[26] 1994 United Nations Declaration on Measures to Eliminate International Terrorism annex to UN General Assembly resolution 49/60,"Measures to Eliminate International Terrorism", of 9 December 1994, UN Doc. A/Res/60/49.
[27] Hofman, Bruce, *Inside terrorism*, Columbia University Press, 2006 (revised edition), p. 40.
[28] See Feeley, Malcolm M., and Jonathan Simon, "The New Penology : Notes on the Emerging Strategy of Corrections and its Implications", *Criminology*, Vol. 30, No. 4, 1992, pp. 449-474.

surveillance and statistical analysis is the main rule and individual autonomy and privacy are the exception.

2 THE CO-EVOLUTION OF SURVEILLANCE TECHNOLOGIES AND SURVEILLANCE PRACTICES

Kerstin Goos, Michael Friedewald, Fraunhofer ISI
William Webster, Charles Leleux, University of Stirling

2.1 INTRODUCTION

In this chapter, we explore the historical development of electronic surveillances technologies starting with a special focus on computer-mediated surveillance since the end of World War II. We analyse how surveillance technology and surveillance practices of governments and corporations have co-evolved over time. We do that by distinguishing different historical periods.[29] In section 2.2, we deal with the origins of surveillance and argue that surveillance is an integral element of human societies and even became a crucial success factor for modern industrial societies. Section 2.3 analyses how the development of computing machinery and surveillance practices have reinforced each other. After briefly touching upon mechanical computing machinery and its impact on census and rationalisation, we focus on various trends in the computer mainframe era (1950-1985) that implicitly or explicitly contributed to an automatisation and sophistication of mass data collection that needed for further rationalisation but with a growing potential for surveillance. Video surveillance, one of the iconic technologies of the emerging surveillance society, is discussed in section 2.4, where we highlight the different factors that shaped the use of video surveillance in the UK and elsewhere in Europe since the early 1990s. In section 2.5, we finally explore the widespread use of surveillance technologies by all kinds of governmental, corporate and private actors in the networked world of the early 21st century. A special focus in this section is put on the instrumentalisation of surveillance in the fight against international terrorism and organised crime.

2.2 THE ORIGINS OF SURVEILLANCE

Surveillance is a multifaceted and ambiguous term, which manifests itself in a range of human behaviours, and social and organisational practices. It is an intrinsic part of human life and is reflected in the way humans relate to one another, how they form their own identities and how social groupings and organisations function. Surveillance as a human practice is rooted in “caring for others”, at an individual level, in the family environment and more widely in societal settings. The desire to “look after” and care for others is extended in social and organisations forms into arrangements which seek to also influence and shape behaviour in ways beneficial to society. This includes the emergence of religious and bureaucratic institutions, which provide a foundation for values, beliefs and practices, which ensure safety, social order and well-being. As such, surveillance is critical to our understanding of religion, human relations and organisational forms. In recent years, developments in new information and communications technologies have transformed the scale and scope of surveillance – and means that surveillance practices, which were once intrinsically human, are now increasingly mediated by new technologies.

[29] We chose this approach even though framing each period is always a bit arbitrary and sometimes criticised as suggesting a logic in history that never existed. See König, Wolfgang, "Das Problem der Periodisierung und die Technikgeschichte", *Technikgeschichte*, Vol. 57, No. 4, 1990, pp. 285-298.

Natural and caring surveillance

The origins of surveillance are timeless and can be claimed to be "natural" in their formation. Surveillance as a human endeavour is embedded in the instinctive protectiveness and care which a mother shows when watching and caring for a new-born infant and by extension how human beings look after each other for their mutual welfare and well-being.[30] Surveillance then is rooted in the need to care for and look after others, both within family settings and beyond. This need to care is normal and results in the monitoring and shaping of behaviour and protecting the ones we care about from detrimental behaviour. The surveillance of others is, therefore, closely linked to controlling the behaviour of others.[31] This takes place not just in the family environment but also in other social settings and results in a desire to provide social order and to nullify socially unacceptable behaviour, which is detrimental to our need to care. Where surveillance is undertaken in order to exert some sort of control over the behaviour of others, it is also concerned with the exercise of power in social relations, between and amongst individuals, and between and amongst social groups.[32]

The importance of care to surveillance and in observing and shaping behaviour can be observed in other social forms, for example, in the development of religious beliefs and practices.[33] Many religions place care at the heart of their doctrine and have institutional arrangements that espouse the importance of caring for others.

Care in a religious setting is also intended to guide behaviour, as we see in the Ten Commandments[34], and there is often an all-seeing, all-knowing panoptic God to ensure the desired behaviour is adhered to. The concept of care and protectionism also transcends to the level of the state when it assumes the role of watching or surveilling its population, supposedly for its own good. This can take the form of surveillance for safety and national security, as well as surveillance for the provision of public services and citizenship – protecting us and caring for our needs. In recent times, the state's role in providing care and protection has required it to use its authority to collect information from citizens and to use its coercive power to shape behaviour. The importance of the caring dimension of surveillance is that it implies that we intrinsically understand the need for surveillance in society and the need for others to undertake surveillance on our behalf and for our benefit.

Surveillance and the state

At the level of the state, surveillance plays a key role in providing safety, security and social order. In most modern state systems, regardless of whether they are a representative democratic or communist system, the state takes on the role of securing national security, safety and social order, whilst at the same time securing the future of the state system. In a modern representative democracy, the role of caring for constituents and communities is undertaken by elected representative and bodies, for example, in parliaments and assemblies, both at the national and regional levels, and involves others acting on our behalf to make

[30] Murakami Wood, David, Kirstie Ball, David Lyon, et al., *A Report on the Surveillance Society*, Report for the Information Commissioner by the Surveillance Studies Network, 2006.
[31] 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.
[32] Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2007.
[33] Stoddart, Eric, *Theological Perspectives on a Surveillance Society: Watching and Being Watched*, Ashgate Publishing, Aldershot, 2011, p. 2.
[34] Exodus 20, 2-17.

decisions about the nature of services to be provided and the allocation of resources. Similarly, a totalitarian or communist state system is intended to ensure the care of the population as well as the longevity and legitimacy of the state system. As Douglas argues: "Thus, surveillance is deeply imbedded in and necessary for the governmental system that seeks to be instantly aware of any potential threats to the state so that it can quash those threats by depoliticizing 'dangerous' portions of the population and exposing them to the pure potentiality of the 'management' of life."[35] In this respect, it is easy to see how the concept of care is translated into paternalistic state activity.

Surveillance in the setting of the nation state is closely associated with military surveillance practices and the development of panoptic activity. Surveillance in a military sense has been undertaken for many years in order to collect, often covertly, information about "enemies of the state". In recent years, such activity has filtered down into domestic settings with technologies and practices designed for military use being used in civil environments.[36] An example of this would be the development of high definition infrared CCTV cameras and systems. A key concept associated with surveillance is the panopticon.[37] The essence of the panopticon was that the physical environment could be shaped in such a way that individuals undertake self-surveillance and self-control and consequently exhibit the types of behaviour desired. Bentham's development of the panoptic prison is the most famous application of the panoptic ideal, but Bentham's vision was that such practices could be extended into all aspects of society, in order to discipline and control citizens.[38]

In this perspective, the physical environment could be manipulated by the state to help deliver social order, public safety and well-being. Surveillance, however, is not the preserve of the state, and it is a mistake to associate surveillance solely with the state's attempts to monitor and control citizens. Its foundation as a normal human activity means that it is equally possible to have the surveillance of the state by citizens and the surveillance of citizens by citizens. For example, in the UK, the introduction of Neighbourhood Watch schemes[39] gives local residents authority to monitor activities in their community in order to encourage desired behaviour, and discourage undesired behaviour.

Surveillance and information

Although the practice of surveillance has its roots in normal human behaviour, developments in technology have transformed surveillance into a set of practices, which appear to be less human and which are often perceived to be about social control. Technological developments, which enabled the development of writing, allowed for the creation of records, and

[35] Douglas, Jeremy, "Disappearing Citizenship: surveillance and the state of exception", *Surveillance and Society*, Vol. 6, No. 1, 2009, pp. 32-42.
[36] Dandeker, Christopher, "Surveillance and Military Transformation", in Haggerty, Kevin D., and Richard V. Ericson (eds.), *The New Politics of Surveillance and Visibility*, University of Toronto Press, Toronto, 2006, pp. 225-249.
[37] Lyon, Surveillance Studies: An Overview, 2007, pp. 203f.
[38] Bentham, Jeremy, "Panopticon": or, the Inspection-House; containing the idea of a new principle of construction applicable to any sort of establishment, in which persons of any description are to be kept under inspection; and in Particular to Penitentiary-houses, Prisons, Houses of industry, Workhouses, Poor Houses, Manufacturies, Madhouses, Lazarettos, Hospitals, and Schools; with a plan of management adopted to the principle; in a series of letters, written in the year 1787, from Crechoff in White Russia, to a friend in England, T. Payne, London, 1791, p. 4.
[39] Webster, C. William R., and J. Hood, "Surveillance in the Community: Community Development Through the Use of Closed Circuit Television", in Keeble, Leigh and Brian Loader (eds.), *Community Informatics: Shaping Computer-Mediated Social Relations*, Routledge, London, 2001, pp. 220-239.

information, which could be collected, stored, used and shared over time.[40] This provided opportunities for the expression of religious beliefs and for the collection of information about citizens, for example, in the form of a census, which could be used for the purposes of taxation and the provision of services. More recently, the development of information and communication technologies has provided new and profound ways of handling information and which have extended the scope and scale of surveillance. In this respect, whilst surveillance is normal, surveillance relations are in many cases mediated by new technology, hence the term TMS: "technologically mediated surveillance".[41]

Surveillance and bureaucracy

Developments in information creation and handling led in the 20th century to the emergence of bureaucracies, especially in relation to the provision of public services. In this period, the bureaucratic organisational form was deemed to be the most efficient way of organising the delivery of large scales services, fairly, in a modern complex society.[42] The bureaucratic organisational form included: hierarchy, office holders, rules and procedures, specialisation, rational activity and the processing of huge amounts of personal information. In this respect, their bureaucratic form, as a means to administering public services, has always been interested in surveillance.[43] Public administrations have always collected large amounts of information about citizens, in order to undertake taxation and to make decisions about the provision of services. In this respect, they are information rich and, as Zuurmond argues, a modern bureaucracy is actually an "infocracy".[44]

This is not just because of its informational relations with citizens and service users but because information flows within the bureaucracy are essential for co-ordinating organisational activity and realising organisational control. Webster further argues, firstly, that public administration has created a technological platform for, and the machinery of, surveillance: "Not only has it built a large bureaucratic machine to process information but it has also invested in the infrastructure to modernise surveillance through enhanced technological practices",[45] but, secondly, that public administration has normalised surveillance through new ICTs, whereby citizens are being increasingly and routinely required or encouraged to provide information in exchange for access to services. Surveillance as a set of practices and norms in this context has therefore become something with which society has become very familiar, and is largely unafraid of, for example, in the widespread acceptance of the need to pass over personal identity information when travelling by plane. The use of these forms of surveillance practices goes largely unchallenged, and society therefore has come to accept the use of technologically mediated surveillance as a common feature of everyday modern life.

The link between surveillance and the bureaucratic organisational form illustrates the universality of surveillance and how such practices transcend organisation form. Surveillance

[40] Senner, Wayne M., *The Origins of writing*, University of Nebraska Press, Lincoln, 1991, p. 1.
[41] Murakami Wood and Webster, "Living in Surveillance Societies: The normalisation of surveillance in Europe and the threat of Britain's bad example", op. cit., 2009.
[42] Weber, Max, *The Theory of Social and Economic Organization*, Free Press, New York, 1947.
[43] Webster, C. William R., "Public Administration as Surveillance", in Ball, Kirstie, et al. (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, London, 2011, pp. 313-320.
[44] Zuurmond, Arre, "From bureaucracy to infocracy. Are democratic institutions lagging behind", in I.Th.M. Snellen and W.B.H.J. van de Donk (eds.), *Public administration in an information age: A handbook*, IOS Press, Amsterdam, 1998, pp. 259-271.
[45] Webster, "Public Administration as Surveillance", 2011, p. 313.

is thus a key practice in the workplace and can be utilised to control the productivity of workers and to ensure compliance with organisational objectives. However, the direction of the surveillance traffic is not all necessarily one way from the employer to employee(s), as Ball makes the point: "There is also evidence that groups of employees are appropriating information and communication technologies to stare back at their employers, exposing unsavoury practices and organizing collectively."[46] Workplace surveillance, in its widest sense, can now be seen to extend beyond the workplace itself through, for example, the use by some employers of social media sites to gather information on employees' and prospective employees' private activities and contacts, for the purpose of assisting with the assessment of their suitability for advancement or appointment.

Surveillance as practice has extended from family settings into organisational environments and is relevant to broader societal structures and institutions. But, while surveillance is all around us, it is also a complex concept, which embodies different emotions and perspectives, and which conjures contradictory visions of care and control. Humans intrinsically understand the deep-seated need for surveillance and the link between surveillance and control. Whilst surveillance is a normal human activity, new ICT developments have transformed surveillance possibilities, and extended the surveillance scope of the state and commercial enterprises. Surveillance is, therefore, a social and technological phenomenon and by definition concerns power relations in society.

2.3 THE BEGINNINGS OF COMPUTER-MEDIATED SURVEILLANCE

Computing and control are deeply intertwined. As a theory and practice of engineering, control was a main impetus for the emergence of automatic information processing since the 19th century. We already mentioned that the modern, centralised state and the gains of productivity in industrial production were at least partly a result of a systematic collection and processing of information, first manually, later increasingly supported by technological means.

2.3.1 The emergence of the computer and electronic surveillance

We may start our presentation of electronic surveillance with the invention of tabulating machines by Herman Hollerith and others at the end of the 19th century. The invention was made in the context of the US Census, which was carried out every 10 years as the basis for apportioning the seats in the House of Representatives among the states and for sharing direct taxes to the federal government. The labour of statistical preparation of the censuses grew greatly during the 19th century, resulting in a dramatic increase of the collected data sets. The rising numbers were a consequence of increased population (from 23 million in 1850 to 63 million in 1890) as well as an extension of the scope of the inquiries (from 96 collected properties in 1850 to 1,969 properties in 1890) due to a growing demand for statistical details. As a result, the count for the 1880 census took 7.5 years.[47] For the 1890 census, Hollerith took up the approach to code information on punch cards and developed machines that allowed the semi-automatic reading and the automatic counting and tabulating of census data. Hollerith's

[46] Ball, Kirstie, "Workplace surveillance: An overview", *Labor History*, Vol. 51, No. 1, 2010, pp. 87-106, p. 100.
[47] Anderson, Margo J., *The American Census: A Social History*, Yale University Press, New Haven and London, 1988.

technique was successful and the 1890 census was completed in only three years at a savings of $5 million.[48]

In subsequent years, tabulating technology was further developed, first for its original purpose to analyse census data, but quickly it became apparent that tabulating machines could be used for all kinds of applications where large amounts of data had to be collected and statistically analysed. This included railroad companies (for freight accounting and statistics) and especially insurance companies.[49]

The wide introduction of tabulating machines not only in governmental institutions but also in enterprises began after World War I. Companies used the technology. Reinforced by the deep concentration and rationalisation efforts in the interwar period, punch card machines were introduced in the areas of accounting, costing and general planning. The ambivalence of the technology was already unmistakable; for IBM punch card machines were not only a means to organise enterprises, but also a means to monitor and control them (see advertisement in figure 1).[50]

While punch cards and electro-mechanical tabulating machines remained the primary way of information processing until the 1960s, the information needs of public authorities and enterprises remained a driving factor in the development of "real" (i.e., electronic, digital) computers in the 1940s.[51] Though the very first computer prototypes were mainly scientific calculating machines, the first commercially marketed electronic computer, the UNIVAC 1, was delivered in 1951 again to the US Bureau of the Census.[52] This indicates a historical continuity in the way computers were used for monitoring or surveillance purposes. The development of computer-based database software and applications since the mid-1950s then marks a next step in the mass collection, storage and processing of personal data with the intention or at least the possibility of surveillance.

2.3.2 Establishing government databases and the origins of data protection legislation

Even before the term "database" came into use in 1964, users of information processing technologies (punch card systems as well as electronic computers) had been using systems for the storage and analysis of structured data (see above). However, the arrival of affordable disk stores during the 1960s provided information systems managers with the opportunity to scrap and replace their punch cards or magnetic tapes with a single database which at the same time allowed a faster and more convenient analysis of data for the purpose of control or surveillance.[53]

---

[48] Reid-Green, Keith S., "The History of Census Tabulation", *Scientific American*, Vol. 260, No. February, 1989, pp. 98-103; Heide, Lars, "Shaping a Technology: American Punched Card Systems 1880-1914", *IEEE Annals of the History of Computing*, Vol. 19, No. 4, 1997, pp. 28-41. To exploit his inventions, Hollerith set up his own company that finally became IBM in 1924.

[49] Yates, JoAnne, "Early Interactions Between the Life Insurance and Computer Industries: The Prudential's Edmund C. Berkeley", *IEEE Annals of the History of Computing*, Vol. 19, No. 3, 1997, pp. 60-73.

[50] Kaiser, Walter, "Technisierung des Lebens seit 1945", in König, Wolfgang (ed.), Propyläen Technikgeschichte Bd. 5. Energiewirtschaft, Automatisierung, Information, Propyläen Verlag, Berlin, 1992, pp. 281-529.

[51] Garfinkel, Simson, *Database Nation: The Death of Privacy in the 21st Century*, O'Reilly, Sebastopol, 2000.

[52] Campbell-Kelly, Martin and William Aspray, *Computer: A History of the Information Machine*, Basic Books, New York, 1996.

[53] Campbell-Kelly, Martin, *From Airline Reservation to Sonic the Hedgehoc: A History of the Software Industry*, MIT Press, Cambridge, Mass., 2003, p. 145.

Deleuze characterises the 1960s and 1970s as a time of generalised crisis.[54] Salient features of this period are the end of colonialism, the Mutually Assured Destruction (MAD) Cold War stand-off, the Vietnam War, the crisis of the modern institutions, the beginnings of the end of the "Golden Age" of Fordist capitalism, the growing recognition of the oppressive character of many of the "alternatives" presented by Communist regimes and the rise of new forms of political action and organisation in response to the perceived limitations of class politics.[55]

Responses to these developments included new defensive architecture[56] and urban design[57], but appeared also in terms of surveillance.[58]

A prominent and often cited example, which reflects the emergence of surveillance intentions, is the proposal of the US Bureau of the Budget to build a National Data Center in 1965.[59] In addition to the original intention of saving costs, some people soon began to detect additional benefits such as the quick creation of accurate statistics. The National Data Center was never built; instead, the government created dozens of databases for each federal agency. Gradually the agencies started exchanging data and to combine their databases to avoid the time and labour intensive acquisition of data and to realise economic network effects. Another motivation of this development was to provide better services to the clients of government services.[60] The uncontrolled growth of government databases, however, finally led to a federal investigation into the question of their privacy implications. [61] In response to the investigation the Privacy Act of 1974 was adopted by the US congress. It was designed to regulate government surveillance but was little effective in stopping the agencies to collect, store and share data about citizens. Short of continual oversight of routine operations, it is extremely difficult for law and legislation to check this sort of bureaucratic surveillance, when the technology and operations are built right into the organisational structure. [62]

Just as government agencies did, private organisations began to develop and implement their own customer databases. Databases were attractive because they were, compared to earlier forms of data storage, i.e., paper-based index boxes, very compact, cheap to run and fast in processes of searching.[63]

The development in Europe was quite similar as in the US, but delayed and with different consequences. In Germany, for instance, the Constitutional Court had decided as early as 1969 in its "micro census decision" that "it is incompatible with human dignity if government

---

[54] Deleuze, Gilles, "Postscript on the Societies of Control", *October*, Vol. 59, Winter 1992, pp. 3-7.
[55] Murakami Wood, David, "The `Surveillance Society': Questions of History, Place and Culture", *European Journal of Criminology*, Vol. 6, No. 2, 2009, pp. 179-194.
[56] Edwards has called this a "closed world discourse" to characterise the language, technologies and practices that together supported the visions of centrally controlled, automated global power at the heart of American Cold War politics. See Edwards, Paul N., *The Closed World: Computers and the Politics of Discourse in Cold War America*, MIT Press, Cambridge, Mass., 1996.
[57] Newman, Oscar, *Defensible space: Crime prevention through urban design*, MacMillan Co., New York, 1972.
[58] Murakami Wood, "The `Surveillance Society': Questions of History, Place and Culture", 2009.
[59] Garfinkel, 2000; Murakami Wood, "The `Surveillance Society': Questions of History, Place and Culture", 2009. Parenti, Christian, *The Soft Cage: Surveillance in America, from Slave Passes to the Patriot Act*, Basic Books, New York, 2003.
[60] Nunn, Jr., Edgar S. , "The Idea of a National Data Center and the Issue of Personal Privacy", The American Statistician, Vol. 21, No. 1, 1967, pp. 21-27; Garfinkel, 2000.
[61] Ware, Willis H., Records, Computers and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems, The Rand Corporation, Santa Monica, 1973.
[62] Lyon, David, *The Electronic Eye: The Rise of Surveillance Society*, Polity Press, Cambridge, 1994.
[63] Ibid.

claims the right to compulsorily register and index citizens' total personality".[64] This not only led to the first German data protection law in the state of Hesse in 1970 (and eventually the Federal data protection law) but also had consequences for the planned development of government databases.[65]

One of these plans concerned the introduction of a universal personal identifier (Personenkennzeichen, PKZ) as an element of a revised civil registry law in 1973. It was planned to assign a PKZ to every German citizen and all foreigners included in the Central Register of Foreigners with the intention to rationalise administrative processes. The project was finally abolished when the committee of legal affair of the German parliament decided in 1976 (on the basis of the micro census decision of the Constitutional Court) that "the introduction, deployment and use of a uniform system for numbering … is illegal".[66]

The other project was the "Federal Data Base" (Bundesdatenbank) started in 1972 with the similar goal to increase the efficiency of administration by linking hundreds of existing (public and private) data sources from government agencies and administrations. [67] In that respect, the project was similar to the system of "dragnet investigation" that was implemented in the fight against terrorism in the second half of the 1970s (see below). The plan for the "Federal Data Base", however, was abandoned mainly for financial and technical reasons.

2.3.3 Surveillance technologies and practices in the computer age

Apparently, the aforementioned developments offered enhanced surveillance possibilities. The capacities of information collection and storage enabled by databases and networks of databases became a widely used tool for administrative state control, the police, employers and private companies.

In the following sections, a couple of examples of new forms of surveillance are elaborated. Beginning with early forms of databases based on Hollerith machines in the 1930s, up to workplace surveillance enabled by the proliferation of personal computers in the 1980s, we present instances for new database- or computer-enabled surveillance within Europe and the US

2.3.3.1 National security state

Growing surveillance may be seen as a result of the development of the national security state, which also created a need for effective intelligence collection and data analysis.[68]

At least in part, the development drive for better missile guidance systems, early warning and espionage satellites and resilient communications that could survive nuclear attacks within US military research can be held responsible for the actual development of powerful technologies

[64] BVerfG 27;1, 1969.
[65] Mayer-Schönberger, Viktor, "Generational Development of Data Protection in Europe", *Technology and privacy: The new landscape*, Vol. 219-241, 1997, p. 221f.
[66] Opinion of the judiciary committee (Justizausschuss), Bundestagsdrucksache 7/1027, 05 May 1976.
[67] Hohn, Hans-Willy, *Kognitive Strukturen und Steuerungsprobleme der Forschung: Kernphysik und Informatik im Vergleich*, Campus, Frankfurt, 1998, pp. 270 ff.
[68] Bellizzi, Joseph A., and Terry Bristol, "An assessment of supermarket loyalty cards in one major US market", *Journal of Consumer Marketing*, Vol. 21, No. 2, 2008, pp. 144–154.

for surveillance, data collection and data mining.[69] After World War II, surveillance was significantly influenced by the ambitions of the countries that participated in the Cold War.

The computer shrank to a manageable size, increased in capacity and decreased in costs. All information gained through new surveillance technologies such as surveillance based on satellites or wireless bugging was easily storable. Hence, state led databases such as criminal records and policing or other myriad administrative activities emerged. Intelligence services augmented their capacities to monitor citizens through the use of information technology for the surveillance systems applied for national security.[70]

One of the classical approaches to surveillance is the eavesdropping of communications and interaction between citizens, originally over the telephone network, but more recently also over the Internet. One form of eavesdropping is often referred to as wiretapping. This is essentially to install a listening device in the path between two phones that are part of a conversation. Wiretapping can be set up on the subject's telephone, but also on the telephones of persons he or she is expected to contact. For policing purposes, installing a secret device is often unnecessary as they can simply get access to the data required via the network operators.[71]

One of the most notorious systems for eavesdropping is the ECHELON network, set up during the Cold War (as early as 1947) by the USA, UK, Canada, Australia and New Zealand. ECHELON's initial objective was the interception of communications in or to the Soviet Union and the Eastern Bloc. For more than 40 years, ECHELON (and the US National Security Agency, NSA, that was operating the network) was of utmost secrecy. While rumours about ECHELON had existed for more than a decade[72], the existence of the system was widely publicised when the European Parliament's STOA unit (Science and Technology Options Assessment) published a series of reports about the objectives, structures and methods of ECHELON.[73] STOA came to the conclusion that ECHELON used advanced techniques of pattern recognition to identify and extract messages of interest from the bulk of unwanted ones. Messages that had been identified in this way were then analysed manually. ECHELON was able to perform a virtually total surveillance of all types of electronic communications, thereby capturing information relevant for national security and any critical commercial intelligence that might affect national interests. That is worlds away from the popular conception of the old wiretap where a police agent listens to one line. Not only the volume of intercepts but also the potential for abuse are now exponentially higher.

The STOA report also concluded that the network was not as extensive as previously assumed, and after the report, some of the installation were closed. However, the network has

[69] Ibid.; Murakami Wood, "The `Surveillance Society': Questions of History, Place and Culture", 2009.
[70] Lyon, *The Electronic Eye: The Rise of Surveillance Society*, 1994.
[71] Campbell, Duncan, "Inside Echelon: The History, Structure, and Function of the Global Surveillance System Known as Echelon", in Thomas Y. Levin, Ursula Frohne and Peter Weibel (eds.), *CTRL [SPACE]: Rhetorics of Surveillance from Bentham to Big Brother*, MIT Press, Cambridge, MA, 2002, pp. 158-169.
[72] Wright, Steve, "The ECHELON Trail: An Illegal Vision", *Surveillance & Society*, Vol. 3, No. 2/3, 2005, pp. 198-215.
[73] European Parliament, STOA Unit (ed.), *Development of Surveillance Technology and Risk of Abuse of Economic Information* (5 volumes), Luxembourg, 1999; Schmid, Gerhard (rapporteur), "Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI))", A5-0264/2001, European Parliament, Temporary Committee on the ECHELON Interception System, Luxembourg, 2001.

never been officially shut down and its current relevance remains unclear since official information is still lacking accessibility."

Apart from ECHELON, governments perform an increasing amount of eavesdropping on electronic communications (as, for instance, the FBI with its controversial Carnivore program) using a much broader set of technological means.[74]

2.3.3.2 The US Social Security Number

Growing surveillance may be seen as a result of the development of the welfare state, which created a huge demand for data processing technologies to identify individuals.[75] The welfare state created the need to identify whom to deliver social services. We describe the example of the introduction of the US Social Security number in the paragraphs that follow.

In 1935, the American Congress passed the Social Security Act, which was implemented as a reaction to the Great Depression and as part of the creation of the modern welfare state. In order to facilitate the collection and distribution of the money from the Social Security Trust Fund, it became necessary to monitor the earnings of each employee. In order to be able to deal with the huge number of requests, the Social Security Board, which was responsible for the Social Security Trust Fund, assigned each worker a Social Security number (SSN). For each employee, a "summary-of-earnings" punch card was stored and punched with every year's earnings.[76]

After Congress changed the rules under which social security benefits were calculated, it was necessary to store additional information on those individual punch cards. Since the cards weren't big enough to deal with that amount of data, electronic data processing was introduced and in 1956, IBM's first generation of tube-based computers, the IBM 705, was installed.

In the following years, the domains in which the SSN became a prerequisite for diverse requests or operations increased steadily. In the US, the SSN started to serve as a "unique personal identifier".[77] Originally "disparate informational islands"[78] could accurately be mapped. Meanwhile, the SSN functions as an ID for a broad range of actors: state motor vehicle departments, social service agencies, the National Student Loan System, Department of Veteran Affairs, jury selection and taxpayer identification purposes are just a few of the entities requiring the SSN. In addition, private actors such as banks, credit-card companies, employers and health-care providers use the SSN for purposes of routine surveillance practices.[79] The SSN is one striking example of the development of a database which contains sensitive personal information and whose field of application has been expanded step by step over the years.

[74] Nabbali, Talitha, and Mark Perry, "Going for the throat: Carnivore in an Echelon World", *Computer Law & Security Report*, Vol. 19, No. 6, 2003, pp. 456-467, Vol. 20, No 2, 2004, pp. 84-97.
[75] Bellizzi and Bristol, 2008.
[76] Parenti, 2003.
[77] Ibid.
[78] Ibid.
[79] Garfinkel, 2000; Parenti, 2003.

2.3.3.3 Personal identification in Europe

In Europe, the picture is rather diverse when it comes to national regulation about personal identification numbers. In some countries, it is usual practice to assign a personal identification number to each citizen, e.g., in Denmark, where the so-called "CPR-number" is stored in the Civil Registration System. In other countries, such as Austria, personal identification numbers are officially forbidden, but nevertheless other personal numbers function as a de facto personal identification number.

In Germany, discussions about the wide-ranging recording of citizens are rather controversial. Though the personal identification number is unconstitutional (see above), several specific numbers do exist, such as a tax identification number and a social security number.

The roots of critical attitudes towards personal identification numbers can be traced back to the 1930s and the National Socialist regime. Back then, shortly after the Nazis took power in 1933, they redesigned the national census. IBM's German subsidiary Dehomag contracted with the government and was responsible for the census in 1933. Based on Hollerith machines, punch cards were used in order to collect more detailed information of the citizens, including name, birth name, address, gender, date of birth, religion, first language, ethnicity, profession and number of children. Jewish people had to give even more information in an additional count. The Hollerith machines allowed an easy sorting of people into categories related to the information available on the punch cards. Hence, racial politics, deportation and genocide under the National Socialist government were at least facilitated by Hollerith cards and the census in 1933.[80]

This historical experience from the Nazi regime as well as the more recent experience with the fight against terrorism in the 1970s were reasons why the German census that should have been conducted in April 1983 was so controversial. The census was planned as a complete inventory count of the population with an increased number of attributes to be collected. It raised serious concerns among wide groups of citizens who feared that it would lead to an Orwellian surveillance society. The protest finally led to the famous ruling of the German Constitutional Court that delayed the census until 1987, defined the fundamental right to informational self-determination and led to a revised data protection regulation in Germany that served as a blueprint for European regulations in the 1990s.[81]

2.3.3.4 Dragnet investigation

The case of the Federal Criminal Police Office (Bundeskriminalamt, BKA) and its infamous dragnet investigation techniques in Germany in the 1970s is a striking example of the rather

[80] van den Ende, Jan, "The Number Factory: Punched-Card Machines at the Dutch Central Bureau of Statistics", *IEEE Annals of the History of Computing*, Vol. 16, No. 3, 1994, pp. 15-24; Luebke, David Martin, and Sybil Milton, "Locating the Victim: An Overview of Census-Taking, Tabulation Technology, and Persecution in Nazi Germany", *IEEE Annals of the History of Computing*, Vol. 16, No. 3, 1994, pp. 25-39; Aly, Götz, Karl Heinz Roth, Edwin Black, et al., *The Nazi census: Identification and control in the Third Reich*, Temple University Press, Philadelphia, 2004; Heide, Lars, "Monitoring People: Dynamics and Hazards of Record Management in France, 1935-1944", *Technology and Culture*, Vol. 45, No. 1, 2004, pp. 80-101.

[81] BVerfGE 65;1, "Population Census", 15 December 1983. See Mayer-Schönberger, 1997, p. 229 ff; von Lewinski, Kai, "Zur Geschichte von Privatsphäre und Datenschutz - eine rechtshistorische Perspektive", in Schmidt, Jan-Hinrik, and Thilo Weichert (eds.), *Datenschutz: Grundlagen, Entwicklungen und Kontroversen*, Bundeszentrale für politische Bildung, Bonn, 2012, pp. 23-33.

diverse, sometimes even contradictory motives to introduce surveillance systems for internal security and for the often rather limited and even unexpected impacts of these systems.

Though computerisation and dragnet investigation are normally associated with the fight against left-wing terrorism, their original goals were quite different. When Horst Herold became president of the BKA in 1971, he had strong views about the role that computer should play for policing. He complained that the police were making too little use of the vast amount of data that they had already collected. Using technocratic vocabulary, he stated that through the use of computer, the BKA should become the information and communication centre of the German police.[82] Instead of just reactively keeping information from normal police investigations, he wanted to expand this to an active collection of all kinds of data (about family, housing, property, social situation, etc.) and to make use of it to conduct research about the structures and causes of criminality.[83]

This should then be used as the basis for more preventive police work. In that respect, the collection and processing of crime-related data was seen as a way of social engineering, addressing the concerns of a growing fraction of the German population.[84] Moreover, technisation was regarded as a way to make the consideration of evidence before court more transparent and objective. That way, mass collection of policing data should support the democratisation of the judicial system because it enabled "everyone to know everything".[85]

As a result of these plans, the BKA set up various large-scale databases and integrated other governmental and non-governmental databases into their INPOL system.[86] BKA's own databases not only included information about convicted criminals and arrested people, but also increasingly information gained through observational investigation of presumed or potential offenders.[87]

The situation changed significantly with the increasing number of terrorist attacks by the Red Army Faction (RAF) culminating in the so-called "German autumn" in 1977. The BKA now made use of the system they had introduced some years before and turned it into an instrument for investigation. By 1979, the BKA had registered the names of 4.7 million persons and several hundred organisations, fingerprints of 2.1 million suspects and photos of 1.9 million persons. A specialised database included dossiers of more than 3,500 suspicious subjects with even more detailed information.[88]

The most famous technique used by BKA is known as the (negative) dragnet investigation and addressed the problem that a lack of character traits was typical for RAF terrorists and their behaviour. They were disguised as petty bourgeois and their wives, drove average cars and lived in conspiratorial flats whose normality was difficult to characterise. [89]

---

[82] "Kommissar Computer", *Der Spiegel*, 27/1971, pp. 53.
[83] Guggerli, David, *Suchmaschinen: Die Welt als Datenbank*, Suhrkamp, Frankfurt am Main, 2009, p. 54.
[84] Ibid., p. 53.
[85] Ibid., pp. 58-60.
[86] INPOL stands for "Information System of the Police". It made use of data of social insurance, motor vehicle registration offices, energy suppliers, banks, etc. See Bölsche, Jochen, Der Weg in den Überwachungsstaat, Rowohlt, Reinbek bei Hamburg, 1979.
[87] Lindner, Rudolf, Bertram Wohak and Holger Zeltwanger, *Planen, Entscheiden, Herrschen: Vom Rechnen zur elektronischen Datenverarbeitung*, Rowohlt, Reinbek bei Hamburg, 1984, p. 198 f. This became particularly critical when BKA started to collect information about sympathizers and potential sympathizers of the RAF.
[88] Guggerli, 2009, p. 56.
[89] Ibid., p. 63.

To identify these men and women without properties, the BKA developed a technique that aimed not at putting meaningful mosaic stones together to find the deviancies. Instead, it sorted out all persons from the entire population that did not fit in the search grid. In the particular case, the assumptions were rather simple: terrorists and their cars are not officially registered, they paid their rent and electricity bill in cash and do not receive a child allowance.[90] All persons that did not match this rather abstract profile were deleted from the database. The remaining sediment had then to be meaningful, since all meaningless data sets had already been removed.[91]

The massive data collection and dragnet investigations had significant effects, though not the intended ones. Though dragnet investigation was certainly a sophisticated technique,only one suspect was caught as result of dragnet investigation in Germany since the 1970s.[92] On the other hand, the promises of using computer for crime prevention or even social engineering lost its appeal over the years. Citizens became increasingly disenchanted about the promises of "cybernetic" policing and technocratic societal approaches in general. [93] Even worse: instead of searching for the patterns and causes of criminality, the "search engine" had become a repressive instrument for manhunts.[94] It even inverted the principle of presumed innocent: everyone was regarded as a possible offender and those who remain stuck in the dragnet are even considered as suspects.

2.3.3.5 The targeted consumer

Not only the state, but also private actors benefitted from the new possibilities offered by new technologies. New ways of identifying, tracking and attempting to channel the consumption activities of individuals began to be explored. An era of direct marketing evolved, postal zip-codes were combined with census data, credit card service bureaus started to sell data to direct mailers, reports including banks, Social Security numbers, names, addresses, and credit card histories were established and ready to be sold.[95] Targeted telephone calls or junk mails had become a daily commercial routine.

One prominent area of surveillance for marketing purposes (and for security purposes, as discussed in a later chapter) is airports. Personal data of passengers was collected with increasing intensity from the beginning of the existence of searchable databases. The first computerised ticketing systems had been developed and introduced in the 1980s and raised highly competitive stakes by allowing the collection and analysis of patterns of travelling.[96] In

[90] Ibid., p. 64.
[91] Ibid., p. 63.
[92] After the 9/11 terror attacks, a new wave of dragnet investigations was started in Germany to identify possible sleepers. Despite the technical progress made in pattern recognition since the 1970s, the results were rather poor. The investigation resulted mainly in a list of all male students of Islamic faith. See Schulzki-Haddouti, Christiane, "Sicherheit im Netz und digitale Bürgerrechte", *Aus Politik und Zeitgeschichte*, B49-50/2003, pp. 13-19. In 2006, the German Constitutional Court finally decided that dragnet investigations are only allowed in the case of an actual threat to national security or to the lives of citizens. See BVerfGE 115;320, "Dragnet Investigation II", 4 April 2006.
[93] Enzensberger, Hans Magnus, "Der Sonnenstaat des Doktor Herold", *Der Spiegel* 25/1979, pp. 68-78.
[94] Guggerli, 2009, p. 68.
[95] Lyon, *The Electronic Eye: The Rise of Surveillance Society*, 1994.
[96] Lyon, David, "Airports as data filters: Converging surveillance systems after September 11th", *Journal of Information, Communication and Ethics in Society*, Vol. 1, No. 1, 2003, pp. 13-20.

general, two developments within the 1960s may be cited as salient drivers of the intensification of profiling activities in relation to airplane passengers:[97]

First, the commercial aviation industry expanded greatly with the construction of a variety of airplanes applicable for different ranges of flights and different numbers of passengers. As a consequence, the number of passengers transported and the places to which the airlines were flying increased. The newly developed Boeing 707, the first jet engine driven airplane for long-range use, revolutionised civil aviation. A second development was the hijacking of airplanes. In the 1960s, the number of hijackings increased drastically, often with the purpose of escaping from national political repression or of political blackmail.

Until the 1960s, the typical passengers of civil aviation were largely business people, but with economic growth and the growth of the airplane industry, that stereotype was no longer appropriate, and the passenger became the target of marketing activities. Air transportation became less costly and international, and consumer mobility aroused marketers' interest. The roots of contemporary surveillance activities based on consumer tracking and loyalty cards can be found in the tracking of citizens' travel behaviour.

Consumer loyalty had already been encouraged before databases were widely available; nevertheless, with the arrival of cheaper means of collecting and storing consumer purchase histories, loyalty programs grew in popularity. Consumers were offered incentives such as reduced prices in return for the supply of personal information and allowing the scan of all purchases.[98]

Another example in terms of consumer surveillance is the case of credit cards, whose origins can be traced back to the 1950s. The proliferation of credit cards in combination with the increased use of computers facilitated the tracking of consumers and analysis of information trails from the 1970s onwards.[99] Sophisticated networks of interconnected databases allowed almost instant background checks about a citizen. Magnetic–strip cards were invented and new automated teller machines were installed and increased the collection and processing of customer data that not only enabled an analysis of shopping behaviour but also the creation of profiles.

2.3.3.6 Workplace surveillance

With the proliferation of information technologies and computers within the context of work and workplace, some literature dealing with workplace surveillance appeared. Among the prominent books on the subject were Barbara Garson's *The Electronic Sweatshop* (1988)[100], Robert Howard's *Brave New Workplace* (1985)[101] and Shoshana Zuboff's *In the Age of the Smart Machine* (1988).[102] The topic of workplace surveillance had become a salient one during the 1980s. Yet we can ask if new technologies indeed changed surveillance practices.

---

[97] Curry, Michael R., "The Profiler's Question and the Treacherous Traveller: Narratives of Belonging in Commercial Aviation", *Surveillance & Society*, Vol. 1, No. 4, 2004, pp. 475-499.
[98] Bellizzi and Bristol, 2008.
[99] Parenti, 2003.
[100] Garson, Barbara, *The electronic sweatshop: How computers are transforming the office of the future into the factory of the past*, Simon & Schuster, New York, 1988.
[101] Howard, Robert, *Brave new workplace*, Viking, New York, 1985.
[102] Zuboff, Shoshana, *In the age of the smart machine: The future of work and power*, Basic Books, New York, 1988.

In order to approach this, it is worth making a short side trip into the roots of workplace surveillance.

Workplace surveillance was not a new phenomenon that evolved in the 1980s: it existed to some degree in earlier times as well. In his book *Scientific Management*, F.W. Taylor developed the idea of separating knowledge and planning of work from its manual execution, i.e., new techniques for the standardisation of products may be introduced, the principle of cost reduction is followed, planning is centralised, hierarchical authority prevails and organisation is rigid.[103] Ford's assembly line is the perfect exemplification of Taylorism; certainty was ensured through surveillance and production was predictable. The increased structuring and time-dependence of the workplace offered the possibility to implement new patterns of control and surveillance in the post-industrialist organisation of work.

But, as Lyon argues, Fordism failed and wasn't able to cope with specialised and volatile demands. In post-Fordism times, which are characterised by, for example, demand-driven production, the decentralised organisation of work demands an increased intensity of work monitoring. In order to name this development, Lyon coined the term "disorganised surveillance". For him, the need to know where in a production process a product is all the time offers, as a result, the opportunity for the surveillance of the individual worker.[104] Similarly, Rule puts it as follows: "Computerisation creates certain new *occasions* for the monitoring of work.... By making more accessible and accountable to management the movement of *things*, and the activities associated with those things, computing opens the *people* implicated in these processes to closer scrutiny."[105] Rule came to those conclusions as a result of a study he conducted dealing with computerised firms in greater New York. He furthermore discovered that computers bring information together that would otherwise exist but wouldn't be available to management in a usable way.

By the end of the 20th century, electronic surveillance in the workplace had become more extensive and intensive than ever before.[106] Besides the monitoring of the work, the individual worker is scrutinised as well, often without even being able to detect the "watching".[107] This holds in terms of pre-employment screening as well as for the actual electronic monitoring of the work or the workplace itself. Pre-employment screening may include police records or disease checks.[108]

Actual forms of work monitoring include the following: Keystroke counting is one obvious example of automated supervision; further practices include data security systems, telephone call accounting, entry and exit controls using smart cards, active badges and location technologies that enable employers remotely to check on mobile workers,[109] reading of electronic mail and the use of video cameras for visual surveillance.[110] In general, workplace monitoring, e.g., cyclometers for counting keystrokes on typewriters or the monitoring of telephone operators, was also prevalent before computers were invented, but possibilities

[103] Lyon, *The Electronic Eye: The Rise of Surveillance Society*, 1994.
[104] Ibid.
[105] Rule, James B., "High-Tech Workplace Surveillance: What's Really New?", in David Lyon and Elia Zureik (eds.), *Computers, Surveillance, and Privacy*, University of Minnesota Press, Minneapolis, 1996, pp. 66-76.
[106] Lyon, *The Electronic Eye: The Rise of Surveillance Society*, 1994.
[107] Bryant, Susan, "Electronic Surveillance in the Workplace", *Canadian Journal of Communication*, Vol. 20, No. 4, 1995.
[108] Lyon, *Surveillance Studies: An Overview*, 2007.
[109] Ibid.
[110] Lyon, *The Electronic Eye: The Rise of Surveillance Society*, 1994; Bryant, 1995.

increased immensely due to the new capabilities offered by the spread of personal computers.[111] The monitoring of employees became rampant, especially in working environments which were fully digitised (e.g., call centres).

2.3.4 Qualitative and quantitative shifts in surveillance practices

The late 1980s and 1990s marked years of transition for the ways in which surveillance was done. The facilitation of information storing and processing enabled by computer technologies, first mainframes, later personal computers, allowed refined tracking and surveillance of individuals. The advancement of computer and telecommunication technologies which emerged in the 1980s allowed historically new possibilities of linking information about an individual. Sophisticated personal profiles could be constructed by using computer-matching or record-linking technologies.[112] Establishing networks of databases offered a new quality of surveillance.

In his work *Private Lives and Public Surveillance*, James Rule highlighted the difference between the "ordinary world", where people directly impinge on experience, and the "paper world", where facts of individual lives are documented in order to verify, sanction and substantiate the "ordinary world".[113] This may have been true for the pre-computer age, but after the rise of the computer in the 1980s and 1990s, the world of experience was no longer contrasted with the paper world, but with digital worlds.[114] Or as Mark Poster put it, databases constitute some kind of extra self, which lives a life on its own beyond the "real self".[115]

With the rise of the computer age, the possibilities to store and process data improved massively. As a result, surveillance possibilities changed in quantitative terms. A qualitative transformation in the political uses of collected data occurred as well.[116] The computer revolution triggered the ubiquity, decentralisation, anonymity and self-reinforcement of surveillance.

As early as 1988, Roger E. Clarke coined the term "dataveillance", which represents the new surveillance potentials and possibilities, which had been coming with the proliferation of computers. It is no longer the centrality of data storage that raises fears about surveillance practices (as it was with the National Database in the US). Rather, as prerequisites for an extensive digital surveillance, the following three conditions became crucial:[117] (1) the existence of databases that can store and search previously unwieldy amounts of information, (2) the existence of a network or networks of databases that allow the linkage of disparate, unrelated files into technologically and politically coherent systems, and (3) universal personal identifiers or "tags" that allow consistent and unique identification of data or rather specific individuals within large populations.

---

[111] Petersen, Julie K., *Understanding surveillance technologies: Spy devices, privacy, history and applications*, Auerbach Publications, Boca Raton, 2007.
[112] Lyon, *The Electronic Eye: The Rise of Surveillance Society*, 1994.
[113] Rule, James B., *Private Lives and Public Surveillance*, Allen Lane, London, 1973.
[114] Lyon, *The Electronic Eye: The Rise of Surveillance Society*, 1994.
[115] Poster, Mark, *The mode of information: Poststructuralism and social context*, University of Chicago Press, Chicago, 1990.
[116] Parenti, 2003.
[117] Clarke, Roger, "Information Technology and Dataveillance", *Communications of the ACM*, Vol. 31, No. 5, 1988, pp. 498-512; Parenti, 2003.

Clarke lists the following aspects as being relevant components of IT development in the 1980s:[118]

- Magnetic data-storage capabilities had improved immensely between 1965 and 1985.
- A rich assortment of input and output technologies had been developed to support the capture and dissemination of data.
- The management of image and voice data improved, and integrated data management, and conversion between the various forms are addressed.
- Complex deterministic problems could be tackled; progress had been made in modelling probabilistic and stochastic processes.
- Improvements in telecommunications had been made and did continue in relation to speed, cost, reliability, robustness, security and standardisation.

The relationship between information technologies and increasing surveillance capacity can be illustrated by four criteria that had been specified by James Rule[119]: He argued that surveillance systems are limited in terms of the following four factors:

- the size of files held in the system,
- the degree to which they are centralised,
- the speed of flow between points in the systems and
- the number of contact points between the system and the subject.

The 1990s saw two other technological trends that facilitated the processing and exchange of collected data. First, computers became increasingly connected through wide area networks that finally merged into the global Internet after 1992. As a result, the amount of information transmitted electronically increased by magnitudes within a few years. Second, the digitisation of communication networks made it possible to transmit voice signals as well as digital data over the same cables and satellite links. Telecommunications even adopted the protocols developed for data communication (for instance, Voice over Internet Protocol, VoIP). This convergence enabled surveillants to computerise their ways to collect and especially to process and analyse data using ever more powerful computers. [120]

With the proliferation of information technologies during the 1990s, expansion along all four dimensions had been facilitated.[121] First, the size of files has grown in a much more fine-grained and discriminating manner. Second, although centralisation did not increase extensively, increased network capabilities furthered the diversity and facilitated the tracing of individuals. Third, enhanced information and telecommunication systems increased the speed of information flows and flexibility of reactions to altered circumstances. Fourth, the increased diversity of surveillance sites augmented subject transparency.[122]

2.4 THE RISE OF SURVEILLANCE CAMERAS

Video surveillance, or closed circuit television (CCTV), cameras and systems are arguably the most visual and prominent manifestation of contemporary surveillance societies, and from the 1990s onwards, such systems have been introduced into a wide range of social settings and countries. These systems vary in their technological configuration and the ways in which they

[118] Clarke, 1988.
[119] Rule, *Private Lives and Public Surveillance*, 1973.
[120] Solymar, Laszlo, *Getting the Message: A History of Communications*, Oxford University Press, Oxford, 1999, Chapter 16.
[121] Lyon, *The Electronic Eye: The Rise of Surveillance Society*, 1994, Chapter 16.
[122] Ibid.

are used, although typically they are seen to be a key tool in the fight against crime (at least, some forms of crime; they have been less used and successful in capturing corporate malfeasance in the banking industry, for example). There is also a general perception that the United Kingdom has been at the forefront of the development of this technology and that the diffusion of CCTV in the UK has been copied around the world. In the following paragraphs, we examine definitional difficulties, the diffusion of video surveillance cameras in the UK and beyond, and the main reasons for the rise of surveillance cameras in the 1990s onwards. Specific reference is made to the UK situation, as the UK is perceived to be the world leader in the deployment and use of these systems.

2.4.1 Definitional difficulties

Although the presence of video surveillance cameras in public places is a common occurrence throughout Europe, these systems differ in a number of respects, making a precise definition very difficult.[123] In the UK, the term CCTV is used to refer to these systems, whilst in Europe the term "video surveillance" is more common.[124] CCTV is terminologically problematic because it captures very little of the essence of these systems. In a technological sense, they are rarely closed, in that they often use the public telecommunications network, and because "television" is only one of the technological components required to make a system work, other key components include cameras, monitors, transmission and recording equipment, and CCTV control centres and practices.[125] So, although the term CCTV has common currency, in the UK and beyond, it is not a very accurate term. Also, when we break down the technological components of a system in this way, we find that very few systems are alike in terms of their technological capability, such as the power of the camera lens and the quality of images captured.[126]

Another definitional problem relates to the location and operation of these systems. Although the cameras with which we are familiar are located in places to which the public has access, this does not mean that they are all public systems or that they are operated by public agencies.

Typically, systems located in public streets are owned and operated by public agencies, but there are a large number of cameras and systems in other locations to which the public has access, including in shops, shopping centres, sports arenas, transport facilities, airports, car parks, petrol stations, museums and a large number of private locations, including offices and residential properties.[127] Technological developments have also allowed for the installation of CCTV on buses,[128] and trains,[129] in taxis,[130] and on the uniforms of police officers[131] and traffic wardens.[132] The location and ownership of a surveillance camera is significant because

[123] Webster, C. William R., "CCTV Policy in the UK: Reconsidering the Evidence Base", *Surveillance & Society*, Vol. 6, No. 1, 2009, pp. 10-22; Webster, C. William R., "Smart CCTV", Paper presented at: 5th Conference on Computers, Privacy and Data Protection (CPDP), Brussel, 25-27 January 2012.
[124] Webster, C. William R., Eric Töpfer, Francisco R. Klauser, et al. (eds.), *Video Surveillance Practices and Policies in Europe*, IOS Press, Amsterdam, 2012.
[125] Gill, Martin (ed.), *CCTV*, Perpetuity Press, Leicester, 2003.
[126] Webster, "Smart CCTV", 2012.
[127] Webster, C. William R., "The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK", *Surveillance & Society*, Vol. 2, No. 2/3, 2004, pp. 230-250.
[128] BBC News, "Boy's eyes gouged in Birmingham bus attack", 25 Sept 2012.
[129] BBC News, "Man in dress exposes himself on Lincoln-Grimsby train", 19 Oct 2012.
[130] BBC News, "Southampton City Council appeals to keep taxi cameras", 16 Aug 2012.
[131] BBC News, "PSNI urged to wear body cameras to tackle domestic abuse", 18 Oct 2012.
[132] BBC News, "Swansea traffic wardens to wear cameras to record abuse", 22 Sept 2012.

in different countries, different regulations, in terms of legal instruments, apply to different settings and consequently shape the way cameras and images are used.[133] For example, in the UK public agencies can be expected to adhere to the Information Commissioner's Office's "CCTV Code of Practice",[134] whereas private companies and individuals are only bound by the Data Protection Act 1998,[135] and other non-specific legislation, which means that they have a degree of flexibility in how they install and operate systems. The location and operation of systems is also an important factor when trying to count the numbers of cameras and systems. So, whilst surveillance cameras have proliferated, the terms "CCTV" and "video surveillance cameras" are usually understood to be those systems in operation in public places and by public agencies or those operating on behalf of public agencies – and they represent only a small fraction of the cameras installed since the 1990s.

A further definitional issue relates to the purpose of systems.[136] Typically, systems are recognised as a tool in the "fight against crime and disorder" and much of the work undertaken by criminologists seeks to understand CCTV as a crime-fighting tool.[137] However, the deployment of these systems is usually part of a broader strategy and is integrated alongside other measures and activities. For example, the introduction of CCTV may be part of a commercial strategy for a new shopping centre, it may be intended to reduce the fear of crime (as opposed to actual crime), it can be used to deploy police resource, generate evidence for the justice system or gather intelligence for the police of security operations. It may also be introduced alongside other measures, such as improved street lighting, contact points or increased police patrols. Also, in terms of a narrow crime perspective, it is evident in the UK that the use of CCTV has evolved from being associated with combating crime to systems designed to reduce the fear of crime, deter anti-social and undesirable behaviour, and encourage community safety.[138]

To complicate matters further, the computerisation of CCTV systems has meant that they are able to count cars, people and other objects and make subjective assessments about behaviour, based on computer algorithms and the profiling of past behaviours.

From this discussion it is clear that video surveillance cameras and systems differ in the way they are configured and used. Typically most schemes can broadly be categorised into four types of system, those that are proactive, reactive, non-active and interactive ("smart")[139], and that the type of system and its technological capabilities determine the levels of monitoring and the intensity of surveillance that can take place, with the key differences between each of these types being explained in Table 1.[140] This typology is a hierarchy of sophistication. The least sophisticated 'systems' are non-active systems that act as a visual deterrent through the physical presence of passive cameras. They are non-active because there is no monitoring or recording capability. Instead they create the illusion of surveillance because citizens feel like they are being watched when actually they are not. The reactive type links cameras to

[133] Gras, Marianne L., "The Politics of CCTV in Europe and Beyond, The Legal Regulation of CCTV in Europe", *Surveillance & Society*, Vol. 2, No. 2/3, 2004, pp. 216-229.
[134] Information Commissioner's Office, "CCTV Code of Practice, Revised edition", Wilmslow, 2008.
[135] "Data Protection Act", 1998.
[136] Webster, "CCTV Policy in the UK: Reconsidering the Evidence Base", 2009.
[137] Norris, Clive, "The success of failure, Accounting for the global growth of CCTV", in Ball, Kirstie, et al. (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, London, 2012, pp. 251-258.
[138] Webster, "CCTV Policy in the UK: Reconsidering the Evidence Base", 2009.
[139] Ibid.; Wright, David, Michael Friedewald, Serge Gutwirth, et al., "Sorting out smart surveillance", Computer Law and Security Review, Vol. 26, No. 4, 2010, pp. 343-354.
[140] Webster, "CCTV Policy in the UK: Reconsidering the Evidence Base", 2009.

recording, storage and playback facilities allowing access to footage after an event or incident has occurred. With this type there is no live surveillance but they are seen as particularly useful for identifying the perpetrators of criminal acts and in providing evidence for prosecutions. The most sophisticated type of CCTV system include an integrated dedicated surveillance and communications control centre staffed by dedicated local authority or police operatives with direct communications links with the local police force, thereby allowing for real-time continuous surveillance.[141] More recently, developments in networking, data matching, such as face recognition) and computer algorithms and profiling has led to the development of 'smart' CCTV systems in which the systems themselves decide what to surveil and when to alert an operative to an incident of interest.[142]
So, whilst surveillance cameras may at the outset seem similar, the divergent ways they are configured and used result in different types of surveillance practices and relationships and mean that it is almost impossible for the surveilled to know when they are being surveilled or what happens to the images and data collected by surveillance cameras and systems.

Type	Features
Interactive or smart	Computerisation of CCTV processes so that live surveillance is also determined by computer-based algorithms and profiles.
Proactive	Live surveillance from a dedicated control room with recording, storage and playback facilities. Allows for an immediate response to incidents as they occur.
Reactive	Recording, storage and playback facilities. Provides access to footage of incidents after the event has occurred.
Non-active	No monitoring, storage or playback facilities. Acts as a visual deterrent by using fake 'cameras' to create the illusion of surveillance.

Table 1: A typology of CCTV systems
Source: Webster, 2009

2.4.2 The proliferation of surveillance cameras since the 1990s

Although surveillance cameras differ considerably in their technological configuration and use, there is widespread agreement that these systems diffused rapidly and widely from the 1990s onwards.[143] Surveillance cameras are now a normal feature of modern society and are firmly embedded in the consciousness of contemporary populations.[144] At the policy level, surveillance camera systems are also a key policy area and are integrated into national and community safety strategies.[145] In terms of systems operating in public places, and taking into account the definitional issues raised above, CCTV can be found in town and city centres, car parks, bus and rail stations, airports and ports, museums, libraries, sport centres and arenas, parks, schools, hospitals and in residential areas. Surveillance cameras are also found in buses, trains and taxis, in lifts, at reception desks, and on the person of a variety of private and

[141] Webster, "The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK", 2004.
[142] Wright, et al., "Sorting out smart surveillance", 2010; Webster, "Smart CCTV", 2012.
[143] Webster, "The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK", 2004; Webster, "CCTV Policy in the UK: Reconsidering the Evidence Base", 2009.
[144] Murakami Wood and Webster, "Living in Surveillance Societies: The normalisation of surveillance in Europe and the threat of Britain's bad example", 2009.
[145] Webster, "CCTV Policy in the UK: Reconsidering the Evidence Base", 2009.

public sector employees, e.g., police officers and traffic wardens.[146] There is also a range of private locations to which the public have easy access and where video cameras are prevalent, for example, in shops, petrol stations, shopping centres, banks, restaurants, office blocks and gated residential communities. What has been remarkable about the surveillance camera revolution is not just the speed of uptake, but also the wide variety of locations where cameras are used.[147]

The UK is regularly heralded to be at the forefront of the surveillance camera revolution and the widespread proliferation of CCTV in public places in the UK in the 1990s has been copied around the world.[148] It is widely accepted that in the 1990s the UK experienced the greatest expansion and diffusion of public space CCTV systems in Europe,[149] and there are a number of reasons for this expansion.

Norris et al. document the development of CCTV in the UK, starting with police forces in the 1950s using CCTV to assist with traffic control and in the 1960s for monitoring crowds; how the retail sector deployed CCTV for anti-theft purposes in the 1960s; in the 1970s and 1980s, CCTV was deployed in a fairly limited capacity in the London Underground rail system for security purposes, and by the police for monitoring football crowds and political demonstrations.[150] In 1985, the first large-scale public space CCTV system was installed in Bournemouth, which had been the venue the previous year for the Conservative Party conference where the IRA had tried to assassinate the Prime Minister by detonating a bomb in the conference hotel. By 1991, there were "no more than ten" cities in the UK with open street systems.[151] By the mid-1990s, the Home Secretary launched the "City Challenge Competition" which resulted in funding for 106 new CCTV schemes in towns and cities across the UK.[152] Further funding from central government for the installation and operation of CCTV schemes was made available throughout the late 1990s and early 2000s. Whilst the expansion of public space CCTV systems is well recognised, there is some dispute about the number of cameras installed. Part of the problem in trying to estimate the number of CCTV cameras in the UK may be the definitional issues discussed above and may depend on whether or not you are counting all CCTV cameras or just those operating in public places, or even just those operating in public places on behalf of public agencies. McCahill and Norris "guestimated" on the basis of a survey in one London Borough that there may be as many as

[146] "Swansea traffic wardens to wear cameras to record abuse", 2012; Norris, 2012; Smith, Gavin J.D., "Surveillance work(ers)", in Ball, Kirstie, et al. (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, London, 2012, pp. 107-115.

[147] 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, "The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK", 2004.

[148] Webster, et al. (eds.), *Video Surveillance Practices and Policies in Europe*, 2012.

[149] Fyfe, Nicholas, R. and Jon Bannister, "City watching: closed circuit television in public spaces", *Area*, Vol. 28, No. 1, 1996, pp. 37-46; Webster, "Closed circuit television and governance: The eve of a surveillance age", 1996; Norris, Clive, Mike McCahill and David Wood, "The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space", *Surveillance & Society*, Vol. 2, No. 2/3, 2004, pp. 110-135.

[150] Norris, et al., "The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space", 2004.

[151] Ibid.

[152] Webster, "Closed circuit television and governance: The eve of a surveillance age", 1996; Webster, "The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK", 2004; Norris, "The success of failure, Accounting for the global growth of CCTV", 2012.

4.2 million cameras in the UK, which equated then to 1 for every 14 citizens.[153] However, more robust research points to far fewer surveillance cameras and systems.

For example, Webster's national survey of public space systems operated by local authorities in 1999[154] found just 1,300 systems and approximately 21,000 cameras, whilst research undertaken for the Scottish Government in 2007/2008, found that just over 2,200 public space cameras existed in Scotland and that one local authority area did not have any public space systems.[155]

There are a number of interrelated factors that account for the rapid diffusion of CCTV in the UK in the 1990s.

First, and as previously mentioned, considerable funds were made available by central government to cover the capital costs associated with the installation of new systems. The provision of resources in this way was critical because it was local government and not central government that installed and operated new systems. By, "ring fencing" resources for CCTV, central government was able to influence and shape the delivery of CCTV by local government.[156]

Second was the overwhelming levels of political support for CCTV cameras and systems. Politicians in the UK perceived a need to demonstrate that they were "doing something" in the fight against crime and investment in a technology, despite being unproven, was a clear signal that they were committed to addressing the electorate's concerns about crime and disorder. Political rhetoric in favour of CCTV was critical in securing public support and politicians regularly argued that "if you have got nothing to hide, then you have nothing to fear".[157]

A third factor was central government support for CCTV in the form of operational guidance, advice on the technical requirements of systems, anecdotal evidence of success and the processes required in order to secure public support for systems.[158] In this respect, central government played a central role in disseminating knowledge about CCTV and in initiating policy networks. As Webster notes, central government "remains the dominant actor in policy-making and service delivery, through its ability to govern and shape networks".[159]

---

[153] McCahill, Mike, and Clive Norris, "Estimating the Extent, Sophistication and Legality of CCTV in London", in Martin Gill (ed.), *CCTV*, Perpetuity Press, Leicester, 2003, pp. 51-66.

[154] Webster, C. William R., "Cyber society or surveillance society? Findings from a national survey on closed circuit television in the UK", in John Armitage and Joanne Roberts (eds.), *Exploring Cyber Society: Social, Political and Cultural Issues*, Proceedings of the Conference, Volume 2, University of Northumbria, Newcastle UK, 1999; Webster, C. William R., "The Policy Process and Governance in the Information Age: The Case of Closed Circuit Television", Unpublished PhD Thesis, Caledonian University, Glasgow, 2004.

[155] Bannister, Jon , Simon Mackenzie and Paul Norris, "Space CCTV in Scotland: Results of a National Survey of Scotland's Local Authorities", Public Report 03/09, *The Scottish Centre for Crime and Justice Research*, Glasgow, 2009.

[156] Webster, "The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK", 2004; Webster, "CCTV Policy in the UK: Reconsidering the Evidence Base", 2009.

[157] Norris, Clive, and Gary Armstrong, *The Maximum Surveillance Society: The Rise of CCTV*, Berg Publishers, Oxford, 1999; Fussey, Pete, "New Labour and New Surveillance: Theoretical and Political Ramifications of CCTV Implementation in the UK", *Surveillance & Society*, Vol. 2, No. 2/3, 2004, pp. 251-269; Webster, "The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK", 2004.

[158] Webster, "The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK", 2004.

[159] Ibid., p. 247.

A fourth factor relevant to the diffusion of CCTV in the 1990s was the way in which CCTV entered the general consciousness of the population. It has been argued that the tragic death of toddler Jamie Bulger in 1993 was the critical event which led a whole nation to be aware of the potential and relevance of CCTV.[160] This was because the CCTV cameras in the shopping centre where Jamie was abducted captured the event, with this footage being subsequently broadcast to the nation. Whilst these images are ingrained in the memory of UK citizens the usefulness of CCTV was also demonstrated through TV programmes such as "Police Camera Action"[161] and other "reality" based TV programmes. In this way, our understanding of CCTV, as a useful tool to combat crime, was shaped in a positive way in a period when the provision of CCTV could have been contested.[162] Such TV programmes also normalised a society to the presence and need for CCTV.[163]

A fifth factor shaping the provision of CCTV in the 1990s was the technological and security companies looking for new domestic markets for products which had initially been designed for military and security purposes.[164] This point demonstrates another set of vested interests with a stake in the successful diffusion of CCTV.

The combination of these factors led to a situation in the 1990s where the policy environment and society were malleable to the provision of CCTV. This was despite concerns being raised about civil liberties and the costs of running systems.[165] In this respect, the rapid diffusion of CCTV in the UK in the 1990s can best be understood as a process in which a range of vested interests were satisfied by the provision of CCTV and that a range of factors aligned in order for this to happen.

Although the diffusion of CCTV in the UK is a well recognised phenomenon, there have been subtle changes in the nature of this diffusion as the technology has developed and the policy environment matured. Webster refers to three eras of diffusion as eras of (1) innovation and experimentation, (2) acceptance and expansion and (3) retrenchment, during which policy networks and the technology become more sophisticated.[166] A key change in this period is the core focus or purpose of the cameras. Initially, they were seen as a tool in the fight against crime and disorder and their success was measured in relation to crime statistics. However, as CCTV schemes migrated from the police to local authorities, in order to avert claims of a police state, their purpose evolved into being more concerned with community safety, the fear of crime and anti-social and undesirable behaviour. This may have been because the local authorities in the UK have a broader remit for community safety or because the robust emerging academic analysis of CCTV questioned whether it was really effective in reducing crime.[167]

---

[160] Norris, "The success of failure, Accounting for the global growth of CCTV", 2012, p. 252.
[161] Police Camera Action, Documentary Television Series, Carlton Television for ITV, 1994-
[162] Webster, "The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK", 2004.
[163] Murakami Wood and Webster, "Living in Surveillance Societies: The normalisation of surveillance in Europe and the threat of Britain's bad example", 2009.
[164] Lyon, Surveillance Studies: An Overview, 2007.
[165] Webster, "The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK", 2004.
[166] Ibid., p. 238
[167] 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; Welsh, Brandon C., and David P. Farrington, *Crime prevention effects of closed circuit television: A systematic review*, Home Office Research Study, Home Office, London, 2002; Norris, "The success of failure, Accounting for the global growth of CCTV", 2012, pp. 254 f.

More recently, the focus of CCTV has evolved further and now includes a role in national security, especially in relation to the threat of terrorism.[168]

The introduction of CCTV in the UK has, despite general political, policy and public support, raised a number of concerns. On the whole, these have been accommodated by a policy process which has been shaped by vested interests to accommodate the diffusion of CCTV.[169] Nevertheless many issues raised during the 1990s are still relevant today. The main concerns are whether CCTV has a negative impact on civil liberties,[170] works as a crime reduction tool,[171] is too expensive to install maintain and operate,[172] changes the nature of relations in society, particularly the state-citizen relationship,[173] is ineffective as a tool for national security and anti-terrorism,[174] meets the evidence requirements of the criminal justice system,[175] operators are effective,[176] and whether or not there is a healthy level of discourse and understanding amongst the general population.[177] In sum, it is apparent, that despite a history of operating CCTV in public places for more than 20 years, the implications and consequences of these systems are still poorly understood.

2.4.3 Video surveillance cameras in Europe

Beyond the UK, other countries have not been immune to the surveillance camera revolution, although the diffusion of cameras may not have been so rapid elsewhere. The Urbaneye project found that there had also been a relatively rapid expansion of surveillance cameras in urban areas across Europe, both in terms of public and private space, and that this had occurred largely independently of the general political conditions: "Although CCTV has been present in public space since its inception its public presence exploded not only in the UK but in many European countries since the 1990s by utilising cameras against street crime. By this development CCTV as instrument of social control has 'left' private and semi-private space to which it was confined from the 1970s till the mid-1980s."[178]

Other authors have also noted the expansion of CCTV in European settings, albeit not as rapid as the rate of expansion in the UK.[179] Today, video surveillance cameras are a common feature of public spaces throughout Europe and in many countries throughout the world.[180]

---

[168] Gerrard, Graeme, Garry Parkins, Ian Cunningham, et al., *National CCTV Strategy*, Home Office, London, 2007; Webster, "Public Administration as Surveillance", 2011, p. 317; Fussey, Pete, and Jon Coaffee, "Urban spaces of surveillance", in Ball, Kirstie, et al. (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, London, 2012, pp. 201-208.
[169] Webster, "The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK", 2004.
[170] Abu-Laban, Yasmeen, "The politics of surveillance, Civil liberties, human rights and ethics", in Ball, Kirstie, et al. (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, London, 2012, pp. 420-427.
[171] Short, Emma, and Jason Ditton, "Does CCTV affect crime?", *CCTV Today*, Vol. 2, No. 2, 1995, pp. 10-12.
[172] Groombridge, Nic, "Stars of CCTV? How the Home Office wasted millions – a radical 'Treasury/Audit Commission' view'", *Surveillance & Society*, Vol. 5, No. 1, 2008, pp. 73-80.
[173] See Chapter 6.
[174] Gerrard, et al., 2007.
[175] Ibid.
[176] Smith, Gavin J.D., "Behind the Screens: Examining Constructions of Deviance and Informal Practices among CCTV Control Room Operators in the UK", *Surveillance &Society*, Vol. 2, No. 2/3, 2004, pp. 376-395.
[177] Webster, "CCTV Policy in the UK: Reconsidering the Evidence Base", 2009.
[178] Hempel, Leon and Eric Töpfer, "Urban Eye: Inception Report to the European Commission", Working Paper, Technical University Berlin, Berlin, 2002.
[179] Webster, "Closed circuit television and governance: The eve of a surveillance age", 1996; Norris, et al., "The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space", 2004, p. 113.
[180] Webster, et al. (eds.), *Video Surveillance Practices and Policies in Europe*, 2012.

However, such a blanket statement hides the subtlety in which the diffusion of CCTV is shaped by different institutional arrangements and cultures in different national settings. For example, countries with a past history of authoritarian or communist regimes have been far more reluctant to install a technology which can be perceived to be a "tool of political control".[181] In France, legislative legacies relating to laws governing photography in public places were initially seen to be a barrier to the provision of CCTV,[182] and in Spain, institutional arrangements between central and local and regional government meant restrictions on the provision of CCTV because only certain agencies had the authority (but not the desire) to operate systems in local communities.[183] The key point here is that CCTV has diffused in different ways in different policy environments and social settings and that those settings shape the way CCTV is configured and used. History, culture, legislative legacies, administrative rules and procedures, vested interests, all play a role in shaping the use of such technologies.

2.4.4 Summary

Video surveillance cameras and systems, referred to as CCTV in the UK, have diffused widely throughout Europe and are one of the most visual manifestations of modern surveillance societies. The highest number of public space CCTV systems and their rate of expansion in the 1990s have undoubtedly been in the UK, although other European countries have also experienced a sustained growth in open street CCTV, especially in urban areas. In the UK, the diffusion of CCTV was initially associated with detecting and deterring crime and received considerable public, policy, industry and public support. Over time, the core purpose of these systems has evolved to consider community safety, anti-social and undesirable behaviour, and most recently to help combat potential terrorist threats. The reasons for the rapid diffusion of CCTV from the 1990s onwards are manifold, and include: political and public support, the availability of a range of policy instruments (funding, guidance, etc.), technological developments, the emergence of commercial CCTV markets and the normalisation of CCTV within society. These factors have combined to create an environment malleable to the diffusion of such systems.

Developments in video surveillance technologies, policies and practices suggest the diffusion of CCTV is evolving. Developments in computerisation, networking and data matching are leading to the development of what is referred to as smart CCTV systems.[184] These systems have a range of capabilities and incorporate a range of technologies. They can include face and movement recognition systems, infra-red movement sensors, listening devices, data matching and profiling. In this respect, CCTV systems are becoming more "intelligent" and surveillance is becoming automated. A further development relates to the networking and integration of disparate systems so that monitoring can be conducted centrally and so that all

[181] Wright, Steve, "An Appraisal of Technologies of Political Control", Working Document, European Parliament, Scientific and Technological Options Assessment STOA, Luxembourg, 1998; Webster, C. William R., Doina Balahur, Nils Zurawski, et al. (eds.), *Living in Surveillance Societies: The Ghosts of Surveillance*, University of Iasi "Alexandru Ioan Cuza" Press, Iasi, 2012.

[182] Heilmann, Eric, "Video Surveillance and security policy in France: From regulation to widespread acceptance", in Webster, C. William R., et al. (eds.), *Video Surveillance Practices and Policies in Europe*, IOS Press, Amsterdam, 2012, pp. 94-102.

[183] Galdon Clavell, Gemma, "Local surveillance in a global world: Zooming in on the proliferation of CCTV in Catalonia", in Webster, C. William R., et al. (eds.), *Video Surveillance Practices and Policies in Europe*, IOS Press, Amsterdam, 2012, pp. 17-36.

[184] Surette, Ray, "The thinking eye: Pros and cons of second generation CCTV surveillance systems", *Policing*, Vol. 28, No. 1, 2005, pp. 152-173; Wright, et al., "Sorting out smart surveillance", 2010.

images recorded meet agreed technical specifications. These developments are providing new opportunities for using CCTV in different ways, in different contexts and for different purposes. So, whilst the diffusion of CCTV was initiated in the 1990s, it is clearly an on-going and subtle process.

2.5 SURVEILLANCE AFTER 9/11

Scrutinising contemporary surveillance practices reveals that, compared to earlier forms of surveillance, its nature has changed drastically. As demonstrated in the previous sections, surveillance is not a new feature of post-industrial society. But, with the beginning of the 21st century, due to its intensification and broadening, surveillance has become a defining element of contemporary life.

Surveillance has become a ubiquitous phenomenon, an inherent feature of everyday life. While surveillance in earlier times was only experienced in specific context such as tax files or medical records, it is nowadays part of almost every facet of daily life. "Daily routines are now subject to myriad forms of checking, watching, recording and analysing, so much that we often take for granted the fact that we leave trails and traces wherever we are and whatever we do."[185] Travelling, working, shopping, telephoning and walking in the street are recorded in some way by using various surveillance systems such as CCTV, electronic transaction monitoring or biometrics.[186]

The witnessing of this routine surveillance goes along with a shift in theoretical conceptions of surveillance. Haggerty and Ericson drew from the work of Deleuze and Guattari[187] and characterise contemporary surveillance practices as an assemblage. This reflects the idea that surveillance is not solely practised by a central state or capitalistic corporations, or reduced to particular practices, but can rather be characterised in rhizomatic terms.[188] The concept of the surveillance assemblage captures the myriad of technologies, actors and practices of surveillance. A central phenomenon emerging from the surveillance assemblage is that it operates "by abstracting human bodies from their territorial settings and separating them into a series of discrete flows. These flows are then reassembled into distinct 'data doubles' which can be scrutinised and targeted for intervention."[189] The concept of the surveillance assemblage underpins the disconnected and semi-co-ordinated character of surveillance.[190] Several contemporary constituting, though variable, elements of the surveillance assemblage can be identified: Lyon lists military discipline and intelligence, state administration and the census, work monitoring and supervision, policing and crime control, consumer-facing websites as those surveillance sites through which surveillance mostly operates.[191]

Surveillance techniques enabled by the Internet enhance the surveillance assemblage massively and provide surveillance capabilities, which exploit new sources and flow through

---

[185] Lyon, David, "Everyday Surveillance: Personal data and social classifications", *Information, Communication & Society*, Vol. 5, No. 2, 2002, pp. 242-257. Staples, W. G., *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*, Rowman/Littlefield, Lanham, MD, 2000.
[186] Lyon, Surveillance Studies: An Overview, 2007.
[187] Deleuze, Gilles, and Félix Guattari, *A Thousand Plateaus*, University of Minnesota Press, Minneapolis, 1987.
[188] Haggerty and Ericson, 2000.
[189] Ibid.
[190] Haggerty, Kevin D. and Richard V. Ericson, "The New Politics of Surveillance and Visibility", in Kevin D. Haggertyand Richard V. Ericson (eds.), *The New Politics of Surveillance and Visibility*, University of Toronto Press, Toronto, 2006, pp. 3-25.
[191] Lyon, *Surveillance Studies: An Overview*, 2007.

new spaces. Gathering data about people through the use of the Internet "actually represents a marked shift towards planned actuarial strategies that rely upon the analysis of secondary data obtained through the convergence of technologies and databases to surveil individuals and suspect groups who have previously been identified as a potential risk".[192] It's not that the Internet as a technology totally renews concepts of surveillance, but it strengthens the surveillance assemblage to a huge extent.

2.5.1 Causes of contemporary surveillance practices

Surveillance is influenced by a multiplicity of factors and entails complex political implications. Within the vast amount of theoretical and practical considerations within surveillance studies, the approach to define surveillance as a characteristic feature of modernity seems to be axiomatic.[193] Hence, one way to approach the causes of contemporary surveillance practices is to analyse the diverse concomitants of modernity that influence those practices. The following sections, of course, do not offer a totality of driving factors of contemporary surveillance, but instead they focus on the multiplicity of overlapping dynamics that contribute to current surveillance practices.

Consumer capitalism

The idea of "late modernity", a term coined by Anthony Giddens,[194] reflects a phase of changes within the second half of the 20th century, where new relationships between the economy, the state, society and culture have evolved. One important aspect of late modernity is the shift to a consumer capitalist phase.[195] The political-economic context moved towards "consumer capitalism", and the economic significance of personal data increased significantly. Companies use the Internet as a marketplace for exchanging personal data such as e-mail addresses, phone numbers and postal addresses.

The possibility of capturing, storing and transmitting data at low costs via the Internet have played a significant role within these developments. The collecting of customer preferences, choice and histories resulting from digital traces left behind by users' online activities has become a core aspect of customer relationship management.[196] New kinds of surveillance are constituted through detailed data mining and profiling on customers with the main purpose of social sorting (see section below). [197] Technical means are used to extract or create personal data that has been taken from individuals or contexts.[198] Social sorting, which is eventually possible on a large scale due to electronic technologies, is seen as a specificity of contemporary surveillance.

---

[192] Levi, Michael, and David S. Wall, "Crime and Security in the Aftermath of September 11: Security, privacy and law enforcement issues relating to emerging information and communication technologies", in Ioannis Maghiros (ed.), *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*, Office for Official Publications of the European Communities, Luxembourg, 2003, pp. 163-185.

[193] Haggerty, Kevin D., and Richard V. Ericson (eds.), *The new politics of surveillance and visibility*, University of Toronto Press, Toronto, 2006; Murakami Wood, et al., "A Report on the Surveillance Society", 2006; Lauer, Josh, "Surveillance history and the history of new media: An evidential paradigm", *New Media & Society*, Vol. 14, No. 4, 2012, pp. 566-582..

[194] Giddens, Anthony, *The consequences of modernity*, Polity Press, Cambridge, 1990.

[195] Lyon, David, "Globalizing Surveillance", *International Sociology*, Vol. 19, No. 2, 2004, pp. 135-1349.

[196] Lyon, *Surveillance Studies: An Overview*, 2007.

[197] Lyon, David, *Surveillance society. Monitoring everyday life*, Open University Press, Buckingham, 2001; Lyon, "Everyday Surveillance: Personal data and social classifications", 2002.

[198] Marx, Gary T., "What's New About the "New Surveillance"? Classifying for Change and Continuity", *Surveillance & Society*, Vol. 1, No. 1, 2002, pp. 9-29.

Information society

David Lyon argues that information societies are by their very constitution also surveillance societies.[199] Advanced surveillance operations are an inherent part of information societies, in which ICTs are the central means of co-ordination and exchange. In this respect, there is much continuity: While the rise of the industrial society was based on division of physical labour and the surveillance and control of this work, the information society now aims to rationalise intellectual work.[200] However, in the information society surveillance is no longer limited to the workplace.

Taking into account the above mentioned purposes of gathering information about customers to sort them into standardised categories, the ambiguity of information societies comes to the fore: digital technologies reflect means to socially exclude and at the same time help to overcome social barriers and processes of marginalisation.[201] Although surveillance is mostly concerned as a threat, much of our everyday convenience, efficiency and security depend on the collection of data, i.e., upon surveillance.

Surveillance can be framed as one form of communication to compensate the increasing demand for "tokens of trust" due to the increasing disappearance of bodies and the abilities to organise everyday life at a distance.[202] Resulting from the proliferation of new technologies, face-to-face communication has been supplemented by forms of communication that do not require the physical presence of people.

Contemporary practices of surveillance are better understood as "dataveillance", defined as "the systematic use of personal data systems in the investigation and monitoring of the actions or communications of one or more persons".[203]Surveillance by electronic means is an increasingly significant mode of governance in so-called knowledge-based or information societies.[204] Drawing on Daniel Bell's approach to define current societies as knowledge societies, where the central axis is knowledge, the collection and processing of information become the real creation of value.

Highly connected to the concept of information societies is the centrality of the risk logic within modern societies. What Ulrich Beck called the "risk society" has evolved as an outcome of industrial society, since the "social, political, ecological, and individual risks created by the momentum of innovation increasingly elude the control and protective institutions of industrial society".[205] Beck argues that the provident state is less and less willing to bear the costs of individualised risks which replaced the calculable risks of the post-industrial times where the influence and care of the state grew. Today, surveillance can be understood as a practice of collecting information about individuals with the purpose of calculating and eventually reducing risks.[206]

---

[199] Lyon, "Everyday Surveillance: Personal data and social classifications", 2002.
[200] Beniger, 1986.
[201] Graham, Stephen, and David Murakami Wood, "Digitizing surveillance: Categorization, space, inequality", *Critical Social Policy*, Vol. 23, No. 2, 2003, pp. 227-248.
[202] Lyon, "Everyday Surveillance: Personal data and social classifications", 2002.
[203] Clarke, 1988.
[204] Lyon, "Everyday Surveillance: Personal data and social classifications", 2002.
[205] Beck, Ulrich, "Risk Society and the Provident State", in Scott M. Lash, et al. (eds.), *Risk, Environment and Modernity: Towards a New Ecology*, Sage Publications, London, 1996, pp. 27–43.
[206] Lyon, "Globalizing Surveillance", 2004.

Globalisation

A further aspect of late modernity is globalisation.[207] Surveillance is closely related to the economic, social, cultural and political dimensions of globalisation due to the fact that the need to act at a distance is an inherent characteristic of globalisation. As stated above, in a "distant world", surveillance acts as a form of communication where new proofs of identity and sorts of trust are necessary. As a matter of fact, the facilitated and increased flow of data around the world also increases the flow of surveillance data. While in earlier times surveillance had its boundaries in different form, e.g. ,work places or nation states, nowadays surveillance has become global. Personal data collected or processed by governmental or commercial agencies can be exchanged globally. New nodes and networks become structurally important,[208] and searchable databases, where the aforementioned "tokens of trust" such as ID cards, telephone numbers or drivers' licences are stored, are a requirement for transactions. Striking examples of such systems transcending national boundaries are electronic commerce or air travel.[209] In general terms, policing and e-commerce across borders involves cross-border data flow.

However, Lyon argues that surveillance is "glocalized" (a term coined by Roland Robertson[210]), since surveillance practices highly depend on factors such as economic priorities, technological development levels, legal oversight or civil societal opposition, which are shaped differently in different countries.[211] Nevertheless, the increasing internationality of the surveillant assemblage and the fact that surveillance blurs the old borders are not deniable.

2.5.2 Surveillance technologies after 9/11

The events of 11 September 2001 are milestones for the co-evolution of surveillance technologies and practices. Surveillance had also increasingly been accepted as being part of everyday life before the terrorist attacks, but nevertheless, since then it has become even more obvious.[212] Since the end of the Cold War, a move away from "reactive policing" towards "intelligence gathering policing" was already taking place, but this process accelerated after the events of 9/11.[213] Technologies and techniques of information collection and information processing tend to work towards a model of pre-emptive activities for which intensive surveillance is required[214] in order to combat real or perceived security threats.

The inherent ambiguities of contemporary surveillance have become especially obvious since 9/11. On the one hand, surveillance is supposed to be a mechanism that guarantees the security of the citizens or a society. But, at the same time, complaints about personal data abuses and intrusions from new security laws have been raised. Hence the boundaries between the guarantee of security and social control are blurred.

---

[207] Ibid.
[208] Castells, Manuel, *The rise of the network society* (3 volumes), Blackwell, Oxford, 1996.
[209] Lyon, "Globalizing Surveillance", 2004.
[210] Robertson, Roland, "Glocalization: Time-space and homogeneity-heterogeneity", in F. Featherstone, et al. (eds.), *Global Modernities*, Sage, London, 1995.
[211] Lyon, Surveillance Studies: An Overview, 2007.
[212] Lyon, David, "9/11, Synopticon, and Scopophilia: Watching and Being Watched", in Kevin D. Haggerty and Richard V. Ericson (eds.), *The New Politics of Surveillance and Visibility*, University of Toronto Press, 2006, pp. 35-54.
[213] Levi and Wall, 2003.
[214] Lyon, *Surveillance Studies: An Overview*, 2007.

A salient feature of digital surveillance is the possibility to collect, store and process huge amounts of data. But digital surveillance does not only differ from analogue surveillance systems in quantitative terms, but also in qualitative terms:[215] the data processing can be automated, algorithms can be applied, and various surveillance systems, i.e., databases based on different surveillance technologies, can be connected. After this rather general perspective of contemporary surveillance, we briefly analyse a range of specific surveillance technologies and techniques. Below, we elaborate slightly Clarke's concept of dataveillance.

2.5.2.1 Enhanced dataveillance

Roger Clarke coined the term dataveillance in the 1980s, when he tried to capture the spread of computers and the possibilities to process data that came along with that (see section 2.3.4). In 2003, he re-thought his ideas about dataveillance taking into account recent developments. In his 1988 paper, he already drew attention to the consolidation of personal data from multiple sources, the emergence of new technologies to exploit that data, and the central role of multi-purpose identification schemes.[216] Data matching, profiling, cross-system enforcement and front-end verification are techniques that had already been used when he coined the term dataveillance. New modes of surveillance, which he added in his revision in 2003, include Internet tracing, digital rights management, chip-based identification, biometrics, person locating and tracking.[217]

Clarke distinguishes between "personal dataveillance", the monitoring of the data of one specific person, and "mass dataveillance", the systematic investigation or monitoring of groups of people via their data traces.[218] The data gathered for *personal dataveillance* may include credit card usage, shopping patterns (using loyalty cards or access to the databases of Internet shops in the case of online shopping), or monitoring the surveilled's e-mail and Internet usage (e.g., via his or her Internet service provider). To some extent, personal dataveillance can also reveal the surveilled's whereabouts. The location can be inferred, for example, from the monitoring of financial transactions (by knowing when and where a credit or debit card has been used), or from electronic toll collection systems installed in the target's car. Typically, personal dataveillance is complementary to communication surveillance (e.g., phone calls) and physical surveillance (e.g., physical location).

Mass dataveillance monitors the data traces of large groups of people in order to identify individuals with a specific profile (e.g., individuals considered potentially dangerous): "mass dataveillance is concerned with groups of people and involves the generalised suspicion that some (as yet unidentified) members of the group might be of interest".[219]

2.5.2.2 Data collection technologies

As follows, we introduce a selection of contemporary surveillance technologies, based on the criterion of increased usage and relevance for policy strategies after 9/11.

[215] Ibid.
[216] Clarke, 1988.
[217] Clarke, Roger, "Dataveillance - 15 Years On", Paper presented at: Privacy Issues Forum run by the New Zealand Privacy Commissioner, Wellington, 28 March 2003.
[218] Clarke, "Information Technology and Dataveillance", 1988.
[219] Ibid.

Web-generated data

The Web is one important touch point for practices of surveillance, which enables the creation of vast amounts of personal data. The term "cyber surveillance" usually refers to the tracking of online behaviour, which is related to Web surfing. In a broader sense, it can also include the monitoring of e-mail exchange, peer-to-peer connections, VoIP, remote logins, file download or instant messaging. Information may be collected from forms, transactions or clickstream records, which allow path analyses, shopping cart analyses, analyses of entry and exit points, analyses of search terms or key words entered, etc.

Probably the most prevalent form of cyber surveillance is represented by so-called cookies. Cookies are small pieces of text, which a web server can place on the client's computer to store precisely such data. Whenever the user subsequently visits (i.e., requests) one of the pages of the same website, the browser will send the previously stored cookie along with the request. For example, the state of a virtual shopping cart can be stored inside a cookie; at each new visit, the cart's previous state is still available.[220]

While the basic functionality is innocuous enough, the fact that web pages can be combined with elements (e.g., images) from many different Internet sources allows a single site to track users across a range of different sites. Many companies have since specialised in tracking users in such a fashion using so-called "tracking cookies" or "web bugs" across two or more seemingly unrelated websites to learn about the user's surfing preferences.[221]

More powerful surveillance opportunities lie with Internet service providers (ISPs). In many countries, ISPs are already required by law to record so-called "traffic data", i.e., the individual connections made from each connected computer, for several months. Aside from webpage URLs, these connections include, for example, e-mail headers, FTP connections and VoIP calls. ISPs can also use a technique called "deep packet inspection" (DPI),[222] which analyses each data packet passing between their customers and the Internet in order to extract its semantic content. While DPI can be used for non-surveillance purposes (such as network management or Internet statistics),[223] it can also be used as a censorship tool, for example, by blocking certain data types or content. Anyone with an Internet connection is subject to surveillance via the storage of traffic data.[224]

Apart from tools for ISPs, there is a plethora of so-called "parental control" software that locally monitors computer activity, including text-based communication.[225] Once installed, on purpose or automatically, e.g. via a Trojan horse, such software exhaustively monitors all activity on the computer, such as the content of sent and received emails and IM chats, social network activity, visited websites and more. All keystrokes are registered and the surveillant receives hidden, complete reports at an e-mail of choice, with an adjustable frequency of 30

[220] Gutwirth, et al., 2012, p 33.
[221] Symantec, "Tracking Cookie". http://www.symantec.com/security_response/writeup.jsp?docid=2006-080217-3524-99
[222] See Fuchs, Christian, "Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society", Privacy & Security Research Paper #1, PACT Project, Uppsala, 2012. Bendrath, Ralf and Milton Mueller, "The End of the Net as we know it? Deep Packet Inspection and Internet Governance", New Media & Society, Vol. 13, No. 7, 2011, pp. 1142–1160.
[223] See, for example, iPoque's study about the relative weight of different Internet applications: Schulze, Hendrik and Klaus Mochalski, "Internet Study 2008/2009", ipoque GmbH, Leipzig, 2009.
[224] Gutwirth, et al., 2012, p.33.
[225] Naraine, Ryan, "First Look: Sentry Remote and eBlaster 6.0", PCWorld, 15 November 2007.

minutes to 24 hours. Without administrator's rights, the average user has little chance to find out that such sniffing software is installed, and even with administrator access, the software is difficult to discover.[226]

RFID

The roots of radio frequency identification (RFID) techniques can be found in inventory control systems; nevertheless, they are applied in everyday life.[227] Products, tickets, animals, passports or any other objects can be tagged with an RFID for the purpose of identifying or locating objects.[228] RFID systems can be distinguished into active and passive systems.[229] The tags of the active systems have their own battery and can send information up to a few hundred meters. The tags of the passive systems, which are already very widespread, do not possess their own power source, but only react to requests. Passive RFID tags have a reading range of a few metres maximum, and often just a few centimetres. RFID allows the implicit localisation of persons or objects that can be assigned to persons, which offers significant surveillance potential.

GPS, GSM and Wi-Fi-based location determination

The Global Positioning System is a worldwide satellite-based, geo-localisation system.[230] A network of 24 satellites circle the earth twice a day and constantly transmit messages containing the satellite position and the time the message was sent. Based on this information, a GPS receiver can calculate a two-dimensional position (if locked on to the signal of three satellites) or a three-dimensional position (if locked on to the signal of four or more satellites).[231] Since the actual location is computed on the receiver's side only, GPS devices are traditionally not suitable for any kind of surveillance. However, GPS devices are increasingly equipped with a data communication module using UMTS or LTE,[232] via which the device can communicate its position. For instance, emergency assistance systems (the "e-call") for vehicles are such a novel service.

Location determination based on mobile phones offers, due to the popularity of mobile phones, several surveillance possibilities. Mobile phones can be located based on proximity sensing, which means that a phone can be traced if it is within a specific grid cell and communicates with the corresponding cell tower. Hence, mobile telephone providers may

[226] Gutwirth, et al., 2012, p. 34; Greene, Thomas C., "eBlaster spyware has Achilles heel: Well designed, yet easily defeated", The Register, 16 June 2003.. These technologies are also often used for surveillance of employees at the workplace. See Nouwt, Sjaak, Berend R. de Vries and Corien Prins (eds.), Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy, TCM Asser Press, The Hague, 2005.

[227] van Lieshout, Marc, Luigi Grossi, Graziella Spinelli, et al., *RFID Technologies: Emerging Issues, Challenges and Policy Options*, IPTS Technical Report Series EUR 22770 EN, Office for Official Publications of the European Communities, Luxembourg, 2007; Wolfram, Gerd, Birgit Gampl and Peter Gabriel (eds.), The RFID Roadmap: The Next Steps for Europe, Springer, Berlin, Heidelberg, 2008.

[228] Kern, Christian, *Anwendungen von RFID-Systemen*, Springer, Berlin, Heidelberg, 2007.

[229] Finkenzeller, Klaus, *RFID-Handbuch: Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten*, Hanser, München, 2006.

[230] Gutwirth, Serge, Rocco Bellanova, Michael Friedewald, et al., "Smart Surveillance - State of the Art Report", Deliverable 1, SAPIENT Project, 2012.

[231] Xu, Guochang, GPS: Theory, Algorithms and Applications, Springer, Berlin, Heidelberg, New York, 2007.

[232] Wikipedia defines LTE as an initialism of Long Term Evolution, marketed as 4G LTE, a standard for wireless communication of high-speed data for mobile phones and data terminals. UMTS stands for Universal Mobile Telecommunications System, a third generation mobile cellular system.

locate a mobile phone without difficulties. Similar to the GSM-based localisation, Wi-Fi signals may also be used to track a mobile phone. Based on Wi-Fi signals, which are especially widespread in urban areas, the position of a Wi-Fi enabled mobile device can be located without being logged into the respective Wi-Fi network. Since Wi-Fi antennas are typically not under the control of a single authority and a database with Wi-Fi network information is necessary to track a phone, the technology has its drawbacks but in principle has surveillance capabilities.[233]

Communications surveillance

As communication technologies have evolved, so enhanced forms of wiretapping have developed. For instance, nowadays the switches of telephone companies allow copying bit streams of unencrypted digitised voice traces.[234] If the network is encrypted, wiretapping is possible at the telephone itself or within the target's organisation before the device that encrypts the signal.[235] Concerning mobile phones, which are based on the transmission of GSM signals, the challenge "is not to wiretap (which consists of the technologically trivial creation of a copy of an unencrypted bit stream inside one of the network's switches), but to repel abuse."[236]

With the exponential diffusion of the Internet, the costs of communication have reduced immensely. In contrast to traditional telephone lines, which are based on circuit switching, Voice over IP uses small packets, which are sent between Internet users. Because there is no fixed circuit for the duration of a VoIP call, and no guarantee that the packets use the same route, wiretapping Internet calls is more challenging than wiretapping telephone lines.

Biometrics

"Biometrics comprise both science and a set of technologies that focus on the measurement of either physiological or behavioural human characteristics."[237] Biometrics can be categorised into physiological and behavioural biometrics. The former covers (more or less) fixed human characteristics such as iris patterns, facial image, odour, hand and finger geometry, DNA and fingerprints, and is mainly used for identification and verification purposes. The latter refers to actions, skills or functions that require an active performance of a person, e.g., typing patterns, gait, voice or signature. Due to sufficient inter-person variability and low intra-person variability, biometrics are mostly used for distinctiveness purposes.[238]

Most of the biometric techniques rely upon a database of known individuals, and identification is only successful if the sought individual is on the database. For instance, facial recognition works by matching an image of a person with an image stored in a database.

---

[233] Rosendaal, Arnold, "Massive Data Collection by Mistake?", in Jan Camenisch, et al. (eds.), *Privacy and Identity Management for Life*: 7th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Trento, Italy, September 5-9, 2011, Revised Selected Papers, Springer, Heidelberg, Berlin, 2012, pp. 274-282.
[234] Diffie, Whitfield, and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, MIT Press, Cambridge, Mass., 2007.
[235] Gutwirth, et al., 2012.
[236] Ibid.
[237] Andronikou, Vassiliki, Angelos Yannopoulos and Theodora Varvarigou, "Biometric Profiling: Opportunities and Risks", in Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer, Dordrecht, 2008, pp. 131-145.
[238] Jain, Anil K., Arun Ross and Salil Prabhakar, "An Introduction to Biometric Recognition", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 14, No. 1, 2004, pp. 4-20.

Suspects can be identified on the basis of DNA profile matching, if information about the DNA of an individual is on a database. Based on such databases, authentication is an important area of application.

In addition to the application of biometrics in the area of criminal investigation and the tracking of suspects, security reinforcement plays a role as potential criminals may also be detected. Psychologists and technologists work together in order to develop techniques, which detect suspect behaviour based on behavioural biometrics, such as gait. Through this, authorities hope to prevent illegal acts by people for whom no information in databases exists.[239]

Biometric techniques are also attractive for daily commerce with advertising purposes. For instance, the profile of a person entering a supermarket could be extracted from a database, e.g., based on facial recognition of behavioural biometrics, and then targeted advertising, e.g., via SMS, could be applied.[240]

2.5.2.3 Data processing

While the previous section introduced some of the technologies which are applied in order to enable the collection and recording of data, it is not just the retrieval of information that is brought into focus, but rather the techniques which allow the profiling of data objects, namely data mining.[241]

Data mining can be defined as "a process that has as its goal the transformation of raw data into information that can be utilised as strategic intelligence within the context of an organisation's identifiable goals"[242] or as "the procedure by which large databases are mined by means of algorithms for patterns of correlations between data."[243] Possible data mining techniques involve complex algorithms, artificial intelligence, neural networks and even genetic-based modelling.[244] By applying those techniques, previously unknown facts, such as relationships between objects within databases, can be discovered. Hypotheses or assumed correlations are not necessarily developed beforehand but are rather a product of data mining processes themselves. Thus, data mining is often referred to as a discovery-driven approach, as opposed to the more traditional assumption-driven approaches.[245] As Zarsky puts it, data mining techniques answer "questions users did not know to ask".[246] Besides these rather predictive implementations of data mining techniques, it can also be descriptive in a sense

[239] Andronikou, et al., 2008.
[240] Ibid.
[241] Definitions are a problem in the area of data mining, as every writer uses the terms differently. The term "data mining" is used in two distinct ways: both to define the entire process (as in Knowledge Discovery in Databases KDD) and to describe the specific stage in which the algorithms are applied. We view data mining as the entire process and thus use it as a synonym for KDD. See Zarsky, Tal Z., "Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion", *Yale Journal of Law and Technology*, Vol. 5, 2003, pp. 1-56.
[242] Gandy, Jr., Oscar H., "Mining, Surveillance, and Discrimination in the Post-9/11 Environment", in Kevin D. Haggerty and Richard V. Ericson (eds.), *The new politics of surveillance and visibility*, University of Toronto Press, Toronto, 2006, pp. 363-384.
[243] Hildebrandt, Mireille, "Defining Profiling", in Mireille Hildebrandt and Serge Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer, Dordrecht, 2008, pp. 17-46.
[244] Zarsky, 2003.
[245] Hildebrandt, 2008.
[246] Zarsky, 2003.

that statistical methods are applied in order to provide condensed summaries of large amounts of information (so-called big data).[247]

Profiling is closely related to data mining; in fact, it can be seen as a result of the process of data mining. Gandy talks about "computer-enhanced discriminatory techniques";[248] Hildebrandt defines profiling as "the use of algorithms or other techniques to create, discover or construct knowledge from huge sets of data".[249] If data mining is the process where the classes of users are defined, then profiling attempts to predict individual future behaviour.[250] Profiling is arguably one of the most significant ways in which dataveillance departs from earlier practices of surveillance.

Similar to Clarke's differentiation between individual and mass dataveillance, a general differentiation can be made between group profiling and personalised profiling. In relation to group profiling, a process of data mining establishes categories of people who have certain attitudes and therefore constitute a group (also called a bucket). The group may explicitly exist or it may be the result of a categorisation that leads to (virtual) community building. Mining of data related to an individual subject enables the building up of personal profiles that can be used to offer specific goods or provide access to certain services.

Both kinds of profiling, individual profiling and group profiling, have led to and are used for marketing (targeted assessment of consumer preferences), insurance (targeted risk assessment) and justice purposes (criminal profiling).[251] Hildebrandt calls those procedures an "actuarial approach", since it is based on predictions of future behaviour and builds on highly sophisticated assessments of risks and opportunities.

Social sorting

After describing the technologies of contemporary surveillance and the processing of data gained by applying those technologies, we now detail for what the collected and categorised data may be used.

As stated above, profiling leads to categories to which people are assigned. As a consequence, people are treated as belonging to a specific group, which in turn suggests what sort of person someone is. The category becomes more important than the individual character.[252] Virtual selves are created for discrimination between categories to facilitate different treatment. Those subjects are not an imitation or replication of the original subject, but rather the creation of a "multiplicity of selves that may be acted upon without the knowledge of the original".[253] The surveillance assemblage, the establishing of networks of surveillance systems and the digitisation of surveillance contribute to the broad utilisation of such processes of sorting.

Lyon exemplifies the appliance of social sorting as follows: "The urban water utility may depend on the automated sorting of customers by postal or zip code to determine how they are

[247] Gandy, 2006.
[248] Ibid.
[249] Hildebrandt, 2008.
[250] Gutwirth, et al., 2012.
[251] Hildebrandt, 2008.
[252] Lyon, *Surveillance Studies: An Overview*, 2007.
[253] Graham and Wood, 2003.

treated depending on their neighbourhood and their past record with the company. Road-use may be decided by automated tolling systems that permit access only to drivers who can pay. Internet access and speed may vary depending on what kinds of commercial transactions are made by surfers. The supermarket may offer deals to certain groups of shoppers and not others, depending on their knowledge of transaction contained in loyalty cards."[254]

In this sense, surveillance can be assessed as a means of governance: "it serves to organise social relationships and contributes to patterns of social ordering".[255] The different kinds of classifications have varying degrees of powerfulness, while surveillance produces categorical suspicion at one end; it produces categorical seduction at the other end. The one side of the continuum, the first one mentioned, can be exemplified by the practice of treating different ethnic groups differently at airport checks. Practices reflecting the other end of the continuum could be the special treatment of owners of loyalty cards, which could, e.g., lead to more favourable conditions for those customers. Due to such practices, price and marketing discriminations resulting in exclusion of classes of individuals from full participation in the marketplace are possible.[256] Similarly, social concerns can be raised about exclusion from the public sphere caused by discriminating access to previously freely available public information.

2.5.2.4 Actors and purposes

Information collecting and data processing is neither reduced to governmental practices nor to the work of corporations. While the primary purpose of the processing of consumer data is to streamline and specify the targeting of consumers, the data collected might in some cases also be used for secondary purposes in law enforcement and the post-9/11 "war on terror".[257] The divide between consumer data management and crime control is not clearly delineated anymore. A prominent example of such practices is the exchange of travel-related data, the so-called passenger name records (PNRs).

Huge amounts of data, especially electronic data such as click paths, have become highly valuable for corporations. Customer activities are tracked and customer relationship management is optimised in order to allow targeted marketing. Customers are grouped and depending on the value of the group to which on adheres, treatment differs. Fraudulent customers are filtered at the bank machine and personalised advertisements "follow" someone who is surfing on the net and has been identified as a potentially valuable customer.

The predominant rationale for interference into the private sphere from state authorities is the idea of reducing risks. Governments wish to protect citizens from illegal immigration, terrorism and crime, which is why they often pass laws introducing or enabling new surveillance systems. Within law enforcement and related contexts, the gathering of information is justified by the positive goals of combating crime and terrorism.[258] For instance, the European Union runs the EURODAC database, which holds fingerprints of asylum seekers, and the Visa Information System (VIS), which holds personal details, facial

[254] Lyon, *Surveillance Studies: An Overview*, 2007. Graham, Stephen, "The software-sorted city: Rethinking the digital divide", in Stephen Graham (ed.), *The Cybercities Reader*, New York, 2004.
[255] Lyon, "Everyday Surveillance: Personal data and social classifications", 2002.
[256] Danna, A., and Oscar Gandy, Jr., "All that Glitters is Not Gold: Digging Beneath the Surface of Data Mining", *Journal of Business Ethics*, Vol. 40, No. 4, 2002, pp. 373-386.
[257] Lyon, *Surveillance Studies: An Overview*, 2007.
[258] Ibid.

images and fingerprints of visa applicants to the EU. Another example is CODIS (the combined DNA index system) and AFIS (the automated fingerprint identification system), systems run in the USA by the FBI with a link to local and state databases. Especially since 9/11, the US and EU policy focus on surveillance activities has increased. Hence, in the following section, we present policy responses to 9/11.

2.5.3 Surveillance as a policy response to 9/11

Contemporary discussions about surveillance are inevitably entangled with the terrorist attacks of 11 September 2001. Although the so-called "war on terror" in the aftermath of 9/11 is only one rationale for the use of surveillance systems, those events intensified anti-terrorist monitoring regimes.[259] However, it is important to note that the proliferation of surveillance techniques and technologies was already increasingly accepted before the events of 9/11. Nevertheless, surveillance systems have become more commonly accepted since then, and much of the public and many policy-makers alike seem to accept widespread deployment of surveillance systems as the price to be paid for the security of citizens.[260] Consequently, mandates for security measures that were carried out after 9/11 and that had been under discussion before then (when they probably would not have been so easily tolerated) were strengthened. 9/11 may be seen as "the occasion rather than the cause of the introduction of a new security paradigm".[261] Lyon even claims that without the media attention prompted by 9/11 and the public opinion effects of "sympathy, anger, fear, and the quest for retribution" it created, "many legal and technical measures, long-cherished dreams of some politicians and technocrats, would never have appeared plausible or workable."[262]

The US took a leading role in the declaration of the "war on terrorism" and implemented measures that would inevitably affect other countries as well.[263] As mentioned earlier, globalisation has changed many facets of society, the economy and political life. In terms of globalised surveillance, partly caused by anti-terror measures, cross-national crime and border control are particularly salient aspects and the most prominent issues are related to questions of immigration, international policing and citizenship. While for some people, borders are as open as they ever have been, for others, borders have never been so tightly controlled as nowadays.[264] For instance, airports represent one important example for a surveillance site where the collection of huge amounts of personal information is facilitated. The transfer of personal data from national governments to foreign governments, from corporations to governments and from citizens to corporations or governments are routine operations for various purposes such as identification, criminal investigation, intelligence or the tracking of individuals. As Lyon observes, new measures of control accompanying the "war on terrorism" particularly focus on airports, "given that the attacks on the symbolic power centres of New York and Washington were carried out by single domestic aeroplanes and that these are the most obvious points of entry by potential enemies into any country".[265] Yet, it is not only the fight against terrorism or attempts to prevent terrorist attacks that guide policy or legal initiativesthat affect the surveillance of individuals. For instance, smart surveillance

[259] Haggerty and Ericson, "The New Politics of Surveillance and Visibility", 2006.
[260] Lyon, "9/11, Synopticon, and Scopophilia: Watching and Being Watched", 2006.
[261] Maghiros, Ioannis, Laurent Beslay, Clara Centeno, et al., *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*, Office for Official Publications of the European Communities, Luxembourg, 2003, p. 8.
[262] Lyon, "9/11, Synopticon, and Scopophilia: Watching and Being Watched", 2006, p. 37.
[263] Lyon, *Surveillance Studies: An Overview*, 2007, p. 121.
[264] Ibid.
[265] Ibid., p. 122.

tools applied for border control play an important role for terrorist tracking but also for the broader purpose of preventing unwanted migration. The hardening of security measures and the strengthening of anti-terrorism legislation may both be seen as characteristic of post 9/11 national and international governmental activities.

In the aftermath of 9/11 "states of emergency" and "exceptional circumstances" have been routinised and the so-called "safety state" has developed.[266] Wide-ranging national and EU-wide legal and policy initiatives emerged as a result of a perceived increase in terrorist threats. In the following section, we briefly describe a selection of politically significant legislative measures after 9/11 within the EU and the US.

2.5.3.1 US response to 9/11

It seems to be justified to cite Lyon[267], who refers to Abrams'[268] comment about "the event", which "is a portentous outcome; it is a transformation device between past and future; it has eventuated from the past and signifies for the future". By all means, 9/11 constitutes such an event. As Parenti puts it, 9/11 did "radically accelerate momentum towards the soft cage of a surveillance society, just as it gave the culture of fear a rejuvenating jolt".[269] Beginning with the establishment of the Department of Homeland Security shortly after 9/11, the US introduced various surveillance-related measures.

US PATRIOT act

One rather drastic and hastily implemented response to the terrorist attacks was the passing of the USA PATRIOT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act by the US government. The PATRIOT Act is probably one of the most influential new measures after 9/11 in terms of surveillance of citizens. The legislation passed Congress in October 2001 and modified or revised 15 federal laws[270] and "introduced a sweeping arsenal of new federal powers".[271] In general, four of the government's main tools of surveillance are expanded by the PATRIOT Act, namely wiretaps, search warrants, subpoenas, and pen/trap orders.[272]

One of those 15 laws on which the PATRIOT Act had a decided impact was the Foreign Intelligence Surveillance Act (FISA) of 1978. FISA originally allowed agents to get warrants from a special warrant court only if foreign counter-intelligence was the "primary purpose". The already low standards of proof had been loosened in a way that agents only had to prove that there was a "significant" foreign intelligence purpose in the investigation.[273]

---

[266] Ibid., p. 119.
[267] Lyon, David, Surveillance after September 11, Polity Press, Cambridge, 2003, p. 15f.
[268] Abrams, Philip, Historical sociology, Cornell University Press, Ithaca, N.Y, 1982, p. 191.
[269] Parenti, 2003, p. 200.
[270] Bloss, William, "Escalating US Police Surveillance after 9/11: an Examination of Causes and Effects", Surveillance & Society, Vol. 4, No. 3, 2007, pp. 208–228.
[271] Parenti, 2003, p. 200.
[272] Ibid. A pen register is an electronic device that records all numbers called from a particular telephone line, while "trap & trace" (or pen/trap) devices record the numbers that call you. The PATRIOT Act broadened the scope of both to the Internet.
[273] Ibid.

Furthermore, the PATRIOT act broadens pen/trap orders in wiretap law in two ways[274]: First, pen/trap orders are valid nationwide, no matter where the judge, who issued the order, is located. Second, the possibilities to access person-related data from the Internet has been widened, e.g., IP addresses maybe recorded. In addition, whereas in the past it was necessary to get a warrant for each telephone line that was tapped, it is now possible to tap all telephone lines a person might use with just one warrant.

Another trend that occurred when the PATRIOT act was implementedis an increase of the number of national security letters (NSLs) sent by the government to private organisations such as banks, credit companies or ISPs. NSLs ask the companies to hand over customer records (e.g., transactional records such as phone numbers or e-mail addresses).[275] The NSLs also contain a gag letter, which forbids the receiver to tell anyone about it. In addition, the information the government obtains will never be destroyed. The FBI is allowed to force third parties to provide personal records about anyone without proving evidence that there is any relation to a foreign power.

The provisions of the government enabled and expanded by the US PATRIOT Act are manifold and could be discussed extensively, but the aforementioned examples are sufficient to exemplify how the PATRIOT Act undermined the legal environment in favour of more surveillance.

Total Information Awareness (TIA)

Another influential US project in terms of surveillance was the Total Information Awareness (TIA) project (later renamed Terrorism Information Awareness) funded by the Pentagon's Defense Advanced Research Projects Agency (DARPA). The Information Awareness Office (IAO), which was funded between January 2002 and March 2003, worked on a plan to pull together all public and private records of everyday life in order to identify and detect potential terrorists.[276] According to the initial call, DARPA "is soliciting innovative research proposals in the area of information technologies that will aid in the detection, classification, identification, and tracking of potential foreign terrorists, wherever they may be, to understand their intentions, and to develop options to prevent their terrorist acts".[277] Based on traces left by, for example, credit cards, banking transactions or library use, the government was going to develop a vast database to be used for extensive data-mining and profiling activities. The program raised public concern to a huge extent, and was supposedly terminated in response to the popular outcry against the project.

In fact, the TIA program was only one facet of the research of the IAO. Related projects dealt with facial recognition based on images created by video cameras (identification at a distance) or the development of a national strategy to cyber security. Although funding for the IAO was terminated in 2003, similar programs continued to be funded under different names and by other government agencies.[278]

---

[274] American Civil Liberties Union, "Surveillance Under the USA/PATRIOT Act", New York, last upated 23 October 2001. http://www.aclu.org/technology-and-liberty/surveillance-under-usapatriot-act

[275] Levi and Wall, 2003.

[276] Parenti, 2003, p. 213.

[277] DARPA solicitation notice, BAA-02-08, as cited in Electronic Privacy Information Center (EPIC), "EPIC Analysis of Total Information Awareness Contractor Documents", last upated February 2003. http://epic.org/privacy/profiling/tia/doc_analysis.html

[278] Williams, Mark, "The Total Information Awareness Project Lives On", MIT Technology Review, 26 April 2006.

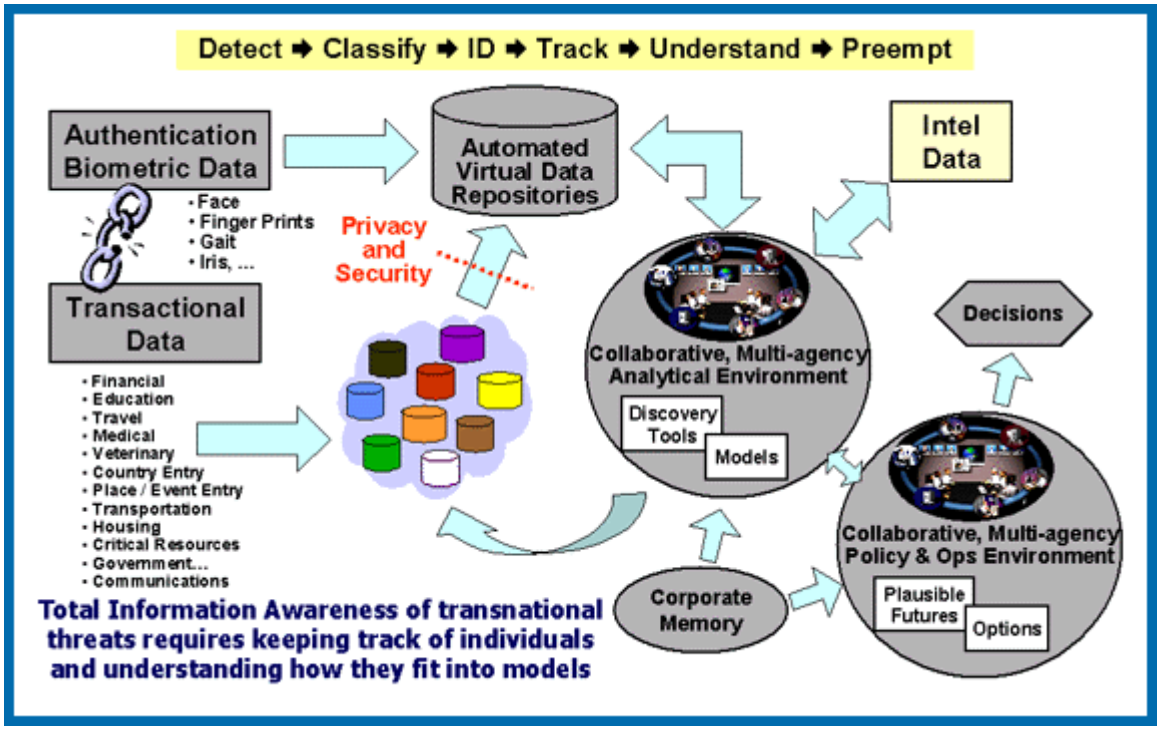


Figure 2: Functional view of the TIA system
Source: DARPA, http://infowar.net/tia/www.darpa.mil/iao/TIASystems.htm (26 October 2012)

Passenger Name Records (PNRs)

Since 9/11, so-called passenger name records (PNR) have been the subject of controversies.[279] A PNR can be defined as a record of the itinerary of a travelling person saved in the database of an airline, usually during the booking process. After 9/11, US authorities unilaterally decided to demand access to PNR data on all passengers travelling to and from the US (bilateral agreements between the US and the EU are discussed below). Similar to the intentions of the TIA, in 2003 the US Department of Homeland Security proposed to implement CAPPS II (computer assisted passenger pre-screening system II), a law that was supposed to allow the profiling of passengers flying into, through or within the US in order to detect suspected terrorists within passengers. CAPPS II was developed for the purpose of keeping terrorists and criminals from boarding commercial flights by using data mining tools which search through PNRs and raise an alert if a suspect from a "no fly" list is detected. Commercial and public databases would be matched with the PNRs. The CAPPS II program has actually never been deployed or field-tested,[280] but would have allowed, like TIA, US law enforcement agencies to retrieve all passenger related information collected by airline companies.

Though CAPPS II has never been deployed, flying into, over, within or out of the US today requires the provision of different kinds of personal data. For instance, with the Secure Flight Program, which is sometimes labelled as the successor to CAPPS II, the Transportation Security Administration (TSA) launched a program that requires the name, date of birth and gender of the traveller 72 hours before a flight. The data is compared to "no fly" and

[279] Bigo, Didier, Sergio Carrera, Gloria González Fuster, et al., "Towards a New EU Legal Framework for Data Protection and Privacy", European Parliament, Brussels, 2011.
[280] Singel, Ryan, "Life After Death for CAPPS II?", *Wired*, 16 July 2004.

"selectee" lists and if a match occurs, the passenger might not be allowed to fly. Furthermore, in order to get a permission to travel to the US, travellers from the Visa Waiver Program countries[281] have to go through a pre-screening process based on the Electronic System for Travel Authorization (ESTA) since 2009. The given information is matched with lists of wanted persons, and possibly the travel authorisation is denied. Also, with installation of the automated Advance Passenger Information System (APIS), since 2005, US agencies require name, biometric data, date of birth, ID number, nationality and gender of passengers before they fly to the US.

Further aviation security measures

In addition to the measures put in place for the purpose of preventing terrorist attacks, crime and illegal immigration, two additional surveillance technologies began to play an important role for aviation security policy, namely, full body scanners and biometrics. The US Transportation Security Administration (TSA) started to deploy full body scanners, or as the TSA euphemistically calls it, advanced imaging technology (AIT), in 2007. The two main body scanner technologies in place are millimetre wave and backscatter. According to the TSA, in 2012, there are approximately 700 units installed at more than 180 US airports.[282] Those body scanners are able to distinguish between the chemical components of a human body and other substances to detect when an individual is carrying concealed weapons.

The situation in the EU is as follows: Discussions and public consultations on the issue of body scanners were held in 2008 and 2009. But when an attempted terrorist attack with hidden explosives at Amsterdam's Schiphol airport in 2009 showed the limits of metal detectors, the policy-making processes about the possible deployment of body scanners sped up.[283] After the European Commission tried to introduce the use of body scanners, the European Parliament objected to their use and raised serious privacy concerns, since body scanner are machines "producing scanned images of persons as if they were naked, equivalent to a virtual strip search".[284] In November 2011, an agreement was found and under several restrictions, EU airports are allowed to implement body scanners. For instance, one restriction is that the passenger has the right to refuse the body scan.[285]

Another measure expected to increase security is the implementation of biometric identification documents. Since 2006, the US government requests passports that contain biometric features for those who want to travel visa-free to the US within the Visa Waiver program.[286] The US also introduced biometric passports, based on the Enhanced Border

[281] The Visa Waiver Program (VWP) enables nationals of 37 participating countries to travel to the United States for tourism or business for stays of 90 days or less without obtaining a visa. See US Department of State, "Visa Waiver Program (VWP)", Washington, D.C., last upated 2 October 2012. http://travel.state.gov/visa/temp/without/without_1990.html#vwp

[282] Transportation Security Administration, "Advanced Imaging Technology (AIT)", last upated 11 October 2012. http://www.tsa.gov/traveler-information/advanced-imaging-technology-ait

[283] European Union Agency for Fundamental Rights, "The Use of Body Scanners: 10 Questions and Answers", Vienna, 2010.

[284] European Parliament, "Resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection", B6-0562/2008, Strasbourg, 2008.

[285] "Commission implementing regulation (EU) No 1147/2011 of 11 November 2011 amending Regulation (EU) No 185/2010 implementing the common basic standards on civil aviation security as regards the use of security scanners at EU airport", Official Journal of the European Union L 294, Vol. 54, 12.11.2011, pp. 7-11.

[286] Kurz, Constanze, and Frank Rieger, Die Datenfresser: Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen, S. Fischer, Frankfurt am Main, 2011.

Security and Visa Entry Reform Act of 2002.[287] The EU introduced biometric passports in 2004, when the European Commission specified technicalities, which are binding for the Schengen agreement members.[288] Most of the participating countries decided to introduce passports with biometric photos that allow facial recognition; some countries additionally record fingerprints. Those passports contain RFID chips, on which the personal information is stored, allowing an automatic readout of information.[289]

2.5.3.2 EU response to 9/11

The EU initiated several programs and policy initiatives in order to facilitate the prevention of terrorist attacks as well. On the one hand, the EU reacted to the US pressing ahead with various counter-terrorist initiatives, some of which were of questionable legitimacy. But on the other hand, Europe also experienced severe terrorist attacks, such as that in Madrid in 2004 and London in 2005, which had an impact on the EU's sense of security and surveillance measures.

EU counter-terrorism strategy

For the purpose of contributing to global security, the EU and the United Nations (UN) established a counter-terrorism strategy in 2005, which is based on prevention, protection, pursuit and response.[290] This strategy is broken down into detailed action plans, where all the measures for the implementation of the strategy are listed.[291] The first pillar, prevention, "aims to combat radicalisation and recruitment of terrorists by identifying the methods, propaganda and the instruments used by terrorists".[292] In practice, the EU offers a framework that helps to co-ordinate national policies and supports research, facilitates sharing best practice cases and promotes good governance. The second pillar, protection, aims to "reduce the vulnerability of targets to attack and to limit the resulting impact of attack".[293] Concrete measures are the Schengen Information System II (SIS II), the Visa Information System (VIS) and the FRONTEX agency. In addition to border security, where biometrics plays a crucial role, the protection of critical infrastructure, e.g., cyberspace, is a key priority as well. The third pillar, pursuit, aims "to pursue terrorists across borders, while respecting human rights and international law".[294] In this context, it is proposed to prioritise the strengthening of national capabilities to combat terrorism, to make full use of Europol and Eurojust, and to

[287] US Department of State, "Enhanced Border Security and Visa Entry Reform Act of 2002 ALDAC No.1", Washington, D.C., May 2002. http://travel.state.gov/visa/laws/telegrams/telegrams_1403.html
[288] "Council Regulation (EC) 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States", Official Journal of the European Union L 385, Vol. 47, 29.12.2004, pp. 1-6; "Commission Decision C(2005) 409 of 28 February 2005 establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States (Decision not published)", 28.2.2005; "Commission Decision C(2006) 2909 of 28 June 2006 establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States (Decision not published)", 28.6.2006.
[289] Ström, Pär, *Die Überwachungsmafia: Das lukrative Geschäft mit unseren Daten*, Heyne, München, 2005.
[290] European Commission, DG Home Affairs, "Counter-Terrorism Strategy", last upated 7 December 2011. http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33275_en.htm
[291] Council of the European Union, "Note on the EU Action Plan on combating terrorism", Doc. 7233/1/07 REV 1, Brussels, 2007.
[292] Council of the European Union, "Note on the European Counter-Terrorism Strategy", Doc. 14469/4/05 REV 4, Brussels, 2005.
[293] Ibid.
[294] Ibid.

tackle terrorist financing. Finally, the fourth pillar, response, deals with the resources and assets that could be mobilised by Member States in the case of a terrorist attack.

Passenger Name Records (PNRs)

As stated above, US authorities requested the transmission of personal data of EU citizens travelling to the US, including name, address, birth date, date of ticket reservation, travel agency used, financial data, information on the traveller's previous flights, ethnic group and place of work.[295] The EU Data Protection Directive does not foresee a transmission of personal data to third countries where the level of data protection is lower. Nevertheless, airline companies from EU countries have had to comply and deliver the requested information. As a result, the US and EU negotiated PNR agreements since 2004. In 2004, the first EU-US PNR Agreement was adopted, but was annulled by the European Court of Justice in 2006.[296] Renegotiations followed with the US, but also with Australia and Canada. In 2012, an EU-US PNR agreement, which was provisionally applied in 2007, was adopted. The goal of this agreement[297] is "to set a legal framework for the transfer of Passenger Name Records (PNR) data by carriers operating passenger flights between the European Union and the United States to the US Department of Homeland Security (DHS) and the subsequent use of that data by the US DHS".[298]

The main aspects of the EU-US agreement are as follows:[299]

- a strict purpose limitation, the use of PNR data being limited to the prevention, detection, investigation and prosecution of terrorist offences or transnational crime;
- a legally binding commitment from the US Department of Homeland Security to inform the Member States and EU authorities of any EU relevant intelligence leads flowing from the analysis of these PNR data;
- a robust data protection regime with strong data security and integrity requirements;
- rights of access, rectification and erasure and the possibility to obtain administrative and judicial redress;
- a limited usage of PNR data for a period of 10 years for transnational crime and 15 years for terrorism. After six months, personally identifiable information of PNR data will be masked out and after five years, PNR data will be moved to a dormant database with additional controls.

While the agreement between Australia and the EU has already been concluded in 2011,[300] the negotiations between Canada and the EU are still ongoing.

EU Terrorist Finance Tracking Programme

[295] Maghiros, et al., 2003.
[296] European Court of Justice, "Judgment of the Court (Third Chamber) of 1 June 2006 in Joined Cases C-442/03 P and C-471/03 P", 2006.
[297] "Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security", Official Journal of the European Union L 215, Vol. 55, 11.8.2012, pp. 5-14.
[298] Council of the European Union, "Council adopts new EU-US agreement on Passenger Name Records (PNR)", Press Release, Luxembourg, 2012.
[299] Ibid.
[300] European Council, Decision of 22 September 2011 on the signing, on behalf of the Union, of the Agreement between the European Union and Australia on the processing and transfer of passenger name record (PNR) data by air carriers to the Australian Customs and Border Protection Service, Official Journal of the European Union L186, Vol. 55, 14.07.2012, pp. 4-15.

As it was the case for PNR, the US decision about a Terrorist Finance Tracking Programme (TFTP) demanded an EU reaction. The US Department of Treasury introduced TFTP as an instrument that allows access to databases of bank transfers of financial transactions of suspected terrorists. US authorities gained access to data from the Belgium-based company SWIFT (Society for Worldwide Interbank Financial Telecommunication), and an EU-US agreement on TFTP became necessary when the question came up under which conditions the TFTP would have access to EU-originating financial data. Serious concerns about the compliance with data protection and privacy issues made US-EU negotiations necessary, which lead to the final agreement EI-US TFTP in 2010.[301] This agreement allows sending a bulk of data to US authorities after Europol, the EU law enforcement agency, has assessed the compliance of the request with the agreement.

The negotiations between the EU and the US have stimulated discussions within the EU Member States about the extraction of data within EU territory. Thus, the interest of the EU Member States in such financial data tracking was expressed in a Communication of the European Commission in 2011.[302] Nevertheless, a couple of questions are still open in relation to such an EU agreement, e.g., about the necessity of such a system or the impact of an EU TFTS (Terrorist Finance Tracking System) on the EU-US TFTP agreement.[303]

Prüm Treaty

The Prüm Treaty was signed in 2005 by the seven EU Member States of Austria, Belgium, France, Germany, Luxembourg, the Netherlands and Spain and constitutes an agreement between the signatories, which concerns the exchange of data concerning DNA files, fingerprints and vehicle registration. As stated in the preamble, the Treaty aims "to play a pioneering role in establishing the highest possible standard of cooperation especially by means of exchange of information, particularly in combating terrorism, cross-border crime and illegal migration". [304]

The Prüm decisions represent an intergovernmental form of co-operation between the EU Member States, which are asked to implement the Council decision into their national law. Meanwhile, a couple of other Member States have signed the contracts, and others have expressed interest in joining the agreement. The Prüm system is based on national contact points, which are allowed to perform automated searches on DNA profiles and to compare DNA samples within a national database with the databases of other countries. For the purpose of guaranteeing anonymity, the data exchange is based on a hit-/no-hit principle, which means that in case of a hit, the contact point receives confirmation but no information about the DNA sample. This information needs to be requested from the responsible authority. Concerning fingerprints, an agreement between Austria, Germany and Luxembourg exists, which allows the countries access to each other's fingerprint databases. Finally, the

[301] European Council, Decision of 28 June 2010 on the signing, on behalf of the Union, of the Agreement between the European Union and the United States of America on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program, Official Journal of the European Union L195, Vol. 53, 27.7.2010, pp. 1-2.
[302] European Commission, A European terrorist finance tracking system: available options, COM(2011) 429 final, Brussels, 2011.
[303] Hernanz, Nicholas, and Sergio Carrera, "More Surveillance, More Security? The Landscape of Surveillance in Europe and Challenges to Data Protection and Privacy – Policy Report on the Proceedings of a Conference at the European Parliament", Deliverable 6.4, SAPIENT Project, 2012.
[304] Council of the European Union, "Note on the Prüm Convention", Doc. 10900/05, Brussels, 2005.

Prüm Treaty also includes a provision on the automated searching of vehicle registration data.[305]

EU Data Retention Directive

The first discussions at EU level about the retention of telecommunications data took place in 2002. Back then, the possibilities of Member States of obliging communication providers to store the data and provide it for law enforcement purposes were discussed and put into a directive.[306] As a result of serious concerns about conformity with the European Convention on Human Rights and differences between the Council, the Commission and the Parliament about jurisdiction, the Data Retention Directive was finally approved.[307] Core aspects of the Directive are the obligation for communication providers to store telecommunications data (telephone, e-mail, IP addresses) for at least six months up to a maximum of 24 months for law enforcement and counter-terrorism purposes. In a 2011 evaluation of the Data Retention Directive, the study authors came to the conclusion that several national constitutional courts had annulled the legal instruments and criticised the non-compliance with fundamental rights.[308] Therefore, the European Commission announced a future proposal with amendments to the Directive of 2006 to be released in 2013.

2.6 CONCLUSIONS

In this chapter we have shown that surveillance is (and has always been) a normal element of modern society. Registering and identifying citizens started in the 18th century and was an important prerequisite for a modern centralised government. The data was necessary for taxation, provision of public infrastructure and the modern welfare state. In the 19th and early 20th century surveillance became an important element in the division of labour in industrialism. In the post-industrial age of information surveillance has become a lubricant of the information society. Moreover in times of increasing risks and uncertainties surveillance is the prerequisite for systematic planning in governments and enterprises. In this respect surveillance is a useful tool for the management of industrial and post-industrial societies. However, "the belief that ever more surveillance can overcome the incompleteness of information or the partiality of abstraction is a dangerous delusion."[309]

Most of the examples from the different periods in time show that each useful application of surveillance also bears the danger of totalitarism. Information and their use create an even greater need for more information for even more beneficial purposes. The naïve thinking that those "who have nothing to hide, have nothing to fear" and that people "would be happy to

[305] Luif, Paul, "The Treaty of Prüm: A Replay of Schengen", Deliverable 38c, EU-CONSENT Network of Excellence, 2007.
[306] European Parliament and the Council, Directive 2002/58/EC o of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)", Official Journal of the European Communities L 201, Vol. 45, 31 July 2002, pp. 37-47.
[307] European Parliament and the Council, Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal of the European Union L 105, Vol. 49, 15 March 2006, pp. 54-63.
[308] European Commission, Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC), COM(2011) 225 final, Brussels, 2011.
[309] Lipartito, Kenneth, "The Economy of Surveillance", February 10, 2010.

give up a little privacy in return for more convenience, security"finally leads to a situation where the abuse potential exceeds the real or perceived benefits. Moreover in today's world, it is an illusion to think that one can erase personal information that was once stored in a networked system.

In terms of the dynamics that have shaped the development of surveillance in today's democratic states, the picture is quite diverse and offers room for interpretation in the different periods we investigated. The post World War II and Cold War era was characterised by scientific enthusiasm, where scientific developments were pushed in general, and technologies prone to be used for surveillance purposes were affected as well. One could even say that in this period, especially surveillance technologies played an important role for, in the first place, national defence purposes, for the ECHELON system, GPS or the Internet, which had been supported by US military research. Other periods though, especially in the post-9/11 era, tend to be characterised by a stronger focus on policy initiatives, in the case of 9/11 as a reaction to a special event. Another observation that might be made is that the enhanced technological possibilities to collect, store and process data fuelled surveillance practices. This was seen in the case of the proliferation of databases and computers, and in connection with the commercialisation of the Internet.

Nevertheless, there is no one-way causal relationship between the development of technologies and their application for surveillance purposes – but instead complex context-dependent social, political, historical and technological dynamics which interact and shape surveillance practices. The development of technologies financed by state agencies have gradually shifted from military to civil use. Policy reactions to real or perceived internal or external threats, broader developments affecting society as a whole (such as increased risks in a globalised world and the proliferation of information and communication technologies), the rise of consumer capitalism and changes in the willingness of individuals to share personal information, all play a role in the co-evolutionary development of surveillance technologies and surveillance practices.

Apart from these general observations, there are numerous open questions about the usefulness and effectiveness of surveillance technologies and about possible rebound effects. Especially surveillance measures to fight terrorisms and organised crime have been introduced without knowledge about their effectiveness and negative side effects (topics such as false positive matches, the inversion of the presumption of innocence, costs of intensified security checks). Especially important, and still debated, is the question about what impact an increasing amount of surveillance is having on an open society, if it does not in the end produce more suspicion than trust. Counter movements, however, show that citizens are not always willing to follow the rationale of government agencies and industry. On the other hand, as the case of surveillance cameras has shown, citizens slowly get used to these measures.

Another important trend that can be observed in the history of modern surveillance is that of gradual function creep in different directions. The case of dragnet investigation in Germany shows how an instrument that was originally intended for analysing and fighting the societal root of criminality turned into a law enforcement tool that was finally perceived as being oppressive. In recent years, one could observe the trend that technologies that had been introduced to reduce crime are addressing anti-social and undesirable behaviour and becoming instrumental for community development. Very much related to this trend is the role that surveillance is playing in law enforcement and its shift from identifying offenders to

preventing crime which implies that the presumption of innocence is no longer the normal case but that all citizens are becoming suspects.[310]

[310] Huster, Stefan and Karsten Rudolph (eds.), Vom Rechtsstaat zum Präventionsstaat, Suhrkamp, Frankfurt am Main, 2008.

3 THE SURVEILLANCE INDUSTRY IN EUROPE

Rowena Rodrigues, Trilateral Research & Consulting

3.1 INTRODUCTION

The main objective of this task is to identify and characterise the surveillance industry in Europe. For the purposes of this task, we define the surveillance industry (in a broad manner) as referring to all of the actors involved in the commercial production, trade and/or offering of surveillance products and services (or products and services that satisfy surveillance needs). Our work comprises several elements as follows:

First, we discuss surveillance markets based on desktop research of open data on the subject. We look at surveillance areas such as biometrics, deep packet inspection, smart cards, RFID, smart homes, unmanned aerial systems, x-ray security screening and video surveillance. We profile surveillance customers, and discuss the drivers and inhibitors of markets.

Second, using desktop research, we surveyed the security and allied industries and identified the companies engaged in the business of surveillance in Europe. Since it was impossible to examine all identified companies within the task's limited time frame, we selected a sample of 39 companies for detailed analysis to help us characterise the European surveillance industry. Based on both these studies, we outline the motivations, main offerings and features of the surveillance industry. We also look at the controversies that affect the industry.

Third, we examine the surveillance industry's market prospects and competition. We outline the future market prospects and growth areas and trends, and discuss competition and challenges for the future.

Fourth, we identify industry associations which are highly influential entities in the surveillance and security industry. We look at their nature and role, activities and effect upon the industry.

Fifth, we delve into the impact of the surveillance industry on security policy and research, by examining their participation in influential international security organisations, the intersections and liaisons with national security organisations and intelligence agencies, their lobbying actions and involvement in EU security research projects.

Sixth, we look at the surveillance industry and fundamental rights – we try to determine the attitude of the industry to human rights concerns, highlight some actions and good practices.

Finally, we study the watchers of the surveillance industry, i.e., the entities monitoring the surveillance industry, including government, civil society organisations, media and academia. We examine key organisations, their monitoring motivations, actions taken, effects upon industry and effectiveness.

3.2 SURVEILLANCE MARKETS

The surveillance market is on one hand a sub-set of the security market and on the other an independent entity by itself (e.g., surveillance also has non-security applications). We need to first understand this market which is a patchwork cutting across different sectors. To this effect, we will examine some figures for different surveillance solutions (such as biometrics, deep packet inspection, smart cards, RFID, smart homes, unmanned aerial vehicles, x-ray security screening and video surveillance),[1] customers and clients of the industry, and drivers and inhibitors of the market.

This section collates information on different surveillance solutions and discusses surveillance markets based on our desktop research of open data on the subject.[2] Dimensioning the industry is a challenge. Many independent market reports are expensive and not easily accessible. Additionally, the surveillance industry is a patchwork of many sectors, which makes it difficult to obtain harmonised figures.

Note: Figures in this report stay true to the original sources and therefore might be expressed either in dollars, euros or pounds.

3.2.1 Market data

The global surveillance industry is developing at a rapid pace. The scale of the industry is subject to varying estimates. According to the G4S annual report of 2011, "the "business to business" and "business to government" global security market is estimated to generate revenues of around £90 billion per annum.[3] Privacy International suggests it is worth "$5 billion a year".[4] Though Synetics does not give figures, it provides the following market overview: [5]

> The electronic security and surveillance market is large, growing and in the process of fundamental structural change. Advances in technology have allowed digital recording, transmission, storage and networking of high resolution real-time video images to become economically viable in mainstream surveillance applications. This shift to digital technology will continue, creating substantial opportunities and threats within the rapidly changing competitive order of security systems and equipment suppliers.

Further, Quadnetics/Synectics postulates that:

- the market for standard hardware products will continue to commoditise;
- the market opportunity for specialised hardware products will grow and is likely to be sustainable
- the market opportunity for software will grow and is likely to be sustainable;

[1] These solutions are presented on the basis of data availability.
[2] The sources checked include: media reports, annual reports of companies, industry association publications, security reports and forecasts, government databases, independent research organisations, research projects (e.g., Big Brother Inc).
[3] G4S plc, Annual Report and Accounts 2011. http://www.g4s.com/en/Investors/2011%20Annual%20Report/
[4] Privacy International, Big Brother Inc. https://www.privacyinternational.org/projects/big-brother-inc
[5] Synectics. Vision, Mission and Strategy.
http://www.synecticsplc.com/About_Us/Vision~_Mission_and_Strategy/default.aspx?id=276

- security systems integrators will continue to consolidate, becoming bigger, more diverse and more global;
- information technology companies will seek and gain an increasing share of the security market;
- high integrity digital video surveillance is still sufficiently complex and demanding that it is unlikely to become simply a sub-set of the IT industry, at least not for many years;
- certain specialist customer applications requirements are likely to diverge increasingly from mainstream high volume market offerings. [6]

In the paragraphs that follow, we cite figures for some segments of the surveillance market. This gives us a picture of the (increasing) worth of the surveillance industry and of the overall market trends. It also helps us understand why security and other companies are increasingly allocating resources and diversifying into the surveillance business.

Biometrics

Visiongain (a UK-based independent business information provider for the telecoms, pharmaceutical, defence, energy and metals industries) suggests that "biometric technology systems are increasingly vital components for the digital age" and values the global biometrics market in 2012 at $7.59 billion.[7]

Deep packet inspection

The Infonetics (an international market research and consulting company) research report[8] on Service Provider Deep Packet Inspection (DPI) Products (which looks at standalone DPI vendors and solutions for wireless and fixed line networks) makes the following observations of the DPI market:[9]

- Service provider deep packet inspection (DPI) product revenue grew 29% to over $470 million worldwide in 2011.
- The service provider DPI market will grow to $2 billion in 2016, with thebulk of the growth coming from the mobile space.
- Huawei led the global service provider DPI revenue share in 2011 ahead of Sandvine.
- DPI is increasingly being incorporated into larger solutions, such as video optimisation and mobile offload, creating opportunities for suppliers that offer DPI technology on an OEM basis
- Operators are evaluating alternatives to throttling or blocking high-bandwidth video content, including using DPI for media caching, to prioritize select video content to support guaranteed quality of service (QoS) and as part of a content delivery network strategy.
- Strong growth continues for service provider DPI products in emerging markets in the Asia Pacific, the Middle East and Africa as operators look to address network congestion caused by

[6] Quadnetics. Vision, Mission and Strategy.
http://www.quadnetics.com/About_Us/Vision~_Mission_and_Strategy/default.aspx?id=276
[7] Visiongain, *The Biometrics Market 2012-2022*,19 September 2012.
http://www.visiongain.com/Report/898/The-Biometrics-Market-2012-2022
[8] This biannual report studies market size, vendor market share, forecasts, and in-depth analysis and trends for standalone deep packet inspection products used in wireless and fixed-line service provider networks. It tracks companies such as Allot, Arbor, Cisco, CloudShield, Huawei, ipoque, Procera, Qosmos, Sandvine and others in North America, EMEA (Europe, the Middle East, Africa), Asia Pacific, and CALA (Caribbean and Latin America).
[9] Infonetics Research, Deep packet inspection (DPI) market a $2 billion opportunity by 2016, 23 April 2012. http://www.infonetics.com/pr/2012/2H11-Service-Provider-DPI-Products-Market-Highlights.asp

rapid subscriber growth, comply with regulatory requirements and support cybersecurity initiatives.

Smart cards

Eurosmart, the smart security industry association, provides information on the smart secure devices market. According to it, more than 7 billion smart secure devices will be shipped in 2012.[10] The following tables show figures for global smart cards shipments in 2011 and forecast for 2012:

Worldwide Smart Secure Device shipment - 2011 and 2012 forecasts
Millions of Units (Mu)
(General Assembly, Brussels, April 25 2012)

	2011	2012 forecast	2012 vs 2011 % growth
Telecom	4 700	5 200	11%
Financial services	1 050	1 260	20%
Government - Healthcare	240	300	25%
Transport	100	120	20%
Pay TV	125	135	8%
Others	80	90	13%
Total	6 295	7 105	13%

Fig: Worldwide smart secure device shipment – 2011 and 2012 forecasts

Worldwide Smart Secure Contactless market figures – 2011 and 2012 forecasts
Millions of Units (Mu)
(General Assembly, Brussels, April 25 2012)

	2011	2012 forecast	2012 vs 2011 % growth
Financial services	200	260	30%
Government - Healthcare	130	170	31%
Transport	100	120	20%
Others	50	60	20%
Total	480	610	27%

Fig: Worldwide smart secure contactless market figures – 2011 and 2012 forecasts

[10] Eurosmart, Figures. http://www.eurosmart.com/index.php/publications/market-overview.html

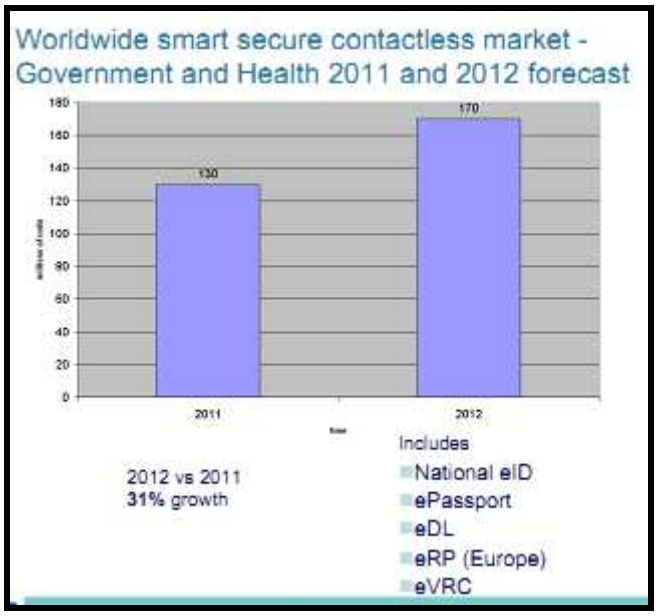


Fig 3: Worldwide smart secure contactless market – Government and Health 2011 and 2012 forecast

The 2011 International Card Manufacturers Association (ICMA) Global Card Market Statistics Report valued the global card market at $17 billion in 2011 (an increase of nearly 14% from 2010).[11] The report says that Europe is the third largest producer with 5 billion units (cards) manufactured in 2011.[12]

RFID

Europe is one of the leaders of RFID technology.[13] In terms of global market share in the RFID business, it ranks second to the US.[14] A report by IDTechEx (a UK-based independent market research company) pegs the value of the entire RFID market (passive and active RFID tags, readers, software, services) at $7.67 billion in 2012 (as compared to $6.51 billion in 2011).[15] Another report pegged the revenue generated by the global chipless RFID market at $1,087 million in 2011 and expected to reach $ 3,925 million in 2016.[16]

Smart homes

The global smart homes market was worth $5,325 million in 2010 and is forecast to increase to $11,000 million in 2015.[17] Europe is the second largest market for smart home technology.

---

[11] ICMA, "Global Card Market Reaches $17 Billion In 2011, Up Nearly 14% From 2010", *Smart Card Trends*, 22 June 2012. http://www.smartcardstrends.com/det_atc.php?idu=16779

[12] Ibid.

[13] FhG IML, *RACE networkRFID, D2.1 – Market analysis consumption report*, 1 March 2009. http://www.rfidineurope.eu/sites/default/files/RACE_deliverable_D2.1.pdf

[14] http://www.marketsandmarkets.com/Market-Reports/chipless-rfid-market-forecasts-793.html

[15] Harrop, Dr Peter, and Raghu Das, RFID Forecasts, Players and Opportunities 2012-2022, June 2012. http://www.idtechex.com/research/reports/rfid-forecasts-players-and-opportunities-2012-2022-000322.asp

[16] Marketsandmarkets.com, *Global Chipless RFID Market* (2011 - 2016) - Forecasts by Products (Tag, Reader, Middleware), Applications (Retail, Supply Chain, Aviation, Healthcare, Smart Card, Public Transit), July 2012. http://www.marketsandmarkets.com/Market-Reports/chipless-rfid-market-forecasts-793.html

[17] Marketsandmarkets.com, *Global Smart Homes Market (2010 – 2015)*, Report Code: SE 1084, April 2011. http://www.marketsandmarkets.com/Market-Reports/smart-homes-and-assisted-living-advanced-technologie-and-global-market-121.html. This report categorises the global market for smart homes on the basis of applications (such as in security, lighting controllers, HVAC, energy management, entertainment, home health, and others) and geography; forecasts revenues and analyses trends.

Unmanned aerial vehicles

According to a market study by the Teal Group, current worldwide unmanned aerial vehicle (UAV) expenditures are US$6.6 billion annually.[18]

Unmanned ground vehicles

Visiongain determined that the global unmanned ground vehicles (UGV) market was worth $651.5 million in 2012.[19] The report names the following 12 as "leading national markets" – US, Israel, UK, Germany, China, Singapore, South Korea, Australia, France, Canada, India and Italy.

X-ray security screening

Homeland Security Research valued the global X-ray security screening (conventional, backscatter, multi-view, coherent and dual energy x-ray) market (including systems sales, service, and upgrades) at $1.2 billion in 2011.[20]

Video surveillance

An IMS Research report suggests that the video surveillance (surveillance cameras, recording equipment and video encoders) market was worth $10.5 billion in 2011 and expected to grow to US $20.5 billion by 2016.[21] Another report suggests that the IP video market (IPVM) globally for 2011 was worth more than US $200 million and growing at an annual rate of more than 25%.[22]

A Visiongain report values the global military video surveillance systems market at US$8.81 billion in 2012.[23]

The various market figures outlined above support the contention that the surveillance industry is developing at a steady if not rapid pace. The worth of the surveillance industry is going up driven by the increased demand for surveillance solutions. Security companies want to capitalise on this boom and are increasingly expanding and diversifying their surveillance portfolios.

---

[18] Teal Group, *World Unmanned Aerial Vehicle Systems, Market Profile and Forecast 2012*. http://tealgroup.com/index.php/about-teal/teal-group-in-the-media/3/79-teal-group-predicts-worldwide-uav-market-will-total-89-billion-in-its-2012-uav-market-profile-and-forecast. This study "examines the worldwide requirements for UAVs, including UAV payloads and companies, and provides ten-year forecasts by country, region, and classes of UAVs."

[19] Visiongain, *The Unmanned Ground Vehicles (UGV) Market 2012-2022*, 10 August 2012. http://www.visiongain.com/Report/870/The-Unmanned-Ground-Vehicles-(UGV)-Market-2012-2022

[20] Homeland Security Research, *X-Ray Security Screening: Technologies & Global Market Outlook – 2012 Edition*, 2012. http://www.homelandsecurityresearch.com/2012/05/x-ray-security-screening-technologies-global-market-outlook-2012-edition/

[21] Axis Communications, Strengthen the position on the security market. http://www.axis.com/corporate/security_market.htm

[22] Major, Marty, "Online Surveillance Market 2011" 6 March 2011. http://ipvm.com/report/online_surveillance_sales_2011

[23] Visiongain, The Military Video Surveillance Systems Market 2012-2022: Full Motion Video for ISR, 16 April 2012. http://www.marketresearch.com/Visiongain-v1531/Military-Video-Surveillance-Systems-Full-6917014/

3.2.2 Surveillance customers

To get a complete picture of the surveillance market, we next identify the various surveillance industry's customers and clients. Whose needs is the surveillance industry catering to? What is the nature of these customers and clients?

Government and its agencies (public sector)

The government (and its myriad agencies) is the largest, most important, influential buyer of surveillance technologies. The government uses surveillance technologies for various purposes ranging from (the broadly defined) national security, public order, preventing and deterring crime, health and safety, protection of critical and strategic infrastructures and locations, social control, determination of benefits and fraud prevention.

The UK House of Lords report on *Surveillance: Citizens and the State* summarises the impetus for surveillance and data use:

> National security, public safety, the prevention and detection of crime, and the control of borders are among the most powerful forces behind the use of a wide range of surveillance techniques and the collection and analysis of large quantities of personal data.[24]

Video military surveillance systems are used by European Union bodies, national air forces, armies, navy, departments and ministries of defence, defence procurement agencies, and police services.[25] Many local authorities invest large budgets in CCTV surveillance solutions as indicated in the following table which shows how much local authorities and councils in the UK spend on CCTV surveillance.

Highest spenders on CCTV (2007-2011)4

	Local Authority	Number of CCTV cameras	Total cost
1	Birmingham	636	£14,293,060.00
2	Westminster	153	£11,831,554.00
3	Leeds	253	£8,762,292.00
4	City of Edinburgh	232	£6,211,425.30
5	Croydon	84	£5,329,589.00
6	Enfield	169	£4,996,900.00
7	Cambridge	141	£4,973,984.00
8	Wandsworth	1158	£4,711,080.14
9	Leicester	2083	£4,762,729.94
10	Barnet	141	£4,690,742.29
11	Nottingham	1120	£4,666,827.83
12	Hounslow	Unstated	£4,597,163.37
13	Knowsley	548	£4,558,481.51
14	Barking and Dagenham	115	£4,518,500.00
15	Bristol, City of	786	£4,220,268.85
16	Caerphilly	146	£4,111,747.00
17	Wakefield	177	£4,110,740.00
18	Lambeth	348	£4,099,625.02

Fig: Highest CCTV spenders (2007-2014)[26]

[24] House of Lords Constitution Committee, Surveillance Citizens and the State, 2008. http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1804.htm#a16

[25] http://www.marketresearch.com/Visiongain-v1531/Military-Video-Surveillance-Systems-Full-6917014/

[26] Big Brother Watch, *The Price of Privacy: How local authorities spent £515m on CCTV in four years*, A Big Brother Watch report, February 2012. http://www.bigbrotherwatch.org.uk/home/2012/02/price-privacy-councils-spend-521m.html

The government (and its agencies) are often the primary sources of business for many surveillance companies such as Boeing,[27] BAE Systems Detica (cyber, security software and consulting services) and Northrop Grumman. Others such as Experian "partner" with the "public sector to assist government departments to authenticate benefit claimants and to prevent fraud".[28] In July 2011, the UK HM Revenue & Customs (HMRC) appointed Experian "to help reduce losses due to fraud and error in the payment of tax credits". This is done through the use of web monitoring and other services that monitor relationships between individuals. 3M Cogent provides finger, palm, face and iris biometric systems for governments, law enforcement agencies (alongside private companies). More than 1,000 government agencies buy Guidance Software's EnCase® Forensic software (which permits investigators to acquire digital data and conduct disk level forensic analysis).[29] Neurotechnology's products are used for civil and criminal purposes – border management, criminal investigations, voter registration systems, verification and duplication checking, passport issue.[30]

Industry (private sector)

Industry (or the private sector) is a key buyer of surveillance solutions. Industry or private sector clients range in size (small, medium, large), sector (financial services, telecommunications, utilities, retail, technology, defence, pharmaceuticals, healthcare etc) and geography (local, national, regional or international).

Employers in particular are a major surveillance client. Presenting the findings of research by Gartner, a news report suggests

> Corporations are starting to embrace technologies used to monitor employee Internet use, with 60 per cent expected to watch workers' social media use for security breaches by 2015.[31]

There is a huge range of companies (large and small) offering employee monitoring surveillance solutions – Amplusnet,[32] Cisco, Flyonthewall,[33] Honeywell, Panoptech[34], and SpectorSoft.[35]

Academia

Academia is another significant surveillance client. Schools[36] and universities[37] use surveillance products for a variety of purposes: to monitor behaviour, protect staff and

---

[27] Boeing's primary customer is the United States Department of Defense (accounting for 76% of its 2011 revenues).
[28] Experian plc, Annual Report 2012. http://www.experianplc.com/~/media/Files/E/Experian-V2/pdf/investor/reports/2012/experian-ar-2012.pdf
[29] http://www.guidancesoftware.com/
[30] http://www.neurotechnology.com
[31] Gross, Grant, "More firms will monitor social media use: Gartner", IDG News Service, 29 May 2012. http://www.computerworld.com/s/article/9227556/Gartner_sees_huge_rise_in_corporate_social_media_monitoring
[32] http://www.cyclope-series.com/company/company.html. More than 7,000 worldwide use Amplusnet's Cyclope-Series employee monitoring software. The company has clients in Europe (Romania, Czech Republic, Slovakia, Hungary, Poland, Croatia, Switzerland), India, China, US and Colombia.
[33] http://www.flyonthewall.uk.com
[34] http://www.panoptech.co.uk/
[35] http:// www.spectorsoft.com/
[36] Harris, John, "School surveillance: how big brother spies on pupils", *The Guardian*, 9 June 2011.

students, prevent vandalism, crime and drug use, register and confirm identity and attendance of students, reduce truancy, monitor entitlements and access to services (e.g., library, sports).[38] The surveillance products used include biometrics,[39] CCTV[40] and RFID.

Companies such as BioStore Limited (fingerprint-based ID systems),[41] CCTVanywhere (CCTV products and systems for schools),[42] Classwatch (fixed and mobile video systems)[43], Darnbro (wearable RFID tracking)[44] and MicroLibrarian Systems (biometric fingerprint recognition for libraries) [45] provide specialised surveillance solutions for schools.

Organised crime groups

This is perhaps the most controversial surveillance industry client or customer, one not explicitly recognised as so. However, we must recognise that the surveillance industry, though not intentionally, but incidentally, provides solutions to *non-acceptable* organisations and groups such as criminal gangs and terrorists, that abuse surveillance technologies to the detriment of society. Examples include abuses of data mining technologies, trade in personal information and unauthorised, covert surveillance of political figures or locations.

Media

The media is a surveillance customer. *The News of the World* (owned by the News Corporation) used covert surveillance technologies (phone and Internet hacking tools) to monitor celebrities, sport stars, politicians and victims of crime on a massive scale in the UK.[46]

---

http://www.guardian.co.uk/uk/2011/jun/09/schools-surveillance-spying-on-pupils

[37] See Bickford Smith, Will, "The Surveillance State: Now Even Universities Are At It", 26 May 2011. http://www.bigbrotherwatch.org.uk/home/2011/05/the-surveillance-state-now-even-universities-are-at-it.html; Bingham, John, "Universities to carry out 'police-like' surveillance" 10 November 2008. http://www.telegraph.co.uk/education/universityeducation/3416269/Universities-to-carry-out-police-like-surveillance.html

[38] Monahan, T., and R.D. Torres (eds.), *Schools under Surveillance: Cultures of control in public education*, Rutgers University Press, London, ; Bryce, T.G.K., M. Nellis, A. Corrigan, H. Gallagher, P. Lee and H. Sercombe, "Biometric Surveillance in Schools: Cause for concern or case for curriculum?", *Scottish Educational Review*, Vol. 42, Issue 1, 2010, pp. 3-22.

[39] Bryce, T.G.K., M. Nellis, A Corrigan, H Gallagher, P. Lee and H. Sercombe, "Biometric Surveillance in Schools: Cause for concern or case for curriculum?", *Scottish Educational Review*, Vol. 42, Issue 1, 2010, pp. 3-22.

[40] Hope, A., "CCTV, school surveillance and social control", *British Educational Research Journal*, Vol. 35, No. 6, pp. 891-907.

[41] http://www.biostore.co.uk/

[42] http://www.cctvanywhere.co.uk/

[43] www.classwatch.co.uk/

[44] http://websites.uk-plc.net/Darnbro_Limited/index.htm

[45] http://www.microlib.co.uk/

[46] See BBC News, Phone-hacking scandal: Timeline. http://www.bbc.co.uk/news/uk-14124020. *The News of the World* closed after 168 years of publication; the London Metropolitan Police have arrested 74 people and charged seven journalists and one private investigator for phone hacking. See also House of Commons Culture, Media and Sport Committee, *News International and Phone-hacking, Eleventh Report of Session 2010-12*, Volume 1, HC 903-I, House of Commons, 30 April 2012. http://www.publications.parliament.uk/pa/cm201012/cmselect/cmcumeds/903/903i.pdf

Individuals

Individuals are surveillance customers and buy a range of surveillance solutions ranging from location-based products and services (such as those provided by Lok8U[47]), personal and asset tracking devices for individuals (such as offered by BlueSkyTracking[48]), access and security controls for home and assets (e.g., CCTV cameras, equipment and security systems offered by IView Cameras[49]), and parental control software solutions for the Internet (e.g., NetNanny).[50]

Thus, in summary, we see how the surveillance industry caters to all types of clients: government and its agencies, the private sector, academia, undesirable organisations and groups, media and individuals. Each of these clients employs surveillance solutions for different purposes. The government uses surveillance for national security, crime and terrorism control; the private sector and academia uses surveillance to protect people and assets, non-acceptable organisations and groups, media and individuals uses surveillance technologies to commit crime and terrorism, the media uses surveillance technologies in investigations, individuals use surveillance solutions to safeguard their person, family and/ or property.

3.2.3 Drivers and inhibitors

This section looks at the drivers and inhibitors that affect the surveillance industry. It provides an insight and understanding into what factors influence or have the potential to influence the surveillance industry and what factors can restrict or challenge its growth and development.

Drivers of the surveillance industry

Legislation

Surveillance-friendly legislation drives the demand and supply of surveillance products and services. Economic incentives embedded in legislation drive surveillance solutions. The booming market in lawful interception is a case in point. Many security and surveillance companies specialise in lawful interception services – Aqsacom (France), ELAMAN GmbH (Germany), IPS SpA (subsidiary of the RESI Group, Italy), and Utimaco Safeware AG (member of the Sophos group, Germany).

Policy

A pro-surveillance policy boosts the demand for and supply of surveillance technologies. One example that illustrates this is the pro-drones policy supported by the European Commission. A working paper released by the Commission[51] sees an "emerging market of innovative aerial services" or Remotely Piloted Aircraft Systems[52] and highlights that

[47] http://www.lok8u.com/
[48] http://www.blueskytracking.com/
[49] http://www.iviewcameras.co.uk
[50] http://www.netnanny.com/
[51] European Commission, Towards a European strategy for the development of Remotely Piloted Aircraft Systems (RPAS), Commission Staff Working Document, 6 September 2012. http://register.consilium.europa.eu/pdf/en/12/st13/st13438.en12.pdf
[52] Used synonymously for Unmanned Aircraft System (UAS) in line with ICAO.

> The expansion of this new market will not only support growth and create highly qualified jobs in the industry producing the RPAS or developing the applications; it will also foster the emergence of a totally new service industry offering RPAS operations and aerial work to commercial and state customers.
> …To reap the full benefits of this new technology for growth and jobs, Europe should remove, in a coordinated way, the existing barriers and support the internal market for civil RPAS services. [53]

The document further calls for a strategy with concrete steps to "foster the development of civil RPAS applications in Europe, including through regulatory, R&D and complementary initiatives, leading to the insertion of RPAS into non-segregated airspace". [54]

In 2011, the UK Chancellor George Osborne wanted the UK to be at the forefront of the emerging global market for data analytics[55] – indicative of a pro-data analytics market policy. Further, the Communication Capabilities Development Programme (CCDP) which aims at preserving "the ability of the security, intelligence and law enforcement agencies to obtain communication data and to intercept communications" exemplifies this.[56] The following excerpt from the Queen's Speech to Parliament in 2012 further highlights the position of the UK government: "My government intends to bring forward measures to maintain the ability of the law enforcement and intelligence agencies to access vital communications data under strict safeguards to protect the public, subject to scrutiny of draft clauses."[57] Positive offical views of surveillance – i.e., surveillance as a security and safety asset – are a driver for the public sector surveillance industry. For instance, the UK Home Office believes that communications data[58] is "vital to law enforcement, especially when dealing with organised crime gangs, paedophile rings and terrorist groups".[59]

Research and innovation

Research and innovation in surveillance products and improvements in existing ones are significant market drivers.[60] Experian reports that

> product innovation is a key driver of growth for Experian in all our markets and we have continued to invest strongly in new data sources and new analytical products, together with the platforms that support their worldwide delivery. Over 10% of our revenues come from products developed during just the past five years.[61]

---

[53] European Commission, Towards a European strategy for the development of Remotely Piloted Aircraft Systems (RPAS), Commission Staff Working Document, 6 September 2012. http://register.consilium.europa.eu/pdf/en/12/st13/st13438.en12.pdf

[54] Ibid.

[55] Tyler, Richard, "Chancellor backs UK grab for data analytics market", *The Telegraph*, 16 May 2011. http://www.telegraph.co.uk/finance/yourbusiness/8516366/Chancellor-backs-UK-grab-for-data-analytics-market.html

[56] Ministry of Defence, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, 2010. http://www.direct.gov.uk/sdsr. Further information is available at

[57] *The Guardian*, "Queen's speech 2012 – full text", 9 May 2012. http://www.guardian.co.uk/politics/2012/may/09/queens-speech-2012-full-text

[58] Defined as information about a communication (e.g., the time, duration and dialling numbers of a phone call, location from which a mobile call is made, 'to' and 'from' addresses of an e-mail, location of the originator of the communication).

[59] Home Office, Communications data. http://www.homeoffice.gov.uk/counter-terrorism/communications-data/

[60] Guidance Software, 2011 Annual Report.

[61] Experian, Experian Annual Report, 2012.

Financial support and funding

Financial support and funding for surveillance solutions boosts their supply. This is particularly evident in the case of technologies such as unmanned aerial systems which are receiving increased funding and being rapidly developed and deployed in intelligence, surveillance and reconnaissance applications.[62]

Profits

Profits drive innovation and growth of the surveillance market. Sensing profit opportunities, BAE Systems Detica has invested heavily in cyber and intelligence solutions (for instance, by acquiring L-1 Identity Solutions, Inc.'s Intelligence Services Group (which specialises in security and counter threat capabilities), Norkom Group plc (a provider of innovative anti-money laundering solutions to counter financial crime to the global financial services industry), ETI A/S (a provider of advanced security products and services to government and commercial clients worldwide) and stratsec.net Pty Limited (an information security company).

Positive media coverage

Positive media coverage is another market driver for the surveillance industry. Media reports that portray surveillance technologies, their developers and providers in a good light influence the public and political perception, often generating and/or maintaining the demand for such solutions. For instance, media reports on the usefulness of CCTV solutions in community safety and crime reduction help foster a demand for such solutions. Surveillance companies and their associations are instrumental in creating and contributing to such media reports. [63]

Public demand

The public demand for safety, security and improved services[64] is considered a major driver of the surveillance market.[65] The UK Commons Select Committee talks about this in some detail, stating:

> The public may have come to expect from government the ability to handle information and deliver personalised services in the same way as the private sector, and may not necessarily see the collection of information for the delivery of these services as surveillance. In other

[62] Marketsandmarkets.com, *Unmanned Aerial Vehicles (UAV) Market - Global Forecasts, Trends and Geographical Analysis (2012 – 2017)*, November 2012. http://www.marketsandmarkets.com/Market-Reports/unmanned-aerial-vehicles-uav-market-662.html

[63] Pati, Anita, "Is community safety at risk as cash-strapped councils cut CCTV?" *The Guardian*, 16 December 2011. http://www.guardian.co.uk/local-government-network/2011/dec/16/community-safety-risk-councils-cctv; Henry Gates and Son Ltd, "Successful CCTV Camera in Cheltenham Capturing 50 Arrests a Month", 13 July 2012. http://www.hg-security-systems.co.uk/blog/successful-cctv-camera-in-cheltenham-capturing-50-arrests-a-month/; Henry Gates and Son Ltd, "Mobile CCTV proving success in Bournemouth", Blogpost, 4 May 2012. http://www.hg-security-systems.co.uk/blog/mobile-cctv-proving-success-in-bournemouth/

[64] For example, in e-government, e-banking or e-business.

[65] Busch, Christophe, "Facing the future of biometrics: Demand for safety and security in the public and private sectors is driving research in this rapidly growing field", *EMBO Reports*, July 2006 July. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1490310. EMBO stands for the European Molecular Biology Organization.

areas, increases in the reach and extent of surveillance have been implemented amidst explicit calls for such increases from some sections of the public.[66]

Some previous Home Office studies found high levels of public support for CCTV solutions.[67] A crucial point here is that the surveillance industry plays a key role in creating awareness of the *need* for surveillance solutions such as biometrics and driving demand.[68] Many companies, such as TSecNet s.r.l,, explicitly talk of surveillance technology as meeting the "public demand for security"[69] (though they do not elaborate what they mean by this concept).

Inhibitors of the surveillance industry

Legislation

While legislation may drive the surveillance industry, it may also function as an inhibitor or barrier. Surveillance companies are subject to domestic and international rules and regulations (such as privacy and data protection laws, tax, trade regulations, export controls) that affect how these companies conduct their business. Surveillance companies incur costs in complying with rules and regulations. Failure to comply may result in liabilities, fines and penalties.

Shifts in policy

Shifts in policy can affect the surveillance business. If a policy disfavours a certain surveillance technology, it could be abandoned leading to a business loss. A dramatic example of this is the case of the UK national ID cards scheme – the Labour government introduced the scheme, but when the Conservative and Liberal Democrats came to power, they abandoned it,[70] which resulted in the scheme being scrapped in most part.[71] Thales, one of the scheme's contractors, received a lesser payment than it would have, if the scheme had gone ahead.

Inadequate innovation, research and development

Inadequate research, development and innovation are another factor that can adversely affect the industry.

---

[66] UK Select Committee on Home Affairs, "Why has the use of surveillance increased?", Fifth Report, 8 June 2008. http://www.publications.parliament.uk/pa/cm200708/cmselect/cmhaff/58/5807.htm

[67] Gill, Martin, and Angela Spriggs, Assessing the impact of CCTV, Home Office Research, Developments and Statistics Directorate, London, 2005, p ix; Spriggs, Angela, Javier Argomaniz et al., "Public attitudes towards CCTV: results from the Pre-intervention Public Attitude Survey carried out in areas implementing CCTV", Home Office Online Report, October 2006, p. 49.

[68] For instance, see securLinx, "Increasing public awareness of the need for biometric solutions", 10 April 2012. http://securlinx.co/?p=549

[69] TSecNet s.r.l, "Video Surveillance and Physical Security". http://www.tsecnet.com/en/solutions/security-systems/1/video-surveillance-and-physical-security

[70] Lettice, John, "Killing ID cards and the NIR - the Tory and LibDem plans", *The Register*, 9 July 2009. http://www.theregister.co.uk/2009/07/09/id_cards_nir_tory_lib_plans/

[71] Home Office, "Identity cards are to be scrapped", 27 May 2010. http://www.homeoffice.gov.uk/media-centre/news/identity-cards-scrapped

Lack of finances and funding

Many surveillance companies, such as Aqsacom, Atos SA, BAE Systems Detica, Boeing and Fox-It, have extensive or exclusive[72] public sector surveillance portfolios and rely heavily on government funding and contracts. A poor economic environment that leads to government budgets cuts adversely affects the surveillance business.

Losses

Losses (which result in a decrease in operating income) are a major inhibitor of the surveillance industry. Finmeccanica reported significant losses in 2011.[73] Quadnetics Mobile Systems defence activities for 2011 also registered a loss.[74] Losses can be attributed to contract delays, loss of customers, restructuring of business, decreased productivity, declining demand for solutions, etc.

Negative media publicity

Just as positive media coverage boosts the surveillance industry, negative media coverage adversely impacts the surveillance industry. The media coverage of the surveillance industry in Europe has for the most part characterised it in a negative light, particularly in relation to privacy and human rights issues. Companies such as Amesys, Gamma Group, Google and Boeing have experienced such publicity.[75] Despite some legal and policy actions being taken, the level of the effect of such negative media coverage varies and whether it is an effective inhibitor (in how it affects the behaviour of individual companies) is a matter open for discussion.

Public rejection and lack of demand

Public rejection of surveillance technologies is another inhibitor of the surveillance industry. For instance, negative public opinion and campaigns against ID cards in UK succeeded in getting the scheme abolished. Though it was reported that two of the scheme's contractors (IBM and CSC) were not financially affected, Thales got a "relatively meagre £18m deal to build the National Identity Register".[76]

Thus, various factors, such as legislation, policy, research and innovation, financial support and funding, profits, positive media coverage, and public demand, drive the surveillance industry. Similarly, factors such as legislation, policy shifts, inadequate research and development, lack of finances/funding, losses, negative media pubilicity and public rejection inhibit or challenge the industry's growth and development.

[72] For example, Spectronic Systems A/S (Denmark), Elaman GmbH (Germany), Cleartrail (India), Elta Systems (Israel).

[73] Finmeccanica, Profile. http://www.finmeccanica.it/Corporate/EN/Corporate/Il_Gruppo/Profilo/index.sdo

[74] Quadnetics Group plc, "Innovating, Integrating, Protecting: Annual Report and Accounts for the 12 months ended 30 November 2011".
http://www.quadnetics.com/Doc/Pdf/Financials/AnnualInterimReports/AnnualReport2011.pdf

[75] See section 3.3.6 (controversies).

[76] Williams, Christopher, "Contractors dodge ID cards axe", *The Register*, 27 May 2010.
http://www.theregister.co.uk/2010/05/27/id_card_contracts/

3.2.4 Non-EU markets

In addition to their European operations, many surveillance companies have global operations. Examples include Autonomy (with interests in North America, Latin America and Asia-Pacific),[77] dunhummby (Asia, Americas),[78] Dreamlab Technologies AG (Chile),[79] QinetiQ Group plc (USA, Australia, Saudi Arabia),[80] and Tecnobit SLU (USA and Latin America).[81] BAE Systems Detica reports its products are "amongst the first to be brought to market by the Group's new security business in India".[82] The focus on and investment in non-European markets is driven by the economic downturn in Europe, huge potential of these markets, general receptiveness to surveillance solutions.

Recently, the surveillance industry (e.g., Gamma and Finmeccanica) has come under sharp criticism for the export of surveillance technologies to repressive regimes such as Iran, Egypt and Syria.[83]

3.2.5 Conclusion

Research into various surveillance markets reveals that there has been a good demand for surveillance solutions in Europe, a trend that is likely to increase taking into account the overall escalating focus (by policy-makers, regulators and technologists) on surveillance technologies as an effective means of enhancing security and safety. The market data we have examined reveals positive prospects for all the examined areas: biometrics, deep packet inspection, smart cards, RFID, smart homes, unmanned aerial vehicles, x-ray security screening, and video surveillance.

Various factors, such as legislation, policy, research and innovation, financial support and funding, profits, positive media coverage, and public demand, drive the surveillance industry. Similarly, factors such as legislation, policy shifts, inadequate research and development, lack of finances/funding, losses, negative media pubilicity, public rejection inhibit or challenge the industry's growth and development.

3.3 LEADING SURVEILLANCE COMPANIES IN EUROPE

This section reviews the surveillance industry in Europe: it identifies surveillance companies, conducts a sample study of significant surveillance companies and analyses the business of surveillance in Europe. This section aims to discover the motivations of the surveillance industry, present the main offerings (surveillance solutions), distill the key features or characteristics and highlight the controversies surrounding the industry.

All this is essential to help us understand the core essence of the surveillance industry, its true nature, what are the underlying factors steering the industry, the scale and scope of the industry, its dynamic, influential and controversial nature. This will then help us further in

[77] www.autonomy.com/
[78] http://www.dunnhumby.com/
[79] https://www.dreamlab.net/
[80] www.qinetiq.com/
[81] http://www.tecnobit.es
[82] BAE Systems, Annual Report, 2011.
[83] Clark, Liat, "UK must stall export of surveillance tech to brutal regimes, or face legal action", *Wired.co.uk*, 25 July 2012. http://www.wired.co.uk/news/archive/2012-07/25/privacy-international-surveillance

finding and recommending solutions for building resilience in the public to the deleterious effects of the surveillance industry, without disadvantaging unduly the European industry versus its competitors.

3.3.1 Methodology

We surveyed the security and related industries in Europe to identify the leading surveillance companies. We have identified more than 300 companies (see Annex 1) offering a variety of surveillance solutions in Europe. Since it was impossible to examine this long list within limited timeframe available to us, we selected a sample of 39 companies (including some based outside the EU but doing business here)[84] for a more detailed analysis that would help us characterise the European surveillance industry. The short-listed sample[85] represents companies with influential and growing surveillance solutions or portfolios and covers a variety of surveillance companies based on the following criteria: geography, organisational size, nature of business, capacities (manufacturer, service provider, vendor/distributor, systems integrator), experience, focus and surveillance offerings.

For each of the sampled companies, we researched the following items:[86]

1. Inception
2. Headquarters
3. Area of operations
4. Number of employees
5. Annual turnover
6. Vision, mission, values (or objectives)
7. Focus or specialisation
8. Products and services (with a particular focus on surveillance)
9. Customers
10. Partners
11. Investors
12. Contracts and/or sources of funding
13. Acquisitions and mergers
14. Project involvement (e.g., in projects funded under the EC's Sixth and Seventh Framework Programmes, FP6 and FP7)
15. Trade and/or industry affiliations
16. Controversial aspects

The data was collected from company websites, annual reports and other public documents (e.g., brochures, fact sheets, press releases) available from the companies and other independent sources (such as the media).

3.3.2 The sample study

Annex 2 presents the short-listed sample of surveillance companies and presents details such as country (headquarters), focus, area of operations, number of employees, annual turnover (2012 or 2011), customers/clients, partners and their involvement in EU research projects (particularly those with security, ICT focus). We briefly list these below:

1. 3M Cogent

[84] These are relevant because many of them have European operations.
[85] See Shortlisted sample of surveillance companies, Annex 2.
[86] This research was collaboratively carried out by partners in the IRISS consortium from Trilateral Research & Consulting LLP (UK), Fraunhofer Institute for Systems and Innovation Research (Germany) and the University of Barcelona.

2. Acxiom
3. ADT Security Services
4. AGT Group GmbH
5. Atos SA
6. Audiotel International
7. BAE Systems Detica
8. Boeing
9. Bosch Security Systems
10. Cassidian
11. Cognitec Systems GmbH
12. EADS NV
13. Ericsson
14. Experian
15. Finmeccanica
16. G4S plc
17. Gemalto NV
18. Google
19. Honeywell International Inc
20. Indra Sistemas (GIS)
21. Israel Aerospace Industries - IAI (and subsidiary Elta)
22. L-3 Communications Corp
23. Lok8U
24. Microdrones
25. Neurotechnology
26. Nokia Siemens Networks BV
27. Northrop Grumman Information Systems Europe
28. Palantir
29. QinetiQ Group plc
30. Quadnetics (and subsidiary Synectics)
31. Saab AB
32. Safran Morpho
33. Securitas AB
34. Shoghi Communications
35. Siemens
36. Smartrac Technology
37. Thales
38. Trovicor GmbH
39. ZTE Corp

The detailed analysis of these companies against the specified details enabled us to gauge what the surveillance industry in Europe is currently offering as solutions and draw some conclusions about the nature of the surveillance industry and the business of surveillance in Europe. We recommend that the findings of our study be used as a springboard for further research in this area.

3.3.3 Motivations

This section determines the motivations of the surveillance industry, based on a study of the sampled companies' explicitly stated visions, missions and objectives, derived from the companies' websites and other public documents. This gives us an idea about how the industry projects itself (and we can then compare this with how the industry actually conducts itself in the analysis that follows).

One of the key visions expressed by some of the sampled surveillance companies is *to contribute to public safety, security and defence*. Safran Morpho, for example, seeks to "create a climate of confidence by contributing to the safety and security of people, transportation, data and countries around the world".[87] AGT International seeks to enable governments, corporations and individuals to predict, prepare for, prevent and manage public safety and security challenges through collection and analysis of data.[88] Palantir states its work is to "solve the technical problems, so they can solve the human ones. Combating terrorism. Prosecuting crimes. Fighting fraud. Eliminating waste."[89] Shoghi Communications intends "to predict and conceive the needs of combat forces and be ready to provide those technologies, products and systems required for defence.[90] Saab AB seeks to contribute to a safer society and act according to ethical standards.[91] Honeywell believes in making the "world safer and more secure, more comfortable and energy efficient, and more innovative and productive".[92] Northrop Grumman's vision's is

> to be the most trusted provider of systems and technologies that ensure the security and freedom of our nation and its allies. As the technology leader, we will define the future of defense—from undersea to outer space, and in cyberspace.[93]

Here, we see how these companies envision an active participatory influence in their sectors of operation.

Many of the sampled surveillance companies express their mission in terms of *sector or industry leadership.* For instance, the Quadnetics/Synectics vision is "to become a leading global supplier of integrated surveillance and security systems which are a fundamental part of our customers' operations". [94] Israel Aerospace Industries (IAI) aims to "be a world leader in all of its main areas of activity" (i.e., "the development of Israel and its defense and security needs").[95] Ericsson envisions becoming the "prime driver in an all-communication world".[96] Cassidian's vision is to defend world security and its mission is to "support the people whose mission is to protect the world".[97]

Some companies such as Nokia Siemens Networks (NSN) embed *societal values* such as privacy in their company vision. NSN states it helps users "enjoy secure services and preserve their privacy, while enabling operators to maximize profit, minimize leaks and comply to regulations".[98]

---

[87] www.morpho.com
[88] http://agtinternational.com/
[89] Palantir, What we do. http://www.palantir.com/what-we-do/
[90] Shoghi Communications, Director's vision. http://www.shoghicom.com/director-vision.html
[91] Saab AB. http://www.saabgroup.com/Global/Documents%20and%20Images/About%20Saab/Company%20Profile/SAAB_Corporate_Brochure.pdf
[92] Honeywell, About Honeywell. http://honeywell.com/About/Pages/our-company.aspx
[93] Northrop Grumman, Our Vision, Values and Behaviors. http://www.northropgrumman.com/corporate-responsibility/ethics/our-vision-values-and-behaviors.html
[94] Quadnetics Group plc, Vision, mission and strategy. http://www.quadnetics.com/About_Us/Vision~_Mission_and_Strategy/default.aspx?id=276
[95] IAI, Past, present, future. http://www.iai.co.il/12021-en/CompanyInfo-PresentPastFuture.aspx
[96] http://www.ericsson.com/thecompany/company_facts/vision
[97] www.cassidian.com
[98] http://www.nokiasiemensnetworks.com/portfolio/services/security

Google's mission has a particularly strong *stakeholder* spin. It suggests Google's mission is "to organize the world's information and make it universally accessible and useful".[99] The Gemalto vision is similarly worded – to "secure people with solutions that are 'personal', 'portable' and multi-purpose".[100] Detica aims at "helping clients capture, store, retrieve, process, exploit and manage their data; we help them turn it into intelligence they can use to make their operations smarter, secure and more efficient".[101]

Other companies outline their *profit* motives – for instance, Experian seeks "for Experian's people, data and technology to become a necessary part of every major consumer economy" and suggests it is "committed to driving long-term shareholder value by focusing on data and analytics, driving profitable growth and optimising capital efficiency".[102]

Thus, we see a variety of motivations expressed by surveillance companies. Some companies express some of these visions or missions, others express combinations of them. Sometimes these motivations (particularly the profit motive) are not explicitly expressed on company websites or in other manners evident to the public; this might be because of the nature of the solutions the surveillance companies offer – for instance, a company offering a controversial solution such as body scanning technology might not outline its intent to profit from the sale of such technology.

3.3.4 Main offerings

Surveillance companies in Europe offer a wide variety of surveillance solutions that not only relate to the defence and national security sector but cut across different sectors such as banking, employment, e-energy and utilities, entertainment, finance, government, healthcare, insurance, media and technology, manufacturing, policing and justice, retail, telecommunications, transport and travel.

Next, we list the companies' main products and services; different companies offer similar services under different names, i.e., some offerings overlap. Some solutions are specific to government (e.g., defence and national security or policing solutions), while others are more versatile and applicable to government, industry and individual applications (e.g., CCTV). While we have attempted to be as comprehensive as possible, below is a non-exhaustive list of surveillance solutions offered by the industry which shows how wide is the range of products and services on offer.

<u>Government and law enforcement solutions</u>

- Airborne surveillance and reconnaissance aircraft
- Audio surveillance systems
- Automatic identification systems
- Biometric technologies and devices (biometric fingerprint, face, iris and voice identification and object recognition)
- Cellular and telecoms monitoring – e.g., GSM monitoring systems
- Coastal surveillance systems
- Command and control systems

[99] Google Inc., Company. http://www.google.co.in/intl/en/about/company/
[100] Gemalto. http://www.gemalto.com/digitalsecurity/
[101] BAE Systems Detica, Information as an asset. http://www.baesystemsdetica.com/about-us/our-approach/
[102] Experian plc, Annual Report 2012. http://www.experianplc.com/~/media/Files/E/Experian-V2/pdf/investor/reports/2012/experian-ar-2012.pdf

- Communications and intelligence systems
- Cross-domain information sharing tools
- Data compilation and management
- eID
- Electronic intelligence and surveillance systems
- ePassports
- Face recognition systems
- Fingerprint identification systems and technologies
- Geolocation or position determination via GPS or mobile phone triangulation
- Identity management and credentialing solutions
- Information systems
- Intelligence collection and fusion
- Intelligence, surveillance and reconnaissance systems
- Intelligent CCTV with behaviour analysis capabilities
- IP data inspection systems
- Manned and unmanned aerial systems
- Mobile identification
- Mobile identity checks
- Multi-sensor surveillance systems
- National identity systems
- Network surveillance
- Offender monitoring systems
- Operatives based surveillance
- Radar
- Radio monitoring and signal analysis
- Remotely operated robots
- Sensor technologies (e.g., fixed and mobile sensing, line sensors, point sensors, infra-red and thermal sensors)
- Space and intelligence systems (including satellites and satellite monitoring)
- Unmanned ground systems
- Visual-range cameras
- Voice and fax logging and analysis
- Web intelligence tools
- Wireless solutions (high-end radio communication systems for defence and commercial applications)

<u>Commercial solutions</u>

- Advanced IP solutions
- Biometric technologies and devices (biometric fingerprint, face, iris and voice identification, object recognition and eyetracking)
- Business video surveillance
- CCTV
- Consumer information databases
- Counter-surveillance products (counter-surveillance receivers, integrated detectors, radio monitoring systems, phone tap detectors)
- Customer intelligence services
- Data analytics (content analytics, mobile analytics, conversion analytics, social analytics and advertising analytics)
- Data records storage solution
- Employee background screening
- Enterprise risk management platform
- Face recognition systems

- Geolocation or position determination via GPS or mobile phone triangulation
- Hand-held bar code scanners
- Identity solutions
- IP data inspection systems
- Logical access control solutions
- Operatives based surveillance
- Physical access control solutions
- Remote patient monitoring (telehealth)
- Smart cards, readers
- Vehicular surveillance solutions
- Verification systems
- Video analytics
- Wireless sensing

Solutions for individuals

- Child ID solutions
- Counter-surveillance products
- Face recognitions systems and technologies
- GPSand mobile phone tracking
- Home security systems
- Home video surveillance (CCTV)
- Intrusion systems
- Medical alert systems
- Monitoring services
- Operatives based surveillance
- Patient monitoring
- Remote home monitoring
- Security alarm and video surveillance
- Street surveillance

While it was impossible to cover in detail this extensive portfolio of surveillance solutions, some of the more interestingand noteworthy surveillance solutions are:

- L-3's Praetorian Intelligent Surveillance Solution[103]
- Google Plus[104]
- Cyclope-Series employee surveillance software[105]
- Darnbro's wearable RFID[106]
- Sierra Nevada Corporation's Vigilant Stare[107]
- Guardia's advanced 3D and infrared face recognition system[108]
- TraceSpan's DSL Phantom™[109]
- Siemens Integrated surveillance system - Siveillance[110]
- 33Across's SocialDNA™ Targeting[111]

[103] L-3, Solutions. http://www.l3praetorian.com/solutions.htm
[104] Google Inc, https://plus.google.com/
[105] Cyclope-Series, Features. http://www.cyclope-series.com/employee-surveillance/employee-monitoring-software.html
[106] Darnbro Ltd., Security Clothing. http://websites.uk-plc.net/Darnbro_Limited/
[107] www.sncorp.com/pdfs/isr/vigilant_stare.pdf
[108] Guardia, Our products. http://www.guardia.com/products/index.htm
[109] TraceSpan, TraceSpan Products. www.tracespan.com/ipdslphantom.aspx
[110] Siemens, Security solutions with Siveillance. http://www.buildingtechnologies.siemens.com/bt/global/en/security-solution/security-solution-siveillance/pages/security-solution-siveillance.aspx

These technologies and products are significant in terms of their surveillance potential, effects and applicability. L-3's Praetorian Intelligent Surveillance Solution promotes complete and accurate surveillance by enabing users to "see the total picture, understand real-time surveillance information, and act pre-emptively to stop or contain emerging threats" through 3-D immersive displays. [112] Google Plus has a huge potential to track users and transmit their data across networks and devices – it has been termed "a potential privacy landmine".[113] The Cyclope-Series employee surveillance software (which can monitor websites visited by employees and web applications used) is used by more than 7,000 organisations worldwide including non-profit organisations, universities, schools and companies. Darnbro's wearable RFID solution targeted particularly for use in schools is significant for its ubiquitous potential to track, invade and erode the privacy and autonomy of children.[114] Sierra Nevada Corporation's *Vigilant* Stare (in collaboration with ITT Excelis) is a manned aircraft-based Wide-Area Airborne Persistent Surveillance (WAPS) system that facilitates persistent surveillance through providing a "visible and infrared coverage of city-sized areas, providing real-time motion imagery directly to diversified users involved in domestic support mission".[115] TraceSpan's DSL Phantom™ integrates with lawful interception (LI) solutions to monitor and record data transparently, for use by intelligence gathering agencies and law enforcement authorities.[116] The Siemens Integrated surveillance system – Siveillance integrates different surveillance solutions (such as video intelligence analysis and surveillance).[117] 33Across's SocialDNA™ Targeting enables companies to gauge the social characteristics of their customers.[118] These surveillance solutions have far-reaching implications for society and individuals that come under their radar.

3.3.5 Features and characteristics of the industry

Based on the initial scan of the surveillance industry and the detailed sample analysis, we outline the features and characteristics of the surveillance industry in Europe. This will help us characterise the industry. These features include: diversity, variety of solutions, global sales expansion, profit-driven nature, public sector demand and collaborations, strategic partnerships, acquisitions and mergers, growth of non-EU players, surveillance showcasing and lack of openness and transparency.

---

[111] 33Across, Technology. http://33across.com/technology.php#ixzz26emhBYXF
[112] L-3, Solutions. http://www.l3praetorian.com/solutions.htm
[113] Krigsman, Michael, "Google Plus: Is privacy an issue?", *ZDNetNews*, 11 July 2011. http://www.zdnet.com/blog/projectfailures/google-plus-is-privacy-an-issue/13749
[114] Marx, Gary, and Valerie Steeves, "From the Beginning: Children as Subjects and Agents of Surveillance", *Surveillance & Society*, Vol. 7, No. 3/4, 2010, pp. 192-230. http://www.surveillance-and-society.org
[115] ITT Excelis, "Sierra Nevada Corporation and ITT Exelis Partner to Build Advanced Wide-Area Airborne Persistent Surveillance System", press release, 8 July 2012. http://www.exelisinc.com/news/pressreleases/Pages/Sierra-Nevada-Corporation-and-ITT-Exelis-Partner-to-Build-Advanced-.aspx
[116] TraceSpan, TraceSpan Products. www.tracespan.com/ipdslphantom.aspx
[117] Siemens, Security solutions with Siveillance. http://www.buildingtechnologies.siemens.com/bt/global/en/security-solution/security-solution-siveillance/pages/security-solution-siveillance.aspx
[118] 33Across, Technology. http://33across.com/technology.php#ixzz26emhBYXF

Diversity of companies

There is a wide diversity of companies providing surveillance solutions in Europe. The diversity relates to organisational history, revenues, size, location, operation and organisational focus.

Some companies such as Siemens (established in 1847), Finmeccanica (1948) and Boeing (1916) are established players in the security industry; others, such as Lok8U (2008)[119] and Innovative Security Designs (2012),[120] are more recent entrants into the surveillance and security market. Among the biggest companies in terms of turnover are Honeywell, L-3 Communications Corp., Atos SA, G4S Plc and Smartrac NV. In terms of employment, amongst the sampled companies, the largest are G4S plc (657,000 employees), Siemens AG (360,000), Securitas AB (300,000) and Honeywell (132,000).

The sampled surveillance companies also evidenced global presence – in terms of location of customers, production sites, offices, R & D centres, etc. For example, Gemalto has customers in more than 190 countries, 74 sales and marketing offices, 15 production sites, 28 personalisation centres, 14 research and development centres.[121] Thales employs 67,000 people in 56 countries. Cassidian has more than 15,000 suppliers, 700 projects, more than 400 customers and partners and operations in more than 80 countries), Indra Sistemas (operations in over 118 countries – mainly Europe and Central and South America.

Even small companies such as Neurotechnology have global outreach, with distributors in Argentina, Brazil, China, Colombia, Congo DR, El Salvador, Ecuador, Greece, India, Indonesia, Italy, Israel, Korea, Mexico, Pakistan, Peru, Philippines, South Africa, Spain, Taiwan, Thailand, UK, USA, Venezuela and Vietnam. Similarly, Polish Marco Systems (telecommunications interception and data analysis) does business in Europe, Africa and Asia.[122]

The European surveillance industry players are also headquartered across Europe and the world.[123] The US has the largest number of surveillance companies, but the UK, France and Germany also have substantial numbers.

In terms of organisational focus, we also see a diverse range of surveillance thrusts. Some companies are more broadly focussed and offer a variety of surveillance solutions (e.g., Cassidian, G4S, Indra Sistemas); while others have a more specific surveillance focus – e.g., Lok8U (GPS), Microdrones (aerial surveillance), Neurotechnology (biometrics), Smartrac NV (RFID-based solutions).

Variety of solutions

As noted above, the surveillance industry offers a variety of solutions ranging from defence and military surveillance solutions to small solutions aimed at the individual consumer. Surveillance companies are investing increasing budgets into research and development and coming up with improved, more efficient and novel surveillance solutions. For instance,

[119] www.lok8u.com
[120] http://isdcam.com/
[121] Gemalto, About us. http://www.gemalto.com/companyinfo/about/index.html
[122] Marco Systems. http://www.macrosystem.pl/
[123] See Annex 1.

Siemens AG reportedly "spent 3.9 billion euros ($5.1 billion), or 5.3 percent of revenue, on R&D in its last fiscal year through September, up from 5.2 percent a year earlier" and further "plans to increase spending on research and development this year to retain a competitive advantage".[124]

Global sales expansion

As evidenced before, European surveillance companies have a global presence and sell technologies worldwide. European surveillance companies are also constantly looking towards expanding their markets in countries outside the European Union, particularly in markets such as North America, Asia and Africa.

Finmeccanica, for instance, ranks among the top 10 global players in aerospace, defence and security and ranks sixth worldwide in the defence and security electronics market.[125] It has industrial facilities worldwide (350 companies, joint ventures, partnerships and joint industrial projects).[126] It does business with the US government and defence agencies, the Australian government, the Italian government and its defence department, and the Indian navy.

Profit-driven nature

The surveillance industry in Europe is, of course, a profit-driven and profit-motivated industry. Investment in manufacture, integration, provision or sale of surveillance technologies generates high levels of income for companies. Some cases in point – QinetiQ's operating profit for 2012 was £161.3 million (£145.4m for 2011 and £120.3m for 2010).[127] Acxiom's annual revenue (year ended 31 March) was $1.131 billion for 2012, $1.114 billion for 2011, $1.063 billion for 2010.[128] The following table shows Acxiom's operating profit and profit margins:

[124] Weiss, Richard, "Siemens to Increase R&D Spending to Retain Competitive Edge" *Bloomberg*, 23 March 2012. http://www.bloomberg.com/news/2012-03-23/siemens-to-increase-r-d-spending-to-retain-competitive-edge.html
[125] www.finmeccanica.it
[126] Finmeccanica, Profile. http://www.finmeccanica.it/Corporate/EN/Corporate/Il_Gruppo/Profilo/index.sdo
[127] QinetiQ Group plc, Annual Report and Accounts 2012. http://www.qinetiq.com/investors/results-reports/AnnualReportDocuments/QinetiQ-Annual-Report-2012.pdf
[128] Acxiom Corporation, Annual Report 2012. www.acxiom.com/about-acxiom/investor-info/reports/

Operating Profit and Profit Margins

The following table presents the Company's operating profit margin by segment for each of the years in the three-year period ended March 31, 2012 (dollars in thousands):

	2012	2011	2010
Operating profit and profit margin:			
Marketing and data services	$ 96,095	$ 87,254	$ 79,004
	12.5%	11.9%	11.0%
IT Infrastructure management services	$ 24,988	$ 24,467	$ 22,293
	8.6%	8.1%	8.1%
Other services	$ (5,079)	$ (2,270)	$ (4,699)
	(7.5)%	(3.0)%	(7.1)%
Corporate	$ (30,441)	$ (84,274)	$ 944
Total operating profit	$ 85,563	$ 25,177	$ 97,542
Total operating profit margin	7.6%	2.3%	9.2%

Fig: Acxiom operating profit and profit margins[129]

Boosted by the profitability of the surveillance business, traditional security companies are expanding their portfolios and acquiring surveillance-centric businesses[130] to be able to offer surveillance solutions. New start-ups are constantly emerging in the market (e.g., Innovative Security Designs, a 2012 start-up focussing on IP surveillance solutions[131]).

Government and public sector demand, expenditure and collaborations

A major driver of the surveillance industry is the government or public sector demand for such solutions. Our analysis of surveillance companies shows that the government is a major customer of the surveillance industry.[132]

Companies such as 3M Cogent boast of a wide government clientele. 3M Cogent's clients include the UK Border Agency, Policia D'Andorra, Belgium Federal Police, Bulgarian Research Institute of Forensic Sciences and Criminology, Commission of European Communities Directorate-General Justice and Home Affairs, Hungarian Police, Hungarian Institute of Forensic Science, Italian Ministry of Interior Criminal Police, R.I.S. Carabinieri (Italy), UNMIK Police (Kosovo), Lithuanian Police Forensic Science Centre, Netherlands Ministry of Justice, Slovakian National Police, Slovakian Ministry of Interior, Spanish Ministry of Interior, Spanish National Civil Guard and National Police and the Turkish National Police and Gendarme. Cognitec's major client is the German government (visa software).

G4S plc has been accused of running a "private security state"[133] or "shadow security state"[134] due to its huge and ever increasing government and public sector business, ranging from

[129] Ibid.
[130] See section 3.3.5.7 (acquisitions and mergers).
[131] http://isdcam.com/
[132] As shown in section 3.2.2 (surveillance customers), specifically section 3.2.2.1 (government and its agencies).
[133] Grayson, John, "Britain as a private security state: first they came for the asylum seeker", *OpenDemocracy.net*, 9 March 2012. http://www.opendemocracy.net/ourkingdom/john-grayson/britain-as-private-security-state-first-they-came-for-asylum-seeker
[134] Taylor, Matthew, "How G4S is 'securing your world'", *The Guardian*, 20 June 2012. http://www.guardian.co.uk/uk/2012/jun/20/g4s-securing-your-world-policing/

policing operations, prison management, smart metering for homes, guard services, number plate recognition technologies and covert surveillance for insurance companies.

In addition to surveillance companies openly doing business with the government, there are disturbing trends of surveillance companies collaborating with governments (arguably beyond their remit) in citizen surveillance (particularly Internet and mobile based). For instance, Google has been associated with agencies such as the US National Security Agency[135] and the Central Intelligence Agency[136] in web monitoring and there are reports that Google (and other companies) are being pushed by the US Federal Bureau of Investigation to "build in backdoors for government surveillance".[137] Skype has reportedly "expanded its co-operation with law enforcement authorities to make online chats and other user information available to police".[138]

A news report suggests

> In cities across the world, groups composed of telecom companies and government representatives have met to discuss how to integrate surveillance capabilities into existing and developing technologies. The decisions they have made, largely beyond public scrutiny, could lead to a fundamental shift in the Web's basic architecture. [139]

The report highlights how the the European Telecommunications Standards Institute (ETSI) is collaborating with government and law enforcement agencies "to integrate surveillance capabilities into communications infrastructure".[140] ETSI's meetings on lawful interception are attended by government departments and large teleecomunications companies such as British Telecom, Nokia Siemens, RIM and Vodafone. ETSI's paper on "Security for ICT-The Work of ETSI" outlines that its Technical Committee Lawful Interception (TC LI) "has the active participation of the major telecom manufacturers, network operators, and regulatory authorities of Europe and from around the world."[141]

Strategic partnerships and collaborations

Another important feature of the surveillance industry is the formation of strategic partnerships and alliances. Surveillance companies form partnerships or enter into joint

---

[135] Zetter, Kim, "Google Asks NSA to Help Secure Its Network", *Wired*, 4 Feb 2010. http://www.wired.com/threatlevel/2010/02/google-seeks-nsa-help/; Shachtman, Noah "'Don't Be Evil,' Meet 'Spy on Everyone': How the NSA Deal Could Kill Google", *Wired*, 4 Feb 2010. http://www.wired.com/dangerroom/2010/02/from-dont-be-evil-to-spy-on-everyone/; The Associated Press, "Court rules that Google-NSA spy ties can remain secret", published in *USA Today*, 11 May 2012. http://www.usatoday.com/tech/news/story/2012-05-11/court-google-nsa-spy-china/54912902/1

[136] Orlowski, Andrew, "Google buys CIA-backed mapping startup", *The Register*, 28 October 2004. http://www.theregister.co.uk/2004/10/28/google_buys_keyhole/; Jacobson, Bob, "Google and CIA Invest in a Minority Report-Like Technology That May Make Our World a Less Certain Place", *Huffington Post*, 30 July 2010. http://www.huffingtonpost.com/bob-jacobson/google-and-cia-invest-in_b_664525.html

[137] McCullagh, Declan, "FBI: We need wiretap-ready websites – now", CNET News, 4 May 2012. http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/

[138] Timberg, Craig, "Skype joins hands with authorities to assist in online surveillance", *The Washington Post*, 27 July 2012. http://www.smh.com.au/technology/technology-news/skype-joins-hands-with-authorities-to-assist-in-online-surveillance-20120726-22v0t.html

[139] Gallagher, Ryan, "How Governments and Telecom Companies Work Together on Surveillance Laws" *Future Tense*, 14 Aug 2012. http://www.slate.com/articles/technology/future_tense/2012/08/how_governments_and_telecom_companies_work_together_on_surveillance_laws_.html

[140] Ibid.

[141] Rizzo, Carmine, Charles Brookson, "Security for ICT – the Work of ETSI", ETSI White Paper No 1, January 2012. http://www.scribd.com/doc/100874830/ETSI-security-for-ICT-white-paper

ventures with other companies, academia and research institutions. Honeywell International has both technology and academic partners (the technology partners provide technological support to clients and its academic collaborations include curriculum development, technology research, training, and higher education programs).[142] Bosch Security Systems collaborates with major electronic equipment companies.[143]

Microdrones partners with different universities such as the University of Klagenfurt in Austria and the Technical University of Dortmund. Its partners are often its clients.[144] Securitas has service partners (such as Goingsoft for Internet security), media partners and research partners (universities). Smartrac collaborates with the International Association of Public Transport (UITP) and the AIPIA (Active and Intelligent Packaging Industry Association) and partners with semiconductor and communication industry companies such as Sony, Infineon, NXP, Giesecke & Devrient, and Texas Instruments.[145] Thales co-operates with numerous international companies (e.g., with Nokia Siemens Networks for secure communication; Elbit (Israel) for tactical systems of the 'Watchkeeper'), with Oracle, Microsoft, IBM, Adobe for ICT). AGT's Research and Development Centre in Darmstadt collaborates with prominent research institutions in the Rhein-Main-Neckar-Region, the SAP Research Center Darmstadt/Future Public Security Living Lab, CASED, Seeburger, T-Systems, KIT, Software AG, and the Fraunhofer Institute for Secure Information Technology (SIT) and the Fraunhofer Institute for Computer Graphics (IGD).

Acquisitions and mergers

Acquisitions and mergers are seen as an important part of "overall corporate strategy",[146] or "bolt-ons" to "add market share, specialist capabilities and/or geographical position".[147] Companies acquire complementary businesses, products and technologies as a tool for growth and to increase the profit margins of the company – for example, Acxiom reports its "total revenue increased 4.7% or $50.2 million to $1,113.8 million in fiscal 2011. Of the revenue increase, $10.1 million related to the MENA and GoDigital acquisitions".[148] Acquisitions may be used as a means to expand and extend presence (e.g., Experian's acquisition of Computec expanded their presence in Colombia, Peru and Venezuela).[149] Acquisitions are also used by companies to extend leadership, consolidate position or restrict competition in a particular sector. Safran Morpho acquired L-1 Identity Solutions to become the world leader in biometric identity solutions.

[142] Honeywell, Partners. http://www.honeywell.com/sites/htsl/partners.htm
[143] Bosch. http://www.bosch-sicherheitsprodukte.de/content/language1/html/55_DEU_XHTML.asp. See "Lösungen"; http://www.bosch-sicherheitssysteme.de/de/systeme/planer/index.htm; http://www.bosch-sicherheitssysteme.de/de/systeme/elektro/index.htm
[144] Microdrones. http://www.microdrones.com/references/referenzen.php
[145] http://www.smartrac-group.com/en/technology-customers-and-partners.php
[146] Google Inc., Annual Report 2011. http://sec.gov/Archives/edgar/data/1288776/000119312512025336/d260164d10k.htm
[147] Quadnetics Group plc, "Innovating, Integrating, Protecting: Annual Report and Accounts for the 12 months ended 30 November 2011". http://www.quadnetics.com/Doc/Pdf/Financials/AnnualInterimReports/AnnualReport2011.pdf
[148] Acxiom Corporation, Annual Report 2012. www.acxiom.com/about-acxiom/investor-info/reports/
[149] Experian plc, Annual Report 2012. http://www.experianplc.com/~/media/Files/E/Experian-V2/pdf/investor/reports/2012/experian-ar-2012.pdf

Proliferation of non-EU players

As demonstrated by the data we have gathered, a large number of non-European companies are engaged in the surveillance business.

US companies dominate the surveillance industry in Europe. Our research identified more than 100 companies providing a variety of surveillance solutions to customers in Europe.[150] Notable amongst these are: 3M Cogent (biometric identification solutions provider to governments, law enforcement agencies, and commercial enterprises), Phorm (global personalisation technology company – online user surveillance), Science Applications International Corporation – SAIC (satellite, geospatial surveillance, computer surveillance, data mining), United Technologies Corp (video surveillance, products and services for global aerospace and building systems industries), Rapiscan Systems (manufacturer of security equipment and systems designed for checkpoints, cargo, vehicle, baggage, parcel and air cargo security inspection, body scan technology), Boeing (satellites, advanced information communication systems and dynamic network traffic intelligence and analytics through its subsidiary Narus), Palantir (analytics platforms for premier financial and intelligence clients), ADT and Acxiom (consumer data and analytics, databases, data integration and consulting solutions).

We also identified the following companies based elsewhere and doing business in the EU:

> **Canada:** Gens Software Ltd,[151] AdvancedIO, Diamond Aircraft,[152] Genetec Inc,[153] March Networks Corp, Sandvine Incorporated,[154] Vineyard Networks,[155] S.I.C Biometrics Inc,[156] EXFO NetHawk,[157] Seon Design[158]
> **China:** Huawei Technologies,[159] Shanghai Huayuan Electronic Co. Ltd,[160] Vixtel[161] and ZTE Corp.[162]
> **India:** Bharat Electronics Limited (BEL)[163], ClearTrail,[164] Fusion Biometrics,[165] SecureMantra Technologies (P) Ltd,[166] Septier Communications,[167] Shoghi Communications,[168] Ircon,[169] Private Eye (P) Ltd [170]

---

[150] See comprehensive list of surveillance companies – Annex 1
[151] http://www.genssoft.com/
[152] http://www.diamondaircraft.com/
[153] http://www.genetec.com
[154] http://www.sandvine.com/
[155] http://www.vineyardnetworks.com/
[156] http://www.sic.ca
[157] http://www.exfo.com
[158] http://www.seon.com/
[159] http://www.huawei.com/en/. Huawei has been the subject of some unwanted attention recently following allegations of its being a vehicle for state-sponsored surveillance and espionage. See, for example, Anderson, Richard, "Huawei Technologies: Controversial success story", BBC News, 12 Sept 2012. http://www.bbc.co.uk/news/business-19568465. Associated Press, "Australia bans China's Huawei from working on Internet network amid security worries", published in *The Washington Post*, 26 March 2012. http://www.washingtonpost.com/business/australia-bans-chinas-huawei-from-bidding-for-work-on-internet-network-amid-security-worries/2012/03/26/gIQAwl2LbS_story.html
[160] http://shhuayuan.manufacturer.globalsources.com/si/6008823922128/CompanyProfile.htm
[161] http://www.vixtel.com/
[162] http://www.zte.com.cn/cn/
[163] http://www.bel-india.com/
[164] http://www.clear-trail.com/
[165] http://www.fusionbiometrics.com/
[166] http://www.securemantra.org/
[167] http://www.septier.com/

Israel: Ability,[171] Agent video intelligence Inc,[172] Allot,[173] Amdocs Ltd,[174] Cellebrite (fully-owned subsidiary of the Sun Corporation),[175] Elkat,[176] Elta systems (subsidiary of Israel Aerospace Industries),[177] Gita Technologies,[178] Nice Systems,[179] Semptian Technologies,[180] TraceSpan,[181] Elbit Systems[182]
Russia: BioLink,[183] Oxygen Software,[184] Protei[185] and Speech Technology Center Ltd.[186]

In addition to these countries, we also identified surveillance companies from Brazil, Canada, Colombia, Denmark, Hong Kong, Japan, Jordan, Kenya, Mexico, New Zealand, Qatar, Singapore, South Africa, Switzerland, Taiwan and Turkey.[187]

Surveillance showcasing

Surveillance companies are actively involved in pushing (promoting and communicating) their products by organising, sponsoring and participating in events such as conferences, exhibitions, expos, forums, professional development programs, road shows, trade fairs, webinars, etc. Some of these events target a broad audience, while others such as *Security and Policing* (previously Home Office Scientific Development Branch (HOSDB) Exhibition) are closed events with specified visitor criteria.[188]

Many of these events are large, demonstrating growth every year. Eurosatory 2012 (the Land and Airland Defence and Security international exhibition) had 1,432 exhibitors from 53 countries; 53,480 visitors from 129 countries, 684 media persons, 152 official delegations from 84 countries including EU and NATO and covered 163,523 square metres of exhibition space.[189]

Milipol Paris (2011) had 27,243 visitors (62% French and 38% from outside France representing 150 countries).[190] The visitors represented private companies, ministries of the interior and government administrations (such as defence, customs, justice, and local authorities). Of the 887 exhibitors, 47% exhibited in the law enforcement category, 44% in the special forces (anti-terrorism), 36% in civil defence, 32% in urban security, and 31% in

[168] http://www.shoghicom.com/
[169] http://www.ircon.org/
[170] http://www.privateeye-india.com
[171] http://ability.dpages.co.il/
[172] http://www.agentvi.com
[173] http://www.allot.com/
[174] http://www.amdocs.com/
[175] http://www.cellebrite.com/
[176] http://www.elkat.co.il
[177] http://www.iai.co.il/17887-en/Groups_ELTA.aspx
[178] http://www.gita.co.il/
[179] http://www.nice.com/
[180] Website not available.
[181] http://www.tracespan.com/
[182] http://www.elbitsystems.com
[183] http://www.biolinksolutions.com
[184] http://www.oxygensoftware.ru/en/default.asp
[185] http://www.protei.com/
[186] http://speechpro.com/
[187] See Annex 1.
[188] http://www.adsgroup.org.uk/pages/19524782.asp
[189] http://www.eurosatory.com/
[190] http://en.milipol.com/All-about-Milipol/Statistics-2011

port and airport Security. (Note, the numbers do not add up as exhibitors could declare several categories of activity). IFSEC International (the largest largest annual security event held in the UK) 2012 had 24,933 visitors representing 108 countries.[191] 24% of visitors reportedly had budgets of over a million pounds. The event showcases security products and services available in the UK and worldwide and features over 650 manufacturers, suppliers and distributors.

The Counter Terror Expo London had 8,519 attendees (registering a 9.9% increase), 400 exhibiting companies, a five stream conference, live demos and 12 technical workshops.[192] Surveillance related exhibits included solutions such as access control, biometrics, CCTV, covert surveillance systems, communication systems, database management systems, information management and security systems, location and tracking systems, personal equipment and body armour, screening and scanning equipment, sighting and image recording and processing.

These events are important as they showcase surveillance solutions and their application potential, latest developments and advances in technologies, tools, techniques. They also provide information on market trends and best practice. More importantly, they enable industry to collaborate, share experiences and network with other stakeholders, particulary policy and decision-makers in government (particularly intelligence services, defence departments and local law enforcement).

We list some key events below:

Event	Organiser	Target audience
ALARM Expo, Poland	Not found	Professionals from the following market segments: airlines, government agency, alarm installers, banks, border protection, home system installers, hospitals, civil defence and emergency services, close protection, insurance, commercial firms, corporate security professionals, customs, the oil and gas industry, restaurants, electrical services, safety and security services, fire service
Annual ASIS International European Security Conference & Exhibition (sponsored by Nedap, Qinetiq's OptaSense, Securitas and SMR Group)	ASIS International	Security management professionals; corporate executives in IT, supply chain management, strategic planning, human resources, security solutions, law enforcement and fire protection professionals, facility management professionals, intelligence services and military personnel, government officials (justice and home affairs, foreign affairs and defence), academics, consultants, vendors, and architects
Annual ATC Global Exhibition & Conference (backed by industry's key	UBM	Industry and air traffic management stakeholders from around the world, including regulators, ANSPs, airports,

[191] http://www.ifsec.co.uk/page.cfm/link=1
[192] http://www.counterterrorexpo.com/

players and collaborators such as ICAO, EUROCONTROL, SESAR JU, IATA, EUROCAE, EASA, Open Geospatial Consortium and the European Commission)		airlines, military representatives
CARTES (France) – Smart solutions for security, payment, identification and mobility	Comexposium	All smart card user sectors[193]
Counter Terror Expo, London	Clarion Events	Buyers from a range of public and private sectors including: armed forces, architects, border control, central and local government, civil defence, critical national infrastructure, corporate, construction, customs, embassies, finance and banking, Home Office, hotels, intelligence services, UK Ministry of Defence, law, police, prisons, supply chain, prime contractors, tranportation
Eurosatory (Land and Airland Defence and Security international exhibition)	Coges	Land and air defence and security stakeholders
Security & Policing (previously Home Office Scientific Development Branch (HOSDB) exhibition)	Home Office Scientific Development Branch (HOSDB)	Police, law enforcement and security professionals tasked with security, civil protection and national resilience, international professionals and experts from government, law enforcement, police services, critical national infrastructureand industry.
IFSEC International, UK	UBM	Security industry
InfoSecurity Europe	Reed Exhibitions	Every segment of the industry (IT security professionals, IT distribution companies, IT hardware, software, manufacturers and suppliers, finance, banking and insurance professionals, government officials
ISS World Europe (Intelligence Support Systems for Lawful Interception, Criminal Investigations and Intelligence Gathering)	TeleStrategies	European law enforcement, intelligence and homeland security analysts, telecom operators responsible for lawful interception
Annual Information Security Solutions Europe (ISSE)	For 2012 – The European Association for e-Identity and Security (eema), ENISA, INTERREG IVB NEW, LSEC – Leaders In Security (a European information	ICT security professionals and policy makers; Senior managers directly charged with protecting corporate infrastructure; technical experts who determine security requirements and implement solutions; Policy and decision makers with overall security responsibility; legal, compliance, regulatory professionals; government executives and practitioners responsible for protecting systems and critical infrastructures

[193] Listed at http://www.cartes.com/index.php/Exhibit/Why-exhibit-at-CARTES-2012

	security NGO), MCC, Revolution Events, TeleTrust and the European Security Innovation Network	
Milipol Paris	Milipol is owned by consortium of COFREXPORT, PROTECOP, Thales, VISIOM & CIVI.POL Council, a consulting company and service of the French Ministry of Interior.	Private companies, ministries of the interior, administrations (Defence, Customs, Justice, local Authorities)
SICHERHEIT, Zurich – Trade Fair for Safety and Security (biannual)	Exhibit & More AG	Safety and security stakeholders
SPIE Security + Defence Europe	SPIE Europe	Suppliers and project partners in detection, imaging, lasers, and a host of supporting components and devices
World e-ID congress	Strategies Telecoms & Multimedia (Official sponsor: Gemalto; Programme Chair: Infineon)	Identity services managers and decision-makers from public and private sectors
World Smart Week (incorporating the NFC Congress and World e-ID congress), Focus – Contactless e-ID and digital security technologies	Strategies Telecoms & Multimedia	Technology providers, enterprises, public organisations, academics, regulators, trade associations

Lack of openness and transparency

Though many companies aim to be open and transparent with their information, there were some companies for which it was hard to find data. In our sample study, this occurred in the case of Palantir for which we were unable to find data on the number of its employees or annual revenues. Palantir has gained a reputation for secretiveness. It has been called a "secretive data analytics company",[194] "the War on Terror's Secret Weapon"[195], and the "The

[194] Hesseldahl, Arik, "Palantir's $2.5 Billion Mystery, Solved", *AllthingsD.com,* 7 October 2011. http://allthingsd.com/20111007/palantirs-mysterious-investors-have-been-found/

[195] Vance, Ashle,y and Brad Stone, "Palantir, the War on Terror's Secret Weapon", BusinessWeek, 22 November 2011.
http://www.businessweek.com/magazine/palantir-the-vanguard-of-cyberterror-security-11222011.html

Secretive $735 Million Tech Security Company". [196] Palantir does not publish its Annual Report on its website. A search of the United States Securities and Exchange Commission (SEC) filings also failed to reveal its report. In its other SEC filings (for example, the filing of 16 May 2012 FORM D Notice of Exempt Offering of Securities),[197] Palantir did not disclose its revenue.

Similarly, while AGT International suggests that it is one of the fastest growing public safety and security solutions organisations in the world, it is a very discreet company providing hardly any data about its products, projects and clients.[198]

In this section, we identify several features of the surveillance industry in Europe (in addition to its secretiveness). There is a diversity (based on organisational history, revenues, size, location, operation and organisational focus) of companies providing a variety of surveillance solutions in Europe, aimed at different customers within the EU and in markets outside the EU. The surveillance industry in Europe enjoys rising profitability, even as traditional security companies expand into the surveillance business. The industry is driven largely by government and public sector demand and collaborations in providing surveillance solutions. Another important feature of the surveillance industry is the formation of strategic partnerships and alliances and a large prevalence of acquisitions and mergers as part of the overall corporate strategy to consolidate and improve market share.

As noted above, one of the notable features is the large number of non-European companies dominating the surveillance industry in Europe.

As part of their strategy, surveillance companies actively push their products by organising, sponsoring and participating in events such as conferences, exhibitions, expos, forums, professional development programs, road shows, trade fairs, webinars etc.

3.3.6 Controversies

Controversies beleaguer the surveillance industry. Some notable efforts have been made to expose these controversies – for instance, Privacy International's Big Brother Inc project (a global investigation into the international trade in surveillance technologies).[199] Similarly, the Bureau of Investigative Journalism has exposed some controversies.[200] We advance these efforts and present some other controversies involving surveillance companies.

Unethical and illegal business practices

There are several examples of surveillance companies being embroiled in unethical and even illegal business practices. 3M Cogent was found to have aided and abetted the breach of

[196] Gobry, Pascal-Emmanuel, "REVEALED: Palantir Technologies, The Secretive $735 Million Tech Security Company Helping Hedge Funds And Governments", *Business Insider*, 10 March 2011. http://www.businessinsider.com/palantir-technologies-revealed-2011-3?op=1#ixzz20zmtCJ7v

[197] United States Securities and Exchange Commission, FORM D Notice of Exempt Offering of Securities, 16 May 2012. http://www.sec.gov/Archives/edgar/data/1321655/000132165512000002/xslFormDX01/primary_doc.xml

[198] AGT International. http://agtinternational.com/about-us/at-a-glance

[199] Privacy International. https://www.privacyinternational.org/projects/big-brother-inc

[200] Bureau of Investigative Journalism. http://www.thebureauinvestigates.com/

fiduciary duties.[201] Acxiom was implicated in the disclosure of personal information[202] and nominated for the Big Brother Awards for Worst Corporate Invader for data brokering.[203]

Companies such as Cassidian have been criticised for using bribery to increase sales (and even using commercial war threats). Finmeccanica was accused of slush fund bribery charges in 2011. Its chairman Pier Francesco Guarguaglini was investigated and resigned from office (after a golden handshake of €4 million).[204] Detica's parent company BAE Systems has faced allegations of bribery and corruption.[205] Other companies embroiled in bribery allegations are Shoghi Communications (in connection with its relationship with former Indian telecommunications Minister Sukh Ram).[206] Telenor suspended ZTE tenders for new business for six months, suggesting that the Chinese firm had breached its code of conduct for procurements.[207] In 2007, Philippine President Gloria Macapagal Arroyo suspended a $330 million telecommunications deal with ZTE due to allegations of kickbacks.[208]

Surveillance companies such as ADT have been found to be violating consumer laws. The US Federal Trade Commission sued ADT in 2007 for violations of the Telemarketing Consumer Fraud and Abuse Prevention Act. ADT made a $2 million settlement against the charges. Its subsidiaries Alarm King and Direct Security Services were similarly charged and settled for $20,000 and $25,000, respectively.[209]

QinetiQ was involved in a controversial privatisation and floatation – in 2006, the National Audit Office (NAO) investigated QinetiQ's privatisation plans to check if the company's shares had been sold off too cheaply to Carlyle.[210]

Northrop Grumman is reportedly involved in illegal campaign contributions, criminal fraud (illegal campaign contributions, product defects[211] cost overruns,[212] bribery scandals and labour disputes.[213]

---

[201] 3M, Annual Report 2011. http://media.corporate-ir.net/media_files/irol/80/80574/Annual_Report_2011.pdf

[202] EPIC, In the Matter of JetBlue Airways Corporation and Acxiom Corporation, Complaint and Request for Injunction, Investigation and for Other Relief, 22 Sept 2003. http://epic.org/privacy/airtravel/jetblue/ftccomplaint.html

[203] Brennan, Elliot, "Is 'Big Brother' always watching us?", *The Beginner*, 1 June 2011. http://www.thebeginner.eu/technology/all-in-innovation/531-privacy-in-the-21st-century

[204] ANSA (Agenzia Nazionale Stampa Associata), "Finmeccanica chairman steps down amid slush-fund probe: Guarguaglini bows to pressure, CEO Orsi takes over", 1 Dec 2011. http://www.ansa.it/web/notizie/rubriche/english/2011/12/01/visualizza_new.html_11180804.html

[205] King, Eric "Selling arms and snooping technology is no way to help democracy, Cameron," *The Guardian*, 11 April 2012. http://www.guardian.co.uk/commentisfree/2012/apr/11/selling-arms-cameron

[206] Swami, Praveen, "The government's listening to us", *The Hindu*, 1 Dec 2011. http://www.thehindu.com/news/national/article2678501.ece

[207] Reuters, "China's ZTE admits to Telenor ethical breach", 14 Oct 2008. http://www.reuters.com/article/2008/10/14/zte-idUSHKG19992320081014

[208] Reuters, Arroyo suspends telecoms deal with Chinese firm, 22 Sept 2007. http://in.reuters.com/article/2007/09/22/idINIndia-29667620070922

[209] *USA v ADT Security Sevices Inc*, United States District Court Southern District Of Florida Case 9:07-cv-81051-WJZ, Federal Trade Commission. http://www.ftc.gov/os/caselist/0423091/071120adtorder.pdf

[210] BBC News, "Qinetiq listings probe launched," BBC News, 26 Jan 2006. http://news.bbc.co.uk/2/hi/business/4651440.stm

[211] Phillips & Cohen LLP, "Scientist blew whistle on faulty military satellite parts; Northrop Grumman pays $325 million to settle case", Press Release, 2 Apr 2009. http://www.phillipsandcohen.com/2009/Scientist-blew-whistle-on-faulty-military-satellite-parts-Northrop-Grumman-pays-325-million-to-settle-case.shtml

[212] Merle, Renae, "Northrop Settles Billing Case: Shipbuilding Unit Allegedly Overbilled US by $72 Million", *The Washington Post*, 9 Aug 2003. http://pqasb.pqarchiver.com/washingtonpost/access/382495171.html?dids=382495171:382495171&FMT=ABS

Illegal government subsidies

Another major controversy relates to illegal government subsidies that companies receive from governments, in relation to which Boeing came under scrutiny. According to the WTO, Boeing has received $5.3 billion in illegal government subsidies over 17 years.[214]

Privacy and security concerns

A major concern relates to privacy and security. Some companies are failing to effectively protect personal privacy and ensure adequate security of their systems and technologies. In 2008, the UK government conducted an enquiry after Atos Origin lost a memory stick with passwords and user names for an important government computer system which was found in the car park of a pub.[215]

Several complaints have been made to the UK Information Commissioner's Office against Experian in relation to breaches of the UK Data Protection Act 1998.[216] Similarly, there have been concerns about data breaches and insecurity at Acxiom.[217]

The US government is scrutinizing ZTE for security concerns. ZTE's Score phone model, sold in the US, apparently has a security vulnerability (hole or backdoor) that might enable third parties to remotely access and control the device.[218]

Sale of technologies to authoritarian and non-democratic regimes

European surveillance companies are reportedly selling technologies to authoritarian or undemocratic regimes. Narus, Boeing's wholly owned subsidiary, has been criticised for selling Deep Packet Inspection (DPI) technology to Egypt Telecom[219] – which facilitates Internet and mobile usage surveillance that could be used to "crack down on opposition voices and dissenting opinions".[220] The UK House of Lords queried Detica's involvement in the selling of surveillance techology to the deposed Tunisian government.[221] Ericsson was criticised for helping the Iranian government to monitor people.[222]

---

[213] Mattera, Phil, Northrop Grumman, 27 March 2010. http://www.crocodyl.org/wiki/northrop_grumman

[214] Heilprin, John, "World Trade Organization: Boeing got $5.3 billion in illegal subsidies", *The Post and Courier*, 13 Mar 2012. http://www.postandcourier.com/article/20120313/PC04/303139905/1012/world-trade-organization-boeing-got-53-billion-in-illegal-subsidies

[215] BBC News, "Probe into data left in car park", 2 Nov 2008. http://news.bbc.co.uk/2/hi/7704611.stm

[216] Information Commissioner's Office, ICO Disclosure Log Response to Request, Reference: IRQ0408803, 26 Aug 2011. http://www.ico.gov.uk/about_us/how_we_comply/disclosure_log/~/media/documents/disclosure_log/IRQ0408803.ashx.

[217] Acxiom Corporation, Annual Reports for 2004 and 2005.

[218] Wagstaff, Jeremy, and Lee Chyen Yee, "ZTE Confirms Security Hole In US Phone", Reuters, 18 May 2012. http://www.Reuters.Com/Article/2012/05/18/Us-Zte-Phone-Idusbre84h08j20120518

[219] Carr, Timothy, "One US Corporation's Role in Egypt's Brutal Crackdown", *Huffington Post*, 28 Jan 2011. http://www.huffingtonpost.com/timothy-karr/one-us-corporations-role-_b_815281.html

[220] Boglioli-Randall, Bonnie, "Local co. Narus reportedly sold technology to Egypt", *Examiner.com*, 5 Feb 2011. http://www.examiner.com/article/local-co-narus-reportedly-sold-technology-to-egypt

[221] UK House of Lords, Daily Hansard, 21 Nov 2011: Column WA20. http://www.publications.parliament.uk/pa/ld201011/ldhansrd/text/111121w0001.htm

[222] http://www.thelocal.se/37098/20111101/; http://www.swedishwire.com/business/7325-swedens-ericsson-accused-of-monitoring-in-iran

Reuters carried a report that Selex Elsag sold the Syrian government its Tetra mobile communications equipment (a system used by military, police and emergency services as well as companies and other organisations) which allows secure, encrypted communications from vehicles and helicopters[223] even though the EU had imposed sanctions on the Syrian government and condemned its violent repression of the uprising against President Bashar al-Assad. Reuters also reported that ZTE has sold "powerful surveillance system capable of monitoring landline, mobile and internet communications", to the Telecommunication Company of Iran (TCI) as part of a €98.6 million ($130.6 million) contract signed in December 2010.[224]

Trovicor has sold its systems for communication interception to Bahrain and other countries in the Middle-East which use these systems to monitor human rights activists. Critics have lashed out against Honeywell for collaborating with the Chinese government and installing sophisticated security systems for the 2008 Beijing Olympic Games which "will remain in place after the games and could be used to monitor dissidents".[225] Similarly, the German press criticised Microdrones' dealings with the Chinese Armed Police Forces.[226]

Perpetuating human rights abuses

G4S received severe criticism for its operations in the "illegal" Jewish settlements in the West Bank and East Jerusalem.[227] According to a news report, G4S provides and maintains screening equipment at many West Bank military checkpoints, installs and maintains alarm systems in retail and commercial outlets in the West Bank, provides security officers to "prevent theft of items in transit or within retail stores", and provides and services perimeter security systems and control rooms in jails inside Israel. This G4S involvement is perceived as perpetuating human rights abuses, facilitating the occupation, and obstructing Palestinian economic development and peace.[228]

Conflict zone profiteering

Conflict zone profiteering is another significant concern. Boeing, in particular, is constantly in the spotlight for its involvement in conflict zones and has been called a conflict zone "profiteer".[229]

---

[223] Mackenzie, James, "Finmeccanica sold radio equipment to Syria: report", Reuters, 5 July 2012. http://www.reuters.com/article/2012/07/05/us-finmeccanica-syria-idUSBRE86410R20120705

[224] Stecklow, Steve, "Special Report: Chinese firm helps Iran spy on citizens", Reuters, 22 March 2012. http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B820120322.

[225] Mattera, Phil, "Honeywell International", *Crocodyl.org*, 27 March 2010. http://www.crocodyl.org/wiki/honeywell_international. Crocodyl is a collaboration of non-profit organisations such as the Center for Corporate Policy, CorpWatch, Corporate Research Project and other contributing organisations and individuals worldwide.

[226] http://www.microdrones.com/company/media-relations/press-releases/chinese-armed-police-forces-has-decided-on-microdrones.php; http://www.heise.de/newsticker/meldung/Geschaeft-mit-ueberwachungs-Flugdrohnen-boomt-178765.html

[227] Macintyre, Donald, "Government asked: Why are you allowing 'tainted' G4S to handle Olympic security?", *The Independent*, 8 June 2012. http://www.independent.co.uk/news/uk/politics/government-asked-why-are-you-allowing-tainted-g4s-to-handle-olympic-security-7827988.html

[228] Ibid.

[229] Business Pundit, "The 25 Most Vicious Iraq War Profiteers", 22 July 2008. http://www.businesspundit.com/the-25-most-vicious-iraq-war-profiteers/; Tim McGloin, "Pentagon Moolah", *NewsObserver.com*, 30 June 2012. http://www.newsobserver.com/2012/06/30/2168781/tim-mcgloin-pentagon-moolah.html

General surveillance-related profiteering and pro-surveillance thrusts

In addition to profiteering from conflict zones, there is an indication of a motivation on the part of some companies to profit from general surveillance. This is illustrated by Experian's featuring on the Defy-ID "Greasy Palms" list – a list that features companies that bid (independently or in conjunction with others) to participate in the UK National Identity Card Scheme, i.e., "publicly identifiable as either profiting or wanting to profit from the introduction of the Identity Cards and the creation of a National Identity Register".[230]

Some security and even surveillance specific companies actively push the surveillance agenda – for instance, Google's products and services (such as Google Analytics) are controversial as they enable and facilitate surveillance of users through collection of user data, user behaviour, IP tracking and creation of user profiles. Google promotes unlimited data storage and retention practices. This is particularly evident in Gmail.[231]

Misleading customers and end users

Another controversy relates to deception of customers and/or end users of surveillance technologies. Experian was accused of "misleading customers who sign up for a supposedly free service to check their financial records".[232] Though Experian offers visitors "free Experian credit reports", consumers who avail themselves of the offer and provide personal information (including their address and credit card details) after receipt of an online credit report are automatically signed up to a full service that charges £14.99 a month. Opting out of the service is reportedly difficult.

Consumerinfo (or Experian Consumer Direct) has been embroiled in legal problems with the US Federal Trade Commission and had to pay $300,000 to settle charges that ads for its "free credit report" offer failed to disclose adequately that consumers who signed up would be automatically enrolled in a credit-monitoring program and charged $79.95.[233] On 23 March 2011, a class action lawsuit was filed against Consumerinfo.com in the Federal Court of the Southern District of California (complaint no. 11CV0569 DMS BLM) alleging that it "takes money from consumers through deception" and that it "does not sell what it advertises" and finally that their advertisements were "false, misleading and deceptive". The complaint was in response to the fact that Consumerinfo claims that the credit scores are important to how lenders evaluate consumers, when they are not.[234]

---

[230] Defy-ID, "Identity Cards - Who Profits? A guide to corporate involvement in the government's Identity Card Scheme". www.defy-id.org.uk/greasypalms.htm**.** Defy-ID, as its name suggests, is a civi society advocacy organisation.

[231] GoogleWatch, "Gmail is too creepy", 21 Sept 2011. http://www.webcitation.org/61rOfd8To

[232] Verkaik, Robert, "Credit check giant Experian accused of 'ripping off' its customers", *The Daily Mail*, 30 Jan 2011. http://www.dailymail.co.uk/news/article-1351866/Credit-check-giant-Experian-accused-ripping-customers.html#ixzz1yzYgHgsY

[233] Federal Trade Commission, "FTC Alleges Ads For 'Free' Credit Report Violate Federal Court Order", Press release, 21 Feb 2007. http://www.ftc.gov/opa/2007/02/cic.shtm

[234] Ulzheimer, John, "Class Action Lawsuit Filed Against Consumerinfo.com, an Experian Company", 29 March 2011. https://www.smartcredit.com/blog/2011/03/29/class-action-lawsuit-filed-against-consumerinfo-com-an-experian-company/

Violation of employees human rights

This is another concern that raises questions about the ethics of surveillance companies. G4S has been accused of infringing its employees' human rights. A report by the UNI Property Services Global Union suggests that G4S has infringed the right of workers to freedom of association and collective bargaining; that it had not paid workers in Africa a living wage; that it regularly denied some workers in Africa and the US legally required breaks for food and rest; and that it deflected responsibility for providing basic social security to the states where it operates.[235]

Anti-competitive practices

Another major concern is anti-competitive policy and practices prevalent within the surveillance industry, particularly those indulged in by large corporations such as Google. Google has a near monopoly in Web search services.[236] In November 2010, the European Commission Directorate General responsible for competition policy launched a large-scale antitrust investigation to determine if Google had abused its dominant market position.[237] The Commission identified four concerns:

1. That in its general search results on the web, Google displays links to its own vertical search services.
2. The manner in which Google copies content from competing vertical search services and uses it in its own offerings.
3. Agreements between Google and partners on the websites of which Google delivers search advertisements
4. Google's restrictions on the portability of online search advertising campaigns from its platform AdWords to the platforms of competitors.

The analysis of this section shows how the surveillance industry is embroiled and implicated in a number of controversies – unethical and even illegal business practices, illegal government subsidies, failing to effectively protect personal privacy and ensure adequate security of their systems and technologies, sale of technologies to authoritarian or undemocratic regimes, perpetuating human rights abuses, conflict zone profiteering, general surveillance-related profiteering, misleading customers and end users, and anti-competitive practices.

Though some of the companies have acknowledged and attempted to rectify these problems (e.g., through implementing elaborate corporate social responsibility practices), this is still a far from ideal situation in relation to protecting the larger social and individual interests. Due

[235] PRNewswire, "G4S Violates Employees' Human Rights, Says UNI Property Services Global Union", 17 Mar 2012. http://www.prnewswire.co.uk/news-releases/g4s-violates-employees-human-rights-says-uni-property-services-global-union-153163355.html

[236] Wilcox, Joe, "The Google Monopoly Begins", *eWeek Microsoft Watch*, 20 Dec 2007. http://www.microsoft-watch.com/content/web_services_browser/the_google_monopoly_begins.html; Fabio, Michelle, "Is Google a Monopoly?" *LegalZoom*, 13 Sept 2011. https://www.legalzoom.com/legal-headlines/corporate-lawsuits/is-google-monopoly; Rosoff, Matt, "Is Google A Monopoly? 'We're In That Area,' Admits Schmidt", *Business Insider*, 21 Sept 2011.

[237] See Almunia, Joaquín, "Policy Statement of VP Almunia on the Google antitrust investigation", Speech, European Commission, SPEECH/12/372 21, Brussels, May 2012. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/372&format=HTML&aged=0&language=EN&guiLanguage=en

to the nature of some of surveillance technologies and the significant threats they pose, we must find a more efficient and effective means of regulating the industry.

3.4 MARKET PROSPECTS AND COMPETITION

This section looks at the future market prospects and growth areas for the surveillance industry, competition and challenges for its future.

In the first part, to determine growth areas, we consider the following sectors (chosen on the basis of data availability): biometrics, Internet surveillance (including deep packet inspection), RFID, smart homes, unmanned aerial systems, x-ray security screening, and video surveillance. Our research provides some indications of how the industry is projected to progress in the coming years.

3.4.1 Future market prospects and growth areas

This section examines the future market prospects and growth areas for the surveillance industry in Europe, based on data from the industry (surveillance companies and their associations),[238] independent sources such as market research companies and government papers. Most of the surveillance reports predict an increasing demand for surveillance solutions (stand-alone and integrated), rapid growth for the industry and strong market growth prospects. This is demonstrated by the statistics collated and presented next.

Biometrics

The Global Biometrics Technology Market (2010-2015) forecast estimates the biometrics market will be worth $11,229.3 million in 2015 (estimated compound annual growth rate of 21.6% from 2010).[239] The forecast further suggests that the Automated Fingerprint Identification System (AFIS) would generate an estimated $3,283.7 million in 2015 (compound annual growth rate of 19% from 2010) due to its increased adoption in national and civil identification systems.

Another report (which studies global biometric technology, based on types and applications market) suggests that the global biometric technology, types and applications market will reach $13.89 billion by 2017 (estimated compound annual growth rate of 18.7%) with North America being the market leader.[240]

At the end of 2015, the Global Touchless Sensing and Gesture Recognition Market (2010-2015) report projects the touchless sensing market (estimated to be growing rapidly) to reach $3656.8 million.[241] The report suggests that

[238] Websites, annual reports, marketing and investor relations brochures.
[239] Marketsandmarkets.com, Global Biometrics Technology Market (2010-2015) – Market forecast by Products, End-User Application and Geography, Report Code: SE 1302, January 2011. http://www.marketsandmarkets.com/Market-Reports/biometric-market-278.html
[240] Marketsandmarkets.com, Next Generation Biometric Technologies Market – Global Forecast & Analysis (2012 – 2017), Report Code: SE 1161, June 2012. http://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html
[241] Marketsandmarkets.com, Global Touchless Sensing and Gesture Recognition Market (2010-2015), Report Code 1584, June 2011. http://www.marketsandmarkets.com/Market-Reports/touchless-sensing-gesturing-market-369.html

> companies are realizing the potential of this market and answering the customer needs regarding better hygienic factors. The touchless biometrics market is also on the rise. The crime rates are increasing and the general public needs some sort of security which is foolproof. These biometric systems are more accurate than the touch-based biometric systems since they are independent of touch. The touchless fingerprint recognition system can take in a picture of a fingerprint even if the finger has a cut on it or in case of iris recognition and face recognition, the features of the iris or the face do not change over the years.

The same report projects the gesture recognition market (a new market with applications in entertainment, consumer electronics, transportation, healthcare, etc.) will "reach $625 million in 2015 from $200 million in 2010 at an expected compound annual growth rate of 25.6% from 2010 to 2015".[242]

Internet surveillance (including DPI)

The Internet surveillance industry is experiencing tremendous growth – boosted in part by heavy demand from public sector surveillance requirements and by private sector surveillance needs. Gartner Inc. suggests "Monitoring employee behavior in digital environments is on the rise, with 60 percent of corporations expected to implement formal programs for monitoring external social media for security breaches and incidents by 2015".[243] Gartner further suggests that "The popularity of consumer cloud services, such as Facebook, YouTube and LinkedIn, provides new targets for security monitoring."[244]

RFID

The RFID market is set to experience growth in the upcoming years. ABI Research (a US-based market intelligence company specialising in global technology markets) projects:

> The market for RFID transponders, readers, software, and services will generate $70.5 billion from 2012 to the end of 2017. The market was boosted by a growth of $900 million in 2011 and the market is expected to grow 20% YOY per annum. Government, retail, and transportation and logistics have been identified as the most valuable sectors, accounting for 60% of accumulated revenue over the next five years.[245]

Goals such as "efficiency, improved operational capability, and the ability to generate useful business intelligence data" will fuel the growth in RFID adoption.[246]

Smart cards

The smart cards market is expected to continue to grow. BCC Research, a market research company, states that "nearly 2.7 billion smart cards were shipped in Europe" in 2011 and the

[242] Ibid.
[243] Gartner, "Gartner Says Monitoring Employee Behavior in Digital Environments is Rising" 29 May 2012. http://www.gartner.com/it/page.jsp?id=2028215
[244] Ibid.
[245] ABI Research, "The RFID Market Will be Worth over $70 Billion Across the Next Five Years", 16 Apr 2012. http://www.abiresearch.com/press/the-rfid-market-will-be-worth-over-70-billion-acro
[246] ABI Research, RFID Market by Application and Vertical Sector, Research Report. 2012. http://www.abiresearch.com/research/product/1006085-rfid-market-by-application-and-vertical-se/

European smart card market could reach $2.8 billion by 2017 (as compared to $1.8 billion in 2011).[247]

Unmanned aerial systems

Based on the increasing thrust and priority (both military[248] and civil/commercial) on deploying unmanned aerial vehicles (drones), the global market is expected to reach $94 billion over the next 10 years.[249] "Drones also form a key part of the European Commission's $410 million plan to improve border security."[250] Another market study on unmanned aerial vehicles by the Teal Group suggests that expenditure on unmanned aerial vehicles will double from 2012 expenditures of $6.6 billion annually to $11.4 billion in the next 10 years (despite defence cuts).[251]

X-ray security screening

The Homeland Security Research Corporation[252] reports that "the global X-ray security screening market (including systems sales, service, and upgrades) is forecast to grow from $1.2 billion in 2011 to $1.9 billion by 2016."[253] Its analysts forecast "growth at a CAGR of 10% of the global X-ray screening market, led by a dramatic expansion of the Chinese civil aviation (two out of three new airport projects are in mainland China) and internal security funding. Other key markets are terror-troubled India and the replacement market of the US and Europe."[254]

Video surveillance

Continued growth is forecast for video surveillance (CCTV covering, for example, surveillance cameras, recording equipment and video encoders). IMS Research estimates that the market will grow to $20.5 billion by 2016, that network cameras will account for between 50% of total new camera sales by 2015 and that a global growth of 25-30% for network video is expected in the coming years.[255] IMS Research also expects 2013 to be "the tipping point when world network video surveillance equipment sales overtake analogue video surveillance equipment sales".[256]

---

[247] BCC Research, Smart Card Technologies and Global Markets -- Focus on Europe, July 2012. http://www.bccresearch.com/report/smart-card-europe-markets-ift097a.html

[248] Particularly in Europe, Russia and the United States. Military use includes intelligence gathering, targeting, and situational awareness, and attack missions.

[249] Glover, Tony, "Spies in the sky spark privacy fears", *The National*, 19 Aug 2012. http://www.thenational.ae/thenationalconversation/industry-insights/technology/spies-in-the-sky-spark-privacy-fears

[250] Ibid.

[251] Teal Group, "Teal Group Predicts Worldwide UAV Market Will Total $89 Billion in Its 2012 UAV Market Profile and Forecast", *PR Newswire*, 11 April 2012. http://tealgroup.com/index.php/about-teal/teal-group-in-the-media/3/79-teal-group-predicts-worldwide-uav-market-will-total-89-billion-in-its-2012-uav-market-profile-and-forecast

[252] A Washington, DC-based international market research and strategic consulting company providing premium market, technology and industry expertise for global clients.

[253] Homeland Security Research Corporation, X-Ray Security Screening: Technologies & Global Market Outlook – 2012 Edition. http://www.homelandsecurityresearch.com/2012/05/x-ray-security-screening-technologies-global-market-outlook-2012-edition/

[254] Ibid. CAGR = compound annual growth rate.

[255] Axis Communications, The security market. http://www.axis.com/corporate/security_market.htm

[256] IMS Research, "For IP-based Video Surveillance, the Future is Now", *Press release*, 12 June 2012. http://imsresearch.com/press-release/For_IPbased_Video_Surveillance_the_Future_is_Now

Meanwhile, the Homeland Security Research Corporation believes that the next decade will be

> marked by the fusion of CCTV with Biometrics, and human behavioral signatures, which will create a new multibillion premium security market of CCTV-Based Remote Biometric & Behavioral Suspect Detection. This family of technologies results from the need to remove the bottlenecks of current CCTV and people screening systems, the inability to provide reliable real-time alarm when suspects are viewed by the CCTV camera and the staggering cost of security officers, required to operate 24/7 CCTV workstations. This fusion of technologies brings significant growth opportunities to CCTV, biometric and IT systems manufacturers, security systems integrators and entrepreneurs. The new market (including systems sales, upgrades and post warranty service) is forecasted to reach $3.2 billion by 2016, growing at a CAGR of 33%.[257]

In this section, we have presented various projections for different surveillance areas such as biometrics, Internet surveillance (including deep packet inspection), RFID, smart homes, unmanned aerial systems, x-ray security screening, and video surveillance. All the projections show positive growth trends. This means that the future of surveillance seems set and companies might be encouraged to invest further in these solutions to profit from the demand for these solutions.

3.4.2 Trends

We note a few trends from our analysis of the surveillance industry. First is a substantial growth of public sector demand for surveillance bolstered by the adoption of identity schemes,[258] and terrorist detection technologies and markets.[259] Second is an increase in the demand for civil/commercial surveillance. Third is development of a global industry in surveillance. Fourth is an increase in integrated surveillance solutions. And fifth is a rise in international surveillance wars.[260] Many countries and companies alike are using surveillance technologies to spy on and manipulate not only citizen-consumers but also each other.

3.4.3 Competition

---

[257] Homeland Security Research Corporation, *CCTV Based Remote Biometric & Behavioral Suspect Detection: Technologies & Global Markets – 2011-2016*. http://www.homelandsecurityresearch.com/2011/02/cctv-based-remote-biometric-behavioral-suspect-detection-market-2011-2016/

[258] See http://www.eurosmart.com/images/doc/International-events/autres2012/2012-05-02_sdw_london_speech_eurosmart_eid_wg_v3.0_final.pdf

[259] Homeland Security Research Corporation, *Global Standoff Terrorist Detection Technologies & Markets – 2010-2014*, March 2010. http://www.homelandsecurityresearch.com/2010/03/global-standoff-terrorist-detection-technologies-markets-2010-2014/. The report notes "The threat posed by suicide bombers is the key to the emergence of transformational counter-terror technologies and tactics. The maturity and deployment of several standoff technologies capable of detecting suicide and other terrorists at a safe distance will change the landscape of homeland security and the war against terror."

[260] As highlighted by Ron Deibert, director of the Canada Centre for Global Security Studies and the Citizen Lab. Torstar News Service, "Surveillance spyware spreading to smartphones", *Metro News*, 31 August 2012. http://metronews.ca/news/canada/355128/surveillance-spyware-program-spreading-to-smartphones/. In this regard, we note that the Dutch Ministry of Justice and Security has proposed powers "for the police to break into computers, install spyware, search computers and destroy data," even extending to computers located outside the Netherlands. Bits of Freedom has strongly opposed the move. See Bits of Freedom, "Duch proposal to search and destroy foreign computers", 18 Oct 2012. https://www.bof.nl/2012/10/18/dutch-proposal-to-search-and-destroy-foreign-computers/.

Competition occurs at different levels in the surveillance industry. Companies compete on manufacture, sale, product delivery, product lines, prices, support.[261] Competition can result in reduced revenues and market share for companies, and therefore companies have policies and take strategic measures (e.g., acquisitions, mergers)[262] to deal with it.

Surveillance companies from Europe face stiff competition from companies based outside the European Union.[263] A substantial majority of the surveillance companies are headquartered outside the European Union. Companies from countries such as the USA, China, Russia, Israel and India, are vying with each other and with European companies to gain a share of the European surveillance market. This trend will continue in the future.

3.4.4 Challenges for the future

Despite the generally positive outlook for the surveillance industry, it is not without challenges.

One challenge is the lack of security awareness and attitudes. This results in a decreased demand for security and surveillance products and services.

Another challenge is stricter government regulation. Stringent regulatory requirements may stifle the development and growth of the industry.

There are also financial challenges – higher duties and costs applicable to surveillance products might slow the industry's future prospects and growth.

There is also the possibility that some surveillance technologies may be rejected by the public due to privacy, ethical and other human rights concerns.

Competition is another challenge the surveillance industry in Europe faces; it the industry is to successfully flourish, it must learn to deal with this.

3.5 INDUSTRY ASSOCIATIONS

Associations are highly influential entities in industry; this is no less true for the surveillance industry. For the purposes of this section, an industry association refers to an organisation or entity formed and associated with the promotion of business and/or industry interests and where relevant the development of guidelines and standards to advance the industry. This section will identify and analyse surveillance-related industry associations, highlight their role (visions, aims and objectives) and examine their activities. This will help us assess the role these industry associations play in relation to the surveillance industry, their influence and overall impact on European security research and policy.

3.5.1 Surveillance-related industry associations and their nature

There are various industry associations operating in Europe in the security and specific surveillance areas (e.g., biometrics, communications surveillance, dataveillance, location

[261] Tyco International, *2011 Annual Report*. www.tyco.com/2011annualreport/
[262] Section 3.3.5.7 (acquisitions and mergers)
[263] See Section 3.3.5.8 (growth of non-EU players)

determination technologies, sensors and visual surveillance). This section identifies prominent surveillance-related industry associations based on a review of surveillance company and association websites, security industry information, academic literature and media reports.

Annex 3 lists European surveillance-related industry associations. The analysis in this table demonstrates the variety of surveillance-related industry associations in Europe – all with varied motivations and focuses, including security solutions, aerospace, defence and security, geographic information, smart cards,RFID, biometrics, direct marketing, private security, identity, nanotechnology, unmanned aerial systems, Internet communications, mobile technologies. Some of these associations are large (e.g., the Internet Advertising Bureau Europe, the ADS group, the Direct Marketing Association) while others such as the Security Alliance are a partnership of only 15 members.

Some associations operate globally (e.g., European Association for e-identity and Security**,** GSMA, Smartex), while others regionally (e.g., Bundesverband der Hersteller- und Errichterfirmen von Sicherheitssystemen, Federation of European Direct and Interactive Marketing). Some associations focus on an area within a region (e.g., Central Eastern European Smart Card Association and Nordic Biometrics Forum), while others concentrate in promoting their members' interests at the national level (e.g., Association for Geographic Information, RFIDLab Finland).

The associations have different membership categories. Some associations restrict their membership to industry (e.g., Bundesverband der Hersteller- und Errichterfirmen von Sicherheitssystemen, Bundesverband der Deutschen Luft- und Raumfahrtindustrie e.V, British Security Industry Association), while other associations are more broad-based and open to stakeholders of different categories (e.g., Danish Biometrics, Eurosmart, UVS International).

In addition to the above European associations, the following associations operate internationally:

Association	Host country	Industry segment
Asia Pacific Smart Card Association (APSCA)[264]	China	Smart cards
Asian Professional Security Association (APSA)[265]		Security industry
Australian Security Industry Association (ASIAL)[266]	Australia	Security industry
Central Association of Private Security Industry in India (CAPSI)[267]		Security industry
Digital Advertising Alliance[268]	USA	Online behavioural advertising
Digital Analytics Association [269]	USA	
GlobalPlatform[270]	USA	Secure chip technology
International Direct Marketing Federation (IDMF)[271]		Direct marketing
Multos Consortium[272] (*smart cards*)		Smart cards

[264] www.apsca.org
[265] http://www.apsathailand.com/
[266] www.asial.com.au
[267] http://www.capsi.in/
[268] http://www.aboutads.info/
[269] Formerly the WAA. http://www.aboutads.info/
[270] http://www.globalplatform.org/aboutus.asp
[271] http://www.idmf.com/

National Association of Security Companies in the US (NASCO)[273]		Security industry
Network Advertising Inititative (NAI)[274]	USA	Online advertising
New Zealand Security Association (NZSA)[275]		Security industry
Open Network Video Interface Forum (ONVIF)[276]	USA	*IP-based physical security products*)
Russian Security Industry Association[277]	Russia	Security industry
Security Industry Alliance in South-Africa (SIA)[278]		Security industry
Global Lawful Interception Industry Forum[279]	USA	Lawful interception products and services
International Biometric Industry Association[280]	USA	Biometrics
International Card Manufacturers Association (ICMA)[281]	USA	Smart cards
International RFID Business Association- (RFIDba)[282]	USA	RFID
World Security Federation (WSF)[283]		International security issues

3.5.2 Goals

Though the various industry associations operate in different sectors (aerial surveillance, biometrics, Internet, location determination, mobile surveillance, physical security, etc.), the following goals are evident from a study of their vision, aims and objectives.

Promote and increase the use of members products and services

One of the main objectives of security and surveillance industry associations is to promote and increase the use of their members' products and services.

Some industry associations have specific sectoral interests. For example, the mission of the Association for Geographic Information (AGI) is to "maximise the use of geographic information (GI) for the benefit of the citizen, good governance and commerce".[284] The European NanoBusiness Association (ENA) promotes "the professional development of the emerging business of nanotechnology at the European level".[285] Eurosmart (a Brussels-based smart security industry association) promotes smart secure devices and smart secure devices systems by:

- encouraging open system design;
- encouraging interoperability of components and systems;
- promoting an image of high security around Smart Secure Device applications;

[272] http://www.multos.com/
[273] http://www.nasco.org/
[274] http://www.networkadvertising.org/
[275] http://www.security.org.nz/
[276] http://www.onvif.org
[277] http://www.rasi.ru/index_eng.php
[278] www.securityalliance.co.za/
[279] www.gliif.org/
[280] www.ibia.org/
[281] www.icma.com
[282] www.rfidba.org/
[283] http://www.worldsecurityfederation.org/
[284] AGI, Mission and Objectives. www.agi.org.uk/
[285] ENA, www.nanoeurope.org

- defending the reputation and ethics of the Smart Security Industry including by fighting counterfeiting or violations of intellectual property rights.[286]

Other associations have broader visions. For instance, Intellect suggests it "works with and for members to develop the UK's capability to support a strong and growing technology sector".[287] The Internet Advertising Bureau (IAB) Europe seeks to "protect, prove, promote and professionalise the digital industry in Europe". [288]

Find solutions for industry problems

Surveillance industry associations aim to "develop meaningful solutions"[289] for industry problems and concerns. The Ligue Internationale des Sociétés de Surveillance suggests it can develop "techniques and organisational methods more effective than those possible to individual initiative and local resources" to solve problems that are "difficult or insoluble at a national level" which would "improve and increase the overall potential of private security activity in the world".[290]

Assist members with market knowledge

Surveillance industry associations aim to assist their members gain knowledge of actual and potential markets for their products and services. They facilitate their entry into markets at international, regional or local levels. They aim to generate and disseminate data on markets, create awareness of market developments, and familiarise their members with market rules and regulations.

Increase and facilitate collaboration

Surveillance industry associations increase and facilitate collaboration between members, and between members and non-members. Within the organisation, industry associations facilitate member partnerships and collaboration. They seek to provide platforms for members to interact with one another and forge mutual bonds that facilitate mutual business and industry opportunities. Industry associations also endeavour to provide the means and modes for their members to interact and collaborate with external stakeholders such as government bodies, academia, research institutions, civil society, the media and the public. The European Corporate Security Association (ECSA), for instance, aims "to liaise and to promote synergy with relevant Academic, Research, Scientific, Public & Private Organizations and Associations".[291] SIGNATURE, the European Security and Innovation Network, encourages collaboration between "clusters, SMEs and other organisations in the security sector" through common classification and micro-cluster activity. [292]

Promote research and development

Another key objective of surveillance industry associations is promoting research and development. Danish Biometrics, for instance, states that "by research and innovative

[286] Eurosmart, Missions. www.eurosmart.com/index.php/about/missions.html
[287] Intellect, About Intellect. www.intellectuk.org/about-intellect/who-we-are
[288] Internet Advertising Bureau (IAB) Europe, Mission. www.iabeurope.eu/
[289] International Imaging Industry Association (I3A) Europe. http://www.i3a.org
[290] The Ligue Internationale des Sociétés de Surveillance, Objectives. www.security-ligue.org/objectives/
[291] ECSA, www.ecsa-eu.org/
[292] SIGNATURE. http://www.securityinnovationnetwork.com/

exploitation of new technologies as biometrics we should strengthen our compositeness and our cohesive energy in society".[293] The Fingerprint Society aims to "advance the study and application of fingerprint evidence and to facilitate the co-operation among persons interested in this field of personal identification".[294] The European NanoBusiness Association lays emphasis on "ensuring that basic research is becoming a real technology transfer to the private sector".[295]

Establish policy, guidelines and standards for the industry

With the intent of maintaining and continuously improving the quality of products and services, industry associations such as the European Telecommunications Standards Institute – Technical Committee on Lawful Interception (ETSI-LI) seek to produce standards and specifications for surveillance products and services to align and enable compliance with policy and legal requirements, whether at international, regional or national levels.[296] The standards and specifications may be produced in partnership with other technical bodies, projects and organisations. Eurosmart, for example, aims to "support the standardisation of Smart Secure Devices and Smart Secure Devices systems by: orienting the content of standards and promoting European standards world-wide; launching initiatives for building common specifications for future applications".[297]

Increase public acceptance of products and services

One important objective of industry associations is to engage with the public and raise awareness of concerns such as security, safety, crime prevention and prosecution that would ultimately drive and boost the demand for the surveillance industry's products and services. This vision is particularly explicit in the objectives of the following associations: the Bundesverband der Hersteller- und Errichterfirmen von Sicherheitssystemen (BHE), the British Security Industry Association (BSIA), UK Security & Resilience Industry Suppliers Community (RISC), the Unmanned Aerial Vehicle Systems Association (UAVS) and Unmanned Vehicle Systems International (UVS International).

Influence policy

Industry associations seek to influence policy, particularly security policy, at different levels – e.g., government, law, research. A security policy that favours surveillance will ultimately boost demand for surveillance products and services, creating a "favourable environment for growth and employment".[298] The surveillance industry's success and profitability hinges on the demand for surveillance services. Influencing policy is essential to ensure that it does not have an adverse effect on industry – e.g., an anti-body scanning policy would affect companies in such business by impacting the demand for such services. Industry associations, therefore, devote substantial resources to actions influencing policy that is favourable to and drives the industry.[299]

---

[293] Danish Biometrics, International. http://danishbiometrics.org/international/
[294] The Fingerprint Society, History. www.fpsociety.org.uk/thesociety/history.html
[295] Nenotechviews.com, The European NanoBusiness Association. www.neno-tech-views.com/european-nanobusiness-association-ena
[296] ETSI-LI. www.etsi.org/website/technologies/lawfulinterception.aspx
[297] Eurosmart, Missions. www.eurosmart.com/index.php/about/missions.html
[298] Intellect, About Intellect. www.intellectuk.org/about-intellect/who-we-are
[299] See section 3.3.8 on Lobbying and Advocacy.

Drive industrial growth and innovation

Another major objective of industry associations is to boost industrial growth and drive innovation. For example, GSMA Europe is "focused on innovating, incubating and creating new opportunities for its membership, all with the end goal of driving the growth of the mobile communications industry".[300] Industry associations aim to help their members make the right business decisions about products and services that help them increase their profits, boost industrial growth and benefit the economy at large.

3.5.3 Activities of industry associations

In pursuit of their vision, aims and objectives, industry associations undertake a variety of activities, which we outline next.

Events organisation and sponsorship

Industry associations organise and sponsor formal and informal events and activities. These include: awards functions, competitions, conferences, exhibitions, expos, face-to-face meetings, group discussion forums, networking lunches and dinners, road shows, seminars, trade fairs and workshops.

For example, the Association of Security Consultants (ASC) organises the annual international CONSEC Conference and Exhibition and presents the Imbert Awards.[301] The Association for Geographic Information organises an annual conference and trade exhibition.[302] The BDLI organises the ILA Berlin Air Show International Aerospace Exhibition.[303] The SIMalliance organises the SIMposium showcasing new technologies and market challenges[304] and hosts the annual SIMagine Awards.[305] The International Imaging Industry Association (I3A) organises the VISION 2020 Imaging Innovation Awards (for intelligent imaging solutions for capturing, storing, sharing, managing, processing or printing). ADS and the Danish Defence and Security Industries Association (FAD),[306] held a conference and dinner for defence and security sector companies from the UK and Denmark in London on 26 September 2012.[307]

Industry associations often offer members fee discounts for their own and third-party organised events. These varied events and activities provide industry association members platforms to promote their products and services, and network with a wide variety of stakeholders such as Government Ministers, parliamentarians, bureaucrats, academia, researchers, regulators and the media.

---

[300] GSMA Europe. http://www.gsma.com/gsmaeurope/
[301] Association of Security Consultants (ASC), Reasons to join. http://www.securityconsultants.org.uk/reasons_to_join
[302] AGI. www.agi.org.uk/geocommunity/
[303] ILA, ILA Berlin Air Show. www.ila-berlin.de/ila2012/presse/presse_volltext_e.cfm?id_nr=26
[304] Informa UK Ltd. http://simposiumglobal.com/
[305] SIMagine Awards. http://simposiumglobal.com/simagine-awards/. The awards "reward the best secure technologies and services on a device accessing wireless networks and leveraging the use of a secure element (i.e. USIM/ UICC, MIM, Embedded, SD Card etc.)".
[306] FAD. www.fad.di.dk
[307] FAD, "UK – DENMARK Defence and Security Industry Seminar and Dinner", 14 May 2012. http://fad.di.dk/About%20FAD/Newsandpress/Pages/26%20September%20UK%E2%80%93DK%20Defence%20and%20Securtiy%20Industry%20Seminar.aspx

Information, advice and training

Industry associations provide various types of information to members: about current and prospective international, regional and national markets; regulatory policy; technological developments; ethical issues; high-level policy strategy; company-specific matters; industry insights; and general industry information.

The **websites** of industry associations function as vast information portals for members and external audiences. While some information is freely accessible, other information and resources are restricted to members or subscribers. The websites carry information on: organisational profiles and activities, jobs, tenders and contracts, latest developments (industrial, legal or otherwise), business opportunities, allied research and studies, best practice and standards, statistics and industry events.

Industry associations provide information to members through **newsletters and news updates.** Smartex offers its members a daily news update on smart technology, biometrics, NFC, RFID, M2M and smart payments. The RFIDLab Finland sends its members RFID technology related news and events.

Industry associations such as the European Corporate Security Association (ECSA) conduct **information and training sessions.** The ECSA's seminars include topics such as predictive profiling and terrorist threat mitigation, advanced security questioning, and Internet security for dummies.[308] The Irish Security Industry Association (ISIA) has a training division, ISIT Skillnet and conducts Electronic Security seminars.[309]

Industry associations produce **white papers** (e.g., IAB Europe's "Brand Advertising and Digital" [310] and the CoESS White Paper and Guidelines on Critical Infrastructure Security and Protection – The Public-Private Opportunity[311]). They generate **reports and insights** on surveillance issues. IAB Europe launched the Consumer Barometer, in collaboration with with TNS Infratest and Google, to provide consumer behavioural insights.[312] In addition, industry associations such as EOS,[313] FEDMA[314] and the CoESS[315] produce **position papers** on a variety of issues.

Networking activities

In pursuit of their networking objectives, industry associations conduct various activities. One significant example is the maintenance of member contact databases or member directories

[308] ECSA, Security Seminars. http://www.ecsa-eu.org/index.php?option=com_content&view=article&id=120&Itemid=153#
[309] ISIA, Membership benefits. http://www.isia.ie/isia/Main/2008_About_Benefits.htm
[310] IAB Europe, 2010. http://www.iabeurope.eu/committees/brand-advertising.aspx
[311] http://www.coess.org/?CategoryID=204
[312] Consumer Barometer. http://www.consumerbarometer.com/#?app=about&aboutId=0
[313] EOS, Advocacy Successes: Common Positions for the Future Market. http://www.eos-eu.com/?Page=advocacy. On subjects such as concrete action for the EU Internal Security Strategy, a proposal for a Third Party Liability regulation (with ASD), Security, Privacy and Data Protection (initiated with ASD), a "Non Paper" on Transport Security and Positions on specific "hot issues" (e.g., civil aviation security).
[314] FEDMA, FEDMA Position Papers. http://www.fedma.org/index.php?id=55 (data protection, privacy)
[315] CoESS, Tools, Studies and Positions. http://www.coess.org/?CategoryID=204 (on EU Public Procurement Policy)

(e.g., the ADS Group, BHE membership directory, SIGNATURE's online directory of security expertise). Industry associations foster the growth of industry communities such as the Smartex forums.[316] Industry associations are involved in consultation activities with other like-minded associations. For instance, the SIMalliance collaborates with the GSMA, ETSI and the GlobalPlatform.

Research funding, collaboration and dissemination

Industry associations fund and collaborate in research and development activities. IAB Europe organises research projects in collaboration with national Internet advertising bureaus. It disseminates findings of market research companies such as comScore Europe, Insites Consulting, Screen Digest, TNS, Gemius and Nielsen to its members and maintains the Knowledge Bank (a data repository on the European and global online advertising market). It institutes research awards. Eurosmart has an "education mission" which includes training sessions in ICTs[317] and a machine-to-machine (M2M) module for the Smart University. The RFID Lab conducts research in collaboration with its members to advance the spread of RFID-technology.

Best practices, standards and certification

Industry associations publish guidelines and codes of practice to offer guidance and enable member companies to follow established best practice and requirements. For instance, Intellect has published guidelines on data security and data protection,[318] and marketing under the privacy and electronic communications regulations 2003.[319] The BSIA draws up codes of practice and submits them for consideration as British Standards. BHE has guidelines for video surveillance systems.[320]

Industry associations **develop and set standards** for surveillance sectors. For instance, UVS International promotes "establishment of unmanned aircraft systems (UAS) related standards, airworthiness, certification & air traffic management (ATM) norms on national, pan-European and international levels" and co-ordinates "the various national efforts on a global level, in order to contribute towards an early harmonization of the diverse national approaches". Eurosmart pursues card standardisation. The Irish Security Industry Association (ISIA) participates in European Working Committees on standards and training through CoESS. The BSIA has representatives on European standards committees; the ITSPA is actively involved in Technical Forums on future standards.

Some industry associations are involved in **certification and accreditation** activities. BHE, in particular, certifies the quality of its members in accordance with applicable standards and regulations and awards the BHE-quality seal.[321] The ITSPA too awards a Quality Mark if members meet its criteria (i.e., compliance with all ITSPA-approved Best Common Practice

[316] Smartex, Forum Overviews. http://www.smartex.com/files/?Membership_Information:Forum_Overviews
[317] Eurosmart, http://www.eurosmart.com/
[318] Intellect, "Intellect Data Security and Data Protection Guidelines for Offshoring and Outsourcing", 2008. http://www.intellectuk.org/publications/business-guidance/4055
[319] Intellect, "Marketing under the privacy and electronic communications regulations 2003", 2001. http://www.intellectuk.org/publications/business-guidance/4407. Further guidance is available at the following link: http://www.intellectuk.org/publications/business-guidance/
[320] BHE, "BHE policies for video surveillance systems". http://www.bhe.de/die-fachbereiche/videoueberwachung/bhe-richtlinien-fuer-video-ueberwachungsanlagen.html
[321] BHE, http://www.bhe.de/der-verband/qualitaetsmanagement/

Documents, provision of access to and awareness of emergency services for customers; provision of evidence to customers of membership of recognised dispute resolution scheme and provision of a Company Single Point of Contact (SPOC) to facilitate improved communications).[322]

Media and public relations

Industry associations are actively involved in media and public relations activities. They issue press releases, produce brochures and conduct information sessions. These serve to inform others about the organisation's vision and activities and more often than not put a positive spin on their members' products and services. Many industry associations have dedicated teams focussing on media and public relations.

Strategic partnerships

Industry associations forge partnerships with various organisations that help them advance their vision and objectives. For example, the Confederation of European Security Services (CoESS) has formal co-operation agreements with international security organisations such as the World Security Federation (WSF), Russian Association of Security Industry (RASI), Security Industry Alliance in South-Africa (SIA), Asian Professional Security Association (APSA), Central Association of Private Security Industry in India (CAPSI), Australian Security Industry Association (ASIAL), New Zealand Security Association (NZSA), National Association of Security Companies in the US (NASCO) and the Ligue Internationale des Sociétés de Surveillance.

At the European level, the CoESS partners with the European Commission (Employment, Social Affairs and Inclusion, Internal Market, Enterprise and Industry, Education and Culture, Justice, Home Affairs, Mobility and Transport, Enlargement, Economic and Financial Affairs and External Relations), the European Parliament and the Council of the European Union. It is "formally recognised by the EU institutions, is a privileged partner and is granted consultative status in many EU dossiers", thus enabling it to represent the private security services sector.[323]

The ETSI TC-LI partners with other ETSI technical bodies, projects and external organisations to develop technical standards and specifications for lawful enforcement technologies.[324]

Lobbying and advocacy

Industry associations engage in lobbying activities on behalf of their members. For example,the BSIA "lobbies key organisations/bodies to form valuable working partnerships and achieve desirable changes e.g. Members of Parliament, the Home Office, Association of Chief Police Officers, Association of British Insurers".[325] It has "lobbied for regulation of the security industry for over 15 years, culminating in the introduction of the Private Security Industry Act 2001 and the launch of the Security Industry Authority".[326]

[322] ITSPA, "Quality Mark". http://www.itspa.org.uk/quality.html
[323] Confederation of European Security Services. http://www.coess.org/?CategoryID=177
[324] ETSI, Lawful Interception. www.etsi.org/website/technologies/lawfulinterception.aspx
[325] BSIA, About the BSIA. www.bsia.co.uk/about-us
[326] Ibid.

Eurosmart lobbies international and national bodies involved in trade issues such as GATT, taxes, dumping. The Transparency Register[327] reveals Eurosmart had four persons involved in lobbying-related activities and spent under €50,000 representing its interests to EU institutions (FY 05/2010 – 05/2011).[328]

The Irish Security Industry Association (ISIA) has representatives in the Security Congress of Ireland, on the board of the Private Security Authority (PSA) and on the Joint Labour Committee of the security industry. It participates in various European Working Committees on standards and training through the CoESS. It provides its members with the "facility to lobby the relevant bodies including the PSA, Government Departments, An Garda Siochana".[329]

The I3A lists "advocacy" as one of its activities, has an Advocacy Interest Group and engages in the following advocacy activities: representing the imaging industry to governments and regulatory bodies; co-operating with legislative committees; working administrative agencies, regulatory bodies and other governmental groups in the United States and worldwide.[330]

On the basis of the above analysis, we can conclude that surveillance industry associations play a key role in the surveillance industry – in promoting its growth and development and in pushing the adoption of surveillance solutions.

There are a variety of surveillance industry associations operating globally, regionally and nationally in security and specific surveillance areas (e.g., biometrics, communications surveillance, dataveillance, location determination technologies, unmanned aerial systems). These associations vary in nature, motivations and focus (broad versus sectoral or topical). Some restrict membership; others are more open.

The associations perform various functions: promote and increase the use of their members' products and services; increase and facilitate collaboration between members, and between members and non-members; promoting research and development; produce standards and specifications for surveillance products and services; engage with the public and raise awareness of concerns such as security, safety, crime prevention and prosecution which theoretically will ultimately drive and boost the demand for the surveillance industry's products and services; influence policy; and boost industrial growth and drive innovation.

Surveillance industry associations benefit the surveillance industry (and their members in particular) through a variety of activities: formal and informal events and sponsorhips; information advice and training; networking; research funding, collaboration, dissemination; best practices, standards, certification; media and public relations; strategic partnerships; and lobbying and advocacy.

[327] The Transparency Register set up and operated by the European Parliament and the European Commission provides "citizens with a direct and single access to information about who is engaged in activities aiming at influencing the EU decision making process, which interests are being pursued and what level of resources are invested in these activities". http://europa.eu/transparency-register/

[328] European Commission, "Eurosmart" Transparency Register. https://ec.europa.eu/transparencyregister/public/contact/contact.do?locale=en

[329] ISIA, Membership benefits. www.isia.ie/isia/main/2008_About_Benefits.htm

[330] I3A, Advocacy. www.i3a.org/technologies/advocacy/

These surveillance associations do evidence some social responsibility (for instance, by establishing industry standards and guidelines or through certification). Because of their influence and the clout they wield, they could be harnessed in protecting society and individuals from some of the effects of surveillance (or countering the effects of surveillance). This should be explored further in terms of increasing the resilience of surveillance societies.

3.6 IMPACT OF THE SURVEILLANCE INDUSTRY ON SECURITY POLICY

This section explores the relationship of the surveillance industry with European security policy. It assesses how the surveillance industry influences and impacts European security policy and research and shows why the industry is an important stakeholder in furthering the business of surveillance within the umbrella of security policy and research.

The Statewatch *NeoConOpticon* report on the EU security-industrial complex highlighted "a number of prominent European corporations from the defence and IT sectors have enjoyed unprecedented involvement in the development of the security 'research' agenda".[331] This report followed *Arming Big Brother* (2006) which had expressed strong criticism of corporate influence on the EU security programme and the dangers of the "security-industrial complex".[332] These reports broadly focused on security; we will more specifically look the role of surveillance companies, particularly the ones we encountered in our research and their impact on EU security policy and research.

3.6.1 Influence in regional organisations

Surveillance companies exert a great amount of influence through participation in security policy-related bodies such as the European Defence Agency (EDA), the European Organisation for Security (EOS), the European Security Research and Innovation Forum (ESRIF) and the European Security Research Advisory Board (ESRAB).

European Defence Agency

The European Defence Agency (EDA)[333] is a European Union agency established under a Joint Action of the Council of Ministers on 12 July 2004, "to support the Member States and the Council in their effort to improve European defence capabilities in the field of crisis management and to sustain the European Security and Defence Policy as it stands now and develops in the future". The EDA "acts as a catalyst, promotes collaborations, launches new initiatives and introduces solutions to improve defence capabilities". The EDA "brings together all four communities of the chain, from planners to researchers, from programme developers to the production side that is industry".[334]

Participating Member States (i.e., Ministries of Defence) "own" the EDA, and make decisions about defence planning, research and technology investment, equipment procurement and defence industrial and market issues.

---

[331] Hayes, Ben, *NeoConOpticon: The EU Security-Industrial Complex*, TNI/Statewatch, 2009. www.statewatch.org/analyses/neoconopticon-report.pdf

[332] Hayes, Ben, *Arming Big Brother: The EU's Security Research Programme*, TNI/Statewatch., Amsterdam, 2006. http://www.statewatch.org/analyses/bigbrother.pdf

[333] http://www.eda.europa.eu/

[334] http://www.eda.europa.eu/Aboutus/Howweareorganised

European Organisation for Security

The European Organisation for Security (EOS)[335] "represents the interests and expertise of 39 Members involved in Security providing technology solutions and services from 13 different countries of the European Economic Area" (i.e., more than 65% of the European security market and 2 million employees in Europe). It is "one of the most important voices in the public-private dialogue with European and Member States Institutions on security issues" and "facilitates the coherent development of the European Security Market, supporting the widespread deployment and implementation of solutions and services to provide security and safety to citizens, governments and economy".[336]

According to EOS, it is "a tool for European security stakeholders for the comprehensive implementation of existing (and future) security strategies and solutions at National, European and International level". It achieves its objectives by:

- providing coherent links across different sectors (with associations and members of various associations in the domain of ICT, civil protection, border control, and the protection of critical infrastructures), and different European countries (national organisations for security), as well as with different European institutions and, where necessary, national or international organisations (e.g., UN, OSCE, US-DHS), while also promoting global approaches (architectures and integrated systems);
- establishing a dialogue between the public and private sectors at the highest level.

To improve the knowledge of policy-makers (on the existing and future solutions as well as on the position of the European security private sector), EOS

- acts as adviser to and/or has a close dialogue with various Directorates-General of the European Commission such as Home Affairs, Maritime Affairs and Fisheries, Information Society and Media, Energy, European Community Humanitarian Office, Mobility and Transport, the Joint Research Centre, European External Action Service and EC Agencies (Frontex and ENISA), European Defence Agency, the European Parliament (Committee on Civil Liberties, Justice and Home Affairs, Sub-committee on Security and Defence, Committee on Industry, Research and Energy, Committee on Transport and Tourism, and the Committee on Internal Market and Consumer Protection), and the Council (e.g., anti-terrorism co-ordinator), and European organisations for standardisation (e.g., CEN) in support of the definition of security policies, new regulations, future research programs, etc.;
- proposes to the European and national administrations common recommendations prepared by experts of EOS Member companies (White Papers, Position Papers) for the development of concrete actions in the different security sectors.

EOS partners include: Altran (France), Amper (Spain), ASD (Belgium), Atos (Spain), Avio (Italy), Thales (France), TNO (Netherlands), Vitec (France), Teletron Italy, STM (Turkey), Smiths Detection (Belgium), Siemens (Germany), Selex Sistemi Integrati (Finmeccanica), Safran Morpho, Saab (Germany), Rapiscan Systems (UK), Multix (France), L-3 Communications (UK), KEMEA (Greece), IVECO (Italy), Indra (Spain), IBM (UK), EAB (Greece), G4S (UK), Fraunhofer VVS (Germany), Swedish Defence Research Agency (FOI, Sweden), Engineering Ingegneria Informatica SpA (Belgium), EDISOFT (Portugal), EADS

[335] http://www.eos-eu.com/default.aspx?page=home
[336] www.eos-eu.com/?Page=whatiseos

(Belgium), the Belgian branch of DCNS (France), D'Appolonia S.p.A (Italy), BUMAR (Poland), TELETRON (Italy), CORTe (Belgium), IABG (Germany), CEA (France), Conceptivity (Switzerland), Trento Rise (Italy), BAE Systems Detica (UK), United Technologies Research Centre Ireland (UTRCI), IABG (Germany).[337] Many of these companies are surveillance companies.

European Security Research & Innovation Forum

ESRIF was established in 2007 as a joint initiative of the European Commission and the 27 EU Member States to develop a European Security Research and Innovation Agenda (ESRIA).[338] It published its Final Report in 2009; the report presented a mid and long term Joint Security Research and Innovation Agenda linking security research with security policy-making and its implementation. It created a set of context scenarios with a 2030 time horizon to frame how current trends may combine to create alternative futures. ESRIF's plenary of 65 members from 32 countries included independent representatives from industry, public and private end-users, research establishments and universities, as well as non-governmental organisations and EU bodies.

Surveillance industry players involved in ESRIF as members included the European Corporate Security Association (ECSA), Finmeccanica (whose representative Giancarlo Grasso was ESRIF's deputy chairman), Thales Security Solutions & Services Division, Sagem Défense et Sécurité, Saab AB, Smiths Group plc and the Security & Resilience Industry & Suppliers Council (RISC).[339]

The ESRIF report recognises **s**urveillance as "increasingly a central element of security management"[340] and calls for a European approach in the surveillance domain, comprising "improvement of procedures for the design and procurement of new surveillance-systems, facilitation of European suppliers of installations and systems with testing environments for proving and improving the quality of their products, for the reduction of market failure by an improved interaction between suppliers and clients".[341]

European Security Research Advisory Board

The European Security Research Advisory Board (ESRAB) aimed to "draw the strategic lines for European security research and to advise on the principles and mechanism for its implementation within the Commission's seventh framework programme for research and technology development (FP7)".[342] It was formed in April 2005 and brought together "demand articulators and research and technology suppliers in a 50-person-strong board of high-level specialists and strategists with expertise in the field of security research including: public authorities, industry, research institutes and specialist think tanks".[343] The following

[337] http://www.eos-eu.com/?Page=partners
[338] http://www.esrif.eu/
[339] ESRIF, Final Report, December 2009.
http://ec.europa.eu/enterprise/policies/security/.../esrif_final_report_en.pdf
[340] Ibid, p.21.
[341] ESRIF, Final Report, December 2009, p.63.
http://ec.europa.eu/enterprise/policies/security/.../esrif_final_report_en.pdf
[342] ESRAB, *Meeting the Challenge: the European Security Research Agenda*, A report from the European Security Research Advisory Board, Office for Official Publications of the European Communities, Luxembourg, September 2006. http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf
[343] Ibid.

security and surveillance companies influenced its work as members: Telefonica, Novartis International, TNO, Finmeccanica, Alcatel ETCA, EADS, Diehl VA Systeme, Thales, Cybernetica, BAE Systems, Siemens CT, Fincantieri, Sagem Défense Sécurité.[344]

ESRAB made surveillance (in different forms) a priority on the European research and policy agenda. Here are some of the ESRAB report's surveillance-related findings and recommendations:

- Detection and identification capabilities represent a key area for EU investment over the coming years.
- Biometric based systems will support the fight against terrorism, be instrumental in the aftermath of a crisis and will improve access control at both border checkpoints and critical infrastructures.
- A key area for investment includes improved surveillance capabilities with respect to coverage and quality and the fusion of real-time sensor data (space, air, land, sea) in order to establish a common operational picture.
- ESRAB recommends formation of five demonstration programmes, among which would be an European-wide integrated border control system — integrated border management, system encompassing surveillance, monitoring, identity management and advanced training methods/tools.[345]

3.6.2 Intersections with national security agencies

Surveillance companies are increasingly intersecting with the public sector in the performance of traditionally public sector-restricted activities. G4S predicts that private companies, such as itself, will be taking on policing tasks as part of privatisation deals with the government departments in the UK.[346]

Surveillance companies also have old and close links with the governments and their agencies. For instance, Indra Sistemas is closely linked the Spanish government. Reports indicate that the French and German governments "each control 22.35% of EADS through direct and indirect shareholdings".[347] Raytheon provides "full-spectrum training and training support to government and military customers worldwide" including the US Army, NASA and the US Federal Aviation Administration.[348]

3.6.3 Lobbying

Lobbying is a major means of influencing security policy, as demonstrated before in the context of how industry associations lobby regional and national institutions to achieve desired changes in policy and legislation.

---

[344] A full list of members is at: http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf

[345] ESRAB, Meeting the Challenge: the European Security Research Agenda, A report from the European Security Research Advisory Board, Office for Official Publications of the European Communities, Luxembourg, September 2006, p. 7.
http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf

[346] Taylor, Mathew, and Alan Travis, "G4S chief predicts mass police privatisation", *The Guardian*, 20 June 2012. http://www.guardian.co.uk/uk/2012/jun/20/g4s-chief-mass-police-privatisation

[347] Milmo, Dan, "BAE's largest investor voices concerns over EADS merger", *The Guardian*, 8 Oct 2012.
http://www.guardian.co.uk/business/2012/oct/08/invesco-concerns-bae-eads-merger?newsfeed=true

[348] Raytheon, Global Training Solutions: Government and Military.
http://www.raytheon.com/businesses/rts/overview/gts/government/index.html

Organisations such as the European Organisation for Security (EOS) take lobbying and advocacy very seriously. As part of the EOS advocacy activities, it has "developed common positions and strategic recommendations to the EC on main security domains" in the form of white papers.[349] Its 2012 White Papers aim to

- Support the advocacy for the creation of four main EU security programmes with adequate funding;
- Ease the participation at EU Task Forces and advisory groups and support the development and implementation of policy, regulations, technology standards and guidelines;
- Provide suggestions for the definition of an EU industrial security policy (standardisation, validation and certification, pre-commercial procurement, privacy, third party liability limitation)
- Lobby for 2014-2020 budgets in the security area
- Advise on research and innovation in the context of the Commission's new Horizon 2020 research programme).[350]

According to the EOS, the following of its "messages" have already been adopted (or under discussion) by the EU and Member State institutions and other EU bodies: [351]

- Creation of a an EU Internal Security Strategy with concrete actions
- Creation of an EU Industrial Security Policy
- Creation of an EU cyber security policy (under discussion)
- Creation of an EU Transport Security Policy (under discussion)
- Creation of EU rapid reaction capabilities for civil protection and disaster management
- Creation of a common and comprehensive approach for maritime surveillance (now part of EUROSUR)
- Adoption of a "Privacy and Security by Design" approach
- Stronger link between EU security policies and EU R&D activities
- Definition of consistent (across the EU) operational needs from users (under discussion)
- Introduction of cyber security and civil protection preparedness as R&D themes in the European Security Research Programme (ESRP)
- Awareness of possible European dependency on non-EU innovations (e.g., cyber)
- Standardisation, interoperability and public-private dialogue to reduce market fragmentation
- High level public-private dialogue regarding a "Security Summit" (under organisation)
- Focused efforts on main priority topics: EU programmes and platforms (under discussion)
- Focused EU resources and budgets into a co-ordinated EU Internal Security Fund (under discussion).

According to the Transparency Register, the EOS spent around €350,000 to €400,000 representing its interests to EU institutions in 2011 with procurement listed at €60,000.[352] Similarly, the Confederation of European Security Services (CoESS) spent €50,000 to €100,000 in 2011[353] while the Aerospace and Defence Industries Association of Europe

[349] EOS, "Advocacy Successes: Common Positions for the Future Market". http://www.eos-eu.com/?Page=advocacy
[350] Ibid.
[351] EOS, "Advocacy Successes: Common Positions for the Future Market". http://www.eos-eu.com/?Page=advocacy
[352] European Commission, "EOS", Transparency Register. http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=32134385519-64
[353] European Commission, "Confederation of European Security Services", Transparency Register. http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=61991787780-18

(ASD) spent between €1,500,000 and €1,750,000 in 2011, representing their interests to EU institutions.[354]

3.6.4 Involvement in EU security research projects

Statewatch, the UK-based civil society advocacy organisation, highlights that

> the design of the ESRP was largely outsourced to the major players in the nascent European Homeland Security industry, instituting an apparent conflict of interests within which large multinationals have been able to shape the security research agenda, apply for the subsequent R&D funds on offer, and then sell the resulting technologies and systems back to the governments that funded their development.[355]

In this section, we examine the involvement of surveillance companies – such as Atos SA, Finmeccanica, EADS NV, Israel Aerospace Industries (IAI, and its subsidiary Elta),[356] QinetiQ Group plc and Safran Morpho – in various European research projects. Many of these are extensively involved in European security, ICT and other relevant sectoral research programmes. The following table illustrates this involvement for the companies in our short-listed sample (the Annex 2 listed companies):[357]

Organisation	EU security, ICT research involvement
3M Cogent Inc.	• European Global Border Environment (GLOBE)
Atos SA	• +I2 FI-WARE: Future Internet Core Platform • Common assessment and analysis of risk in global supply chains (CASSANDRA) • Pro-active decision support for data-intensive environments (ASTUTE) • Search engine for MultimediA enviRonment generated content (SMART) • Tagging Tool based on a Semantic Discovery Framework (TATOO) • Socio-Economics meets Security (SECOECONOMICS) • Early recognition, monitoring and integrated management of emerging, new technology related risks (INTEG-RISK) • Mastering the Value Function of Security Measures (VALUESEC) • Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSOS)
BAE Systems Detica	• Open Architecture for UAV-based Surveillance System (OPARUS) • Total Airport Security System (TASS) • Context-aware data-centric information sharing (CONSEQUENCE) • Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces (ADABTS) • Strategic crime and immigration information management system (SCIIMS)

[354] European Commission, "Aerospace and Defence Industries Association of Europe", Transparency Register. http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=72699997886-57
[355] Statewatch, "Observatory on the European Security Research Programme (ESRP)". http://www.statewatch.org/Targeted-issues/ESRP/security-research.html
[356] Extensively involved in EU research projects with a total public funding amounting to €148.55 million. Stephen Gardner, "Military spending dressed up as research", *EU Observer*, 17 Feb 2012. http://blogs.euobserver.com/gardner/2012/02/17/military-spending-dressed-up-as-research/
[357] This is not an exhaustive list. Further project involvement can be checked via the European Commission's CORDIS project search facility at http://cordis.europa.eu/fp7/projects_en.html

Boeing	• Protection of European seas and borders through the intelligent use of surveillance (PERSEUS) • Unmanned Aerial Systems in European Airspace (ULTRA)
Bosch Security Systems GmbH	• PANORAMA Project - Ultra Wide Context Aware Imaging
Cassidian (defence and security subsidiary of the EADS group)	• Enhanced Communications in Emergencies by Creating and Exploiting Synergies in Composite Radio Systems (HELP) • Aftermath Crisis Management System-of-systems Demonstration (ACRIMAS) • Deployable SAR Integrated Chain with Unmanned Systems (DARIUS) • European software defined radio for wireless in joint security operations (EULER) • Digital and innovative technologies for security and efficiency of first responders operation (DITSEF) • Versatile InfoRmation Toolkit for end-Users oriented Open Sources explOitation (VIRTUOSO) • Preparedness and Resilience against CBRN Terrorism using Integrated Concepts and Equipment (PRACTICE) • Sea Border Surveillance (EURSUR)
Cognitec Systems GmbH	• 3D FACE
EADS NV	• AIRBorne information for Emergency situation Awareness and Monitoring (AIRBEAM) • Security of critical infrastructures related to mass transportation (DEMASST); • Digital and innovative technologies for security and efficiency of first responders operation (DITSEF) • EUropean software defined radio for wireless in joint security operations (EULER) • Open Architecture for UAV-based Surveillance System (OPARUS) • Protection of European seas and borders through the intelligent use of surveillance (PERSEUS) • Sea Border Surveillance (SeaBILLA) • Preparedness and Resilience against CBRN Terrorism using Integrated Concepts and Equipment (PRACTICE)
Ericsson	• Converging and conflicting ethical values in the internal/external security continuum in Europe (INEX)
Experian Nederland BV	• Best practice Enhancers for Security in Urban Environments (BESECURE)
Finmeccanica S.p.A.	• Coordination action on Risks, Evolution of threatS and context assessment by an Enlarged Network for r&D rOadmap (CRESCENDO) • AIRBorne information for Emergency situation Awareness and Monitoring (AIRBEAM) • Efficient integrated security checkpoints (EFFISEC) • Fast and trustworthy Identity Delivery and check with ePassports leveraging Traveler privacy (FIDELITY) • Intelligent Knowledge Platform for Personal Health Monitoring Services (EHEALTHMONITOR) • Surveillance of unattended baggage and the identification and tracking of the owner (SUBITO) • Suspicious and abnormal behaviour monitoring using a network of cameras & sensors for situation awareness enhancement (SAMURAI)

	• The Railway Industry Partnership for Integrated Security of Rail Transport (PROTECTRAIL) *(as Selex Elsag)* • Wide maritime area airborne surveillance (WIMAAS) • Wireless sensor Networks with self-organization capabilities for critical and emergency applications (WINSOC) As SESM, Soluzioni Evolute per la Sistemistica e i Modelli S.c.a.r.l. (Italy): • AiR Guidance and Surveillance 3D (ARGUS 3D) • Airport detection and Tracking Of dangerous Materials by passive and active sensors arrays (ATOM) • Embedded Monitoring (EMMON)
Gemalto	• Roadmaps for European research on Smartcard Technologies (RESET) • Security Engineering for Lifelong Evolvable Systems (SecureChange)
Google	As Google Ireland: • Synergetic content creation and communication (SYNC3) • A unified framework for multimodal content SEARCH (I-SEARCH) • Policy Gadgets Mashing Underlying Group Knowledge in Web 2.0 Media (PADGETS) • Exploiting Social Networks for Building the Future Internet of Services (SOCIOS) • Reflecting Knowledge Diversity (RENDER) • Policy Formulation and Validation through non moderated crowdsourcing (NOMAD)
Honeywell International	• Unmanned Aerial Systems in European Airspace (ULTRA)
Indra Sistemas	• Protection of European seas and borders through the intelligent use of surveillance (PERSEUS) • Creation of a secure environment for e-Administration services and applications that enables user access via with an electronic ID card (SECURE ID) • Securing the European electricity supply against malicious and accidental threats (SESAME)
Israel Aerospace Industries (IAI) (and subsidiary Elta)	• Transportable autonomous patrol for land border surveillance (TALOS) • Open Architecture for UAV-based Surveillance System (OPARUS) • Smart Intelligent Aircraft Structures (SARISTU)
QinetiQ Group	• Strategic risk assessment and contingency planning in interconnected transport networks (STAR-TRANS) • Protection of Critical Infrastructures against High Power Microwave Threats (HIPOW) • Seamless communication for crisis management (SECRICOM) • Semantically enhanced resilient and secure critical infrastructure services (SERSCIS) • Development of Pre-operational Services for Highly Innovative Maritime Surveillance Capabilities (DOLPHIN)
Saab AB	• EUropean software defined radio for wireless in joint security operations (EULER) • Integrated mobile security kit (IMSK) • Localization of threat substances in urban society (LOTUS) • Protection of European seas and borders through the intelligent use of surveillance (PERSEUS)

Safran Morpho	• Architecture for the Recognition of thrEats to mobile assets using Networks of multiple Affordable sensors (ARENA) • Biometrics Evaluation and Testing (BEAT) • Comprehensive European Approach to the Protection of Civil Aviation (COPRA) • Coordination action on Risks, Evolution of threatS and context assessment by an Enlarged Network for r&D rOadmap (CRESCENDO) • Efficient integrated security checkpoints (EFFISEC) • European security trends and threats in society (ETTIS) • Evaluation of critical and emerging technologies for the elaboration of a security research agenda (ETCETERA) • Explosive Material Production (Hidden) Agile Search and Intelligence System (EMPHASIS) • Fast and trustworthy Identity Delivery and check with ePassports leveraging Traveler privacy (FIDELITY) • Homeland security, biometric identification and personal detection ethics (HIDE) • Hyperspectral imaging IED and explosives reconnaissance system (HYPERION) • Scalable Measures for Automated Recognition Technologies (SMART) • Tactical Approach to Counter Terrorists in Cities (TACTICS)
Securitas AB	• Security UPgrade for PORTs (SUPPORT) • Mobile Authentication using Retina Scanning (MARS)
Siemens AG	• European network for the security of control and real-time systems (ESCORTS) • A Framework for electrical power sysTems vulnerability identification, dEfense and Restoration (AFTER) • CRitical Infrastructure Security AnaLysIS (CRISALIS)
Thales	• Security of critical infrastructures related to mass transportation (DEMASST) • Efficient integrated security checkpoints (EFFISEC) • EUropean software defined radio for wireless in joint security operations (EULER) • Sea Border Surveillance (SeaBILLA) • Video/Audio Networked surveillance system enhAncement through Human-cEntered adaptIve Monitoring (VANAHEIM)

In addition, other surveillance players (outside our short-listed sample) also co-ordinate and participate in European security research projects. Ascending Technologies GmbH participated in the project Swarm of micro flying robots (SFLY). The Total Airport Security System (TASS) consortium included Verint Systems Ltd, Elbit, IBM Research GmbH, QMC Instruments (UK), EADS GmbH, Technion - Israel Institute of Technology, IBM Israel - Science And Technology Ltd. The Surveillance of Unattended Baggage and the Identification and Tracking of the Owner (SUBITO) consortium included industry players such as Selex Sensors and Airborne Systems Ltd, Fiera Di Genova SpA, Österreichisches Forschungs-Und Prüfzentrum Arsenal Ges. M.B.H. (Austria), L-1 Identity Solutions AG (Germany), Elsag Datamat S.P.A. (Italy), Valtion Teknillinen Tutkimuskeskus (Finland).

Thus, we see many surveillance companies capitalising on what Ben Hayes of Statewatch calls the "cash cows" which "no-one from the human rights or civil liberties community in Europe is questioning, never mind challenging".[358]

3.7 THE SURVEILLANCE INDUSTRY AND FUNDAMENTAL RIGHTS

This section tries to answer the following questions: What is the attitude and position of the surveillance industry with regard to fundamental rights? How do surveillance companies show respect for human rights? Are there any good practices that support rather than take away human rights? It is vital to answer these questions because though some might argue that surveillance helps people fee safe and secure, surveillance technologies by their very nature seem antithetical to human rights and have a profound effect upon them.

Various writers have highlighted and cautioned about the potential of surveillance technologies to affect human rights. Ritzer says that the intrusiveness of surveillance technologies is a threat to human rights.[359] Lagoutte, Sano and Scharff Smith suggest that trends of increasing surveillance "serve to undermine the legitimacy of human rights".[360] The UK CCTV Commissioner has warned of the threats to human rights from the increasing sophistication and use of CCTV technology.[361]

3.7.1 Attitudes to human rights

In this section, we examine some companies' perspectives on human rights and try to determine their attitude of the surveillance industry to fundamental rights (human dignity, freedoms, democracy, equality, the rule of law). Here are some excerpts (drawn from company websites and annual reports):

> BAE Systems:
> The Group expects its suppliers to comply with local legislation, and to have and meet equivalent standards on issues such as ethical conduct, health and safety, product safety, the environment, civil liberties and human rights.[362]

While this statement is a good start, it is rather vague in terms of what civil liberties and human rights must be complied with. It also seems to deflect responsibility.

> trovicor:
> Since trovicor was founded in 1993, we have been guided by our core values in a socially responsible manner. This includes corporate governance, a focus on employee success, caring for the environment and participation in the global community.[363]

---

[358] Hayes, Ben, "CLEAN IT: the secret EU surveillance plan that wasn't", *OpenDemocracy*, 9 Oct 2012. http://www.opendemocracy.net/ben-hayes/clean-it-secret-eu-surveillance-plan-that-wasn%E2%80%99t

[359] Ritzer, George, *Globalisation: The Essentials*, Wiley Blackwells, Chichester, 2011, p. 241.

[360] Lagoutte, S., H-O Sano and P. Scharff Smith, "Human Rights in Turmoil: Facing Threats, Consolidating Achievements" in S. Lagoutte, H-O Sano and P. Scharff Smith (eds.), *Human Rights in Turmoil*, Koninklijke, Netherlands, pp. 1-6 [p. 3].

[361] Info4Security, "HD CCTV technology risks breaching human rights", 4 Oct 2012. http://www.info4security.com/story.asp?storycode=4129624

[362] BAE Systems, Annual Report 2011. http://www.baesystems.com/cs/groups/public/documents/document/mdaw/mdu2/~edisp/baes_045566.pdf

[363] trovicor, Corporate Social Responsibility. http://trovicor.com/en/company-en/social-responsibility-en.html

This statement is even more vague than the previous one. It does not even mention human rights. Note that trovicor deals in lawful interception solutions and has been implicated in human rights controversies in the Middle East.[364]

> Google:
> Privacy concerns relating to our technology could damage our reputation and deter current and potential users from using our products and services. From time to time, concerns have been expressed about whether our products and services compromise the privacy of users and others. Concerns about our practices with regard to the collection, use, disclosure, or security of personal information or other privacy related matters, even if unfounded, could damage our reputation and operating results. While we strive to comply with all applicable data protection laws and regulations, as well as our own posted privacy policies, any failure or perceived failure to comply may result, and has resulted, in proceedings or actions against us by government entities or others, or could cause us to lose users and customers, which could potentially have an adverse effect on our business. [365]

Google seems to recognise the damaging effects of non-compliance with privacy concerns.

However, these statements seem like mere lip-service or overt vague assurances that give the impression that a company will act in conformity with legal and social obligations and values. However, others are sceptical. Privacy International has said, with regard to the corporate social responsibility of surveillance companies:

> Of the 246 companies known to partake in the communications surveillance industry, only 62 had publicly available CSR policies. Of these, only four companies had policies that placed specific constraints on doing business with regimes that might use their technology to commit human rights abuses. Typically, social and ethical commitments to groups other than employees, business partners or shareholders amounted to vaguely-worded assurances to 'practice good corporate citizenship' or to 'act with integrity'… The vagueness and flexibility of 'CSR' has enabled surveillance technology firms to claim they act responsibly while supplying their products to foreign governments with appalling human rights records.[366]

Thus, we see how companies project and attempt to incorporate their attitudes to human rights in their policies, and yet if we weigh up the overall industry based on Privacy International's findings of a lack of corporate social responsibility policies, the picture seems grim (this is not to say that all companies lacking corporate social responsibility policies are all human rights violators; such a generalisation is detrimental to collaborating with the industry in furthering human rights).

3.7.2 Concerns

Governments, civil society and the media have expressed various concerns in relation to companies and fundamental rights.[367] We illustrate these below:

---

[364] Zetter, Kim, "Nokia-Siemens Spy Tools Aid Police Torture in Bahrain", *Wired.com*, 23 Aug 2011. http://www.wired.com/threatlevel/2011/08/nokia-siemens-spy-systems/

[365] Google Inc., Annual Report 2011. http://sec.gov/Archives/edgar/data/1288776/000119312512025336/d260164d10k.htm

[366] King, Eric, "Surveillance companies: real responsibility goes beyond the letter of the law", *Privacy International*, 6 Aug 2012. https://www.privacyinternational.org/blog/surveillance-companies-real-responsibility-goes-beyond-the-letter-of-the-law

[367] Distilled from section 3.3.6 (controversies).

Company	Affected right	Concern
Acxiom	Privacy, data protection	Disclosure of personal information
Detica	Privacy, freedom of expression	Telecoms surveillance
Ericsson	Privacy, freedom of expression	Telecoms surveillance
Experian	Privacy, data protection	Data breaches
Honeywell	Privacy, freedom of expression, association, movement	Surveillance systems to monitor dissidents (China)
Microdrones	Privacy, freedom of movement	Citizen surveillance in China
Narus (Boeing)	Privacy, freedom of expression	Internet & mobile surveillance
Selex Elsag (Finmeccanica)	Privacy, freedom of expression	Telecoms surveillance
Trovicor	Privacy, freedom of expression	Communications interception (monitoring of activists)
ZTE	Privacy, freedom of expression	Telecoms surveillance

3.7.3 Respecting human rights – measures and good practices

Here we outline some measures companies are taking to meet their human rights commitments.

Many companies, such as Atos Origin,[368] have codes of ethics in place. Atos participates in the United Nations Global Compact and aims to respect UN human rights principles. Finmeccanica has a charter of values which incorporates its respect for human rights (it states, "The Finmeccanica Group upholds and promotes human rights in every context in which it operates… by creating equal opportunities for its people and fair treatment for all… always respecting the dignity of each individual and of each employee").[369] Thales, believing that "ethical conduct and corporate responsibility are key assets in its strategic plan for success", issues an annual corporate responsibility report, which is publicly available on their website.[370]

G4S treats human rights as a core CSR area and priority,[371] and has a corporate social responsibility checklist used for "assessing new market entries, major contracts and other significant investments to ensure they comply with political, ethical, social, technological, environmental and legal standards". G4S claims it used the checklist "to assess a number of projects throughout the year".[372] In addition, according to its annual report, it has "Commenced a significant human rights project to determine key human rights issues and develop detailed policies and guidelines for implementation in 2012" and "engaged with Malachite, an independent human rights consultancy to carry out a human rights risk assessment based on the countries in which we operate and the services we provide".[373]

After G4S was criticised severely in 2010 and 2011 regarding its West Bank contracts, it reviewed its operations in relation to human rights risks and challenges and developed a new human rights policy, which is under review by internal and external stakeholders. Following

[368] http://atos.net/NR/rdonlyres/5813E9D6-EA97-4CE1-8E03-10A40E6E1E97/0/Codeofethics_20111124.pdf
[369] http://www.finmeccanica.it/EN/Common/files/Corporate/Il_Gruppo/Carta_dei_Valori/carta_ENG_def.pdf
[370] Thales, Business ethics. http://www.thalesgroup.com/Group/Corporate_Responsibility/Business_Ethics/
[371] G4S plc, Annual Report and Accounts 2011. http://www.g4s.com/en/Investors/2011%20Annual%20Report/
[372] G4S, CSR Checklist. http://reports.g4s.com/csr/safeguarding-our-integrity/csr-checkllist.html
[373] G4S plc, Annual Report and Accounts 2011. http://www.g4s.com/en/Investors/2011%20Annual%20Report/

the review and agreement, G4S expects to develop operational guidelines for its implementation.[374]

Another good practice is Google's Transparency Report, which shows some support to the right to freedom of expression.[375] The report discloses:

- Real-time and historical traffic to Google services around the world;
- Numbers of removal requests we receive from copyright owners or governments;
- Numbers of user data requests we receive from government agencies and courts

This practice empowers the public and generates some transparency.

Another good practice is Microsoft's roll out of Internet Explorer 10 with default Do Not Track settings guaranteed to protect user privacy (which is facing severe criticism from large advertising associations and consumer tracking companies).[376]

While many of the large and established players seem to have a code of ethics in place, smaller, yet highly relevant players developing and selling cutting edge surveillance solutions, such as Eye-tech (Italy/automatic video surveillance)[377], Phonexia (Czech Republic/speech record data mining),[378] Neurotechnology (Lithuania/biometrics)[379] and Irisys (UK/intelligent infrared, thermal imaging solutions),[380] do not have a code of ethics or corporate social responsibility statements.

3.7.4 Conclusion

To a great extent, the surveillance industry, while not aiming explicitly to, is at odds with human rights interests. But in this, the industry by itself is not at fault. Government in particular have been chastised for its part in not protecting human rights effectively by extending safeguards in respect of this industry. Note the comments of the Special Rapporteur in the report on the promotion and protection of human rights and fundamental freedoms while countering terrorism:

> States that previously lacked constitutional or statutory safeguards have been able to radically transform their surveillance powers with few restrictions. In countries that have constitutional and legal safeguards, Governments have endangered the protection of the right to privacy by not extending these safeguards to their cooperation with third countries and private actors, or by placing surveillance systems beyond the jurisdiction of their constitutions.
>
> The Special Rapporteur notes that since September 2001 there has been a trend towards outsourcing the collection of intelligence to private contractors... [raising concerns about] lack of proper training, the introduction of a profit motive into situations which are prone to human

[374] Ibid.
[375] Google Inc, Transparency Report. http://www.google.com/transparencyreport/
[376] Keizer, Gregg, "Ad industry calls IE10's 'Do Not Track' setting 'unacceptable'", *PC Advisor*, 4 Oct 2012. http://www.pcadvisor.co.uk/news/security/3402037/ad-industry-calls-ie10s-do-not-track-setting-unacceptable/#ixzz28Va1VEkX
[377] http://www.eye-tech.it/
[378] www.phonexia.com/
[379] http://www.neurotechnology.com/
[380] www.irisys.co.uk/

rights violations, and the often questionable prospect that such contractors will be subject to judicial and parliamentary accountability mechanisms.[381]

In this light, we recommend a more streamlined, yet cautious approach on the part of governments to regulate the surveillance industry, an approach that does not put the European surveillance industry at a disadvantage compared to players based outside the EU.

3.8 WHO WATCHES THE SURVEILLANCE INDUSTRY

This section analyses the various "watchers" of the surveillance industry, i.e., those entities who provide some oversight of the industry. Among these watchers are governments, civil society organisations, the media and academia in Europe. We identify key organisations, monitoring motivations, and actions and activities undertaken. We also consider the effect of the watching actions on the industry and industry's response to these actions (if any). We conclude this section with a brief effectiveness analysis.

3.8.1 Government

The government, through its various departments and agencies, functions as a watcher of the surveillance industry. It watches over the surveillance industry through the legislative, regulatory and judicial systems. This is achieved through enacting legislation, inquiries and investigations and enforcement actions.

Key organisations and monitoring actions

Various EU level and national governmental agencies watch over the surveillance industry. The EU level bodies include the European Parliament and European Commission. The national bodies include: national parliaments, committees, government agencies, data protection authorities, surveillance commissioners, judiciaries and human rights commissions.

Parliaments

Parliament watches over the surveillance industry through enacting laws (on privacy, data protection, human rights, tax, trade, procurement, export controls) and formulating policy on what can and cannot be subject to surveillance (e.g., what is lawful and unlawful interception).[382] Parliaments may use existing committees, set up new committees or commission experts to investigate surveillance concerns.

After concerns were expressed about the sale of surveillance equipment to international regimes violating human rights, the European Parliament passed a resolution prohibiting the grant of general EU authorisations for exports of telecommunication technologies to certain countries (such as China, India, Russia and Turkey) that could be used "in connection with a violation of human rights, democratic principles or freedom of speech... by using interception

[381] Scheinin, Martin, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Human Rights Council, Thirteenth session. A/HRC/13/37 28 December 2009, paras 20 and 41. http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf

[382] E.g., the Regulation of Investigatory Powers Act 2000 (RIPA) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 in the UK.

technologies and digital data transfer devices for monitoring mobile phones and text messages and targeted surveillance of internet use".[383]

In the UK, various parliamentary bodies have examined concerns surrounding surveillance industry practices. The UK House of Commons Justice Committee looked into the protection of private data.[384] The House of Commons Home Affairs Committee presented a comprehensive report on surveillance in the UK.[385] The House of Lords Select Committee on the Constitution examined the topic of "Surveillance: Citizens and the State".[386]

After complaints about Gamma International's FinSpy surveillance software (a "dual use" technology, capable of being used for both civilian and military purposes) being exported to countries such as Turkmenistan, Dubai, Ethiopia, Indonesia, Mongolia and Qatar, the software was assessed, reclassified and made subject to export controls by the UK government "because it is designed to use controlled cryptography".[387]

Government departments and agencies

Government departments and agencies formulate policies and adopt strategies on surveillance technologies that affect surveillance business. They also organise and collaborate in events that promote dialogue between different stakeholders on vital concerns about surveillance technologies (e.g., the Foreign Office in Berlin organised a conference on the Internet and human rights in September 2012 in co-operation with Human Rights Watch, the University of Aarhus, and the Alexander von Humboldt Institute for Internet and Society of the Humboldt University of Berlin).[388]

In UK, the Parliamentary Office of Science and Technology (POST) writes briefings, organises events and assists Select Committees make an "independent, balanced and accessible analysis of public policy issues related to science and technology".[389]

Office of the Surveillance Commissioners (UK)

The UK has an Office of Surveillance Commissioners (OSC) the objective of which is to "provide effective and efficient oversight of the conduct of covert surveillance and covert human intelligence sources by public authorities in accordance with Part III of the Police Act 1997, Parts II and III of Regulation of Investigatory Powers Act (RIPA) and RIP(S) A".[390] The OSC tribunal has 26 people. The Prime Minister appoints the Chief Surveillance Commissioner (CSC), Commissioners and Assistant Commissioners (all of these either hold or have held high judicial office). Their duty is to "scrutinise all notifications, renewals and

[383] See European Parliament, "Controlling dual-use exports", Press release, 4 April 2011. http://www.europarl.europa.eu/pdfs/news/expert/infopress/20110927IPR27586/20110927IPR27586_en.pdf
[384] House of Commons Justice Committee's report on *Protection of Private Data*.
[385] House of Commons Home Affairs Committee, *A Surveillance Society?*, Fifth Report of Session 2007–08, HC 58-1, The Stationery Office Limited, London, 8 June 2008. http://www.publications.parliament.uk/pa/cm200708/cmselect/cmhaff/58/58i.pdf
[386] House of Lords, Select Committee on the Constitution, *Surveillance: Citizens and the State*, 2nd Report of Session 2008-09, HL Paper 18-I, paras. 153-77.
[387] Ross, Alice K, "Government ramps up controls on FinSpy surveillance software", *The Bureau of Investigative Journalism*, 11 Sept 2012. http://www.thebureauinvestigates.com/2012/09/11/government-ramps-up-controls-on-finspy-surveillance-software/
[388] http://internethumanrights.org
[389] http://www.parliament.uk/post
[390] www.surveillancecommissioners.independent.gov.uk

cancellations of authorisations of property interference and intrusive surveillance". The CSC reports annually to the Prime Minister and the Scottish First Minister and the reports are presented to Parliament and the Scottish Parliament.

Though the Office of the Surveillance Commissioner has "no remit to oversee the activity of private enterprises whose activity would otherwise meet statutory tests", it recognises that non-public enterprises (such as private investigators, bailiffs and housing stock management) use covert surveillance techniques.[391] The Chief Surveillance Commissioner has clarified that "where these entities conduct covert surveillance on behalf of a designated public authority", he reserves the option to examine their activities.[392] The CSC understands that he does not have the "capability to oversee an increasing number of entities" and recommends that "Public authorities should be very careful in their cooperation with private enterprises and should have in place arrangements which clarify responsibility and liability in the event of challenge." [393]

Surveillance camera commissioner (UK)

The Protection of Freedoms Act 2012 provides for the regulation of CCTV and other surveillance camera technology in Part 2, Chapter 1. Section 29 mandates the development of a Code of Practice to provide guidance on the development or use of surveillance camera systems and use or processing of images or other information obtained through the use of such systems. The UK government has appointed a surveillance camera commissioner (according to Section 34(1) of the Protection of Freedoms Act 2012). The commissioner's remit includes (a) encouraging compliance with the code, (b) reviewing the operation of the code and (c) providing advice about the code (including changes to it and breaches of it).[394] The Commissioner is expected to

> encourage operators to follow the code and will lay an annual report before parliament in which he can draw attention to any failings and make recommendations to improve how CCTV is used. He will help develop the code to ensure its continued impact and effectiveness and provide advice to users and the public.[395]

The surveillance commissioner's calls for greater regulation of surveillance (in relation to high definition CCTV and video analytics),[396] reported in the national media, drew a reaction from the British Security Industry Association (BSIA) who went on refute the commissioner's

[391] Office of Surveillance Commissioners, Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2011-2012. Presented to Parliament pursuant to section 107(3) of the Police Act 1997, House of Commons, 13 July 2012.
http://surveillancecommissioners.independent.gov.uk/docs1/OSC-annual-report-2011-12.pdf
[392] Ibid.
[393] Office of Surveillance Commissioners, Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2011-2012. Presented to Parliament pursuant to section 107(3) of the Police Act 1997, House of Commons, 13 July 2012.
http://surveillancecommissioners.independent.gov.uk/docs1/OSC-annual-report-2011-12.pdf
[394] Protection of Freedoms Act 2012, S 34(2).
[395] Home Office, "Surveillance camera commissioner appointed", Press release, 13 Sept 2012.
http://www.homeoffice.gov.uk/media-centre/press-releases/surv-cam-comm-appt
[396] The commissioner reportedly stated: "I'm convinced that if we don't regulate it properly – i.e., the technological ability to use millions of images we capture – there will be a huge public backlash. It is the Big Brother scenario playing out large. It's the ability to pick out your face in a crowd from a camera which is probably half a mile away." See Hastings, Rob, "New HD CCTV puts human rights at risk", *The Independent*, 3 Oct. 2012. http://www.independent.co.uk/news/uk/crime/new-hd-cctv-puts-human-rights-at-risk-8194844.html

claims and extol the advantages of CCTV as "vital to the protection of our society" and that the UK security industry was "dedicated to ensuring it is used responsibly".[397]

Data protection authorities

Data protection authorities are currently the most visible watcher of the surveillance industry. They monitor developments in the surveillance industry, including new technologies and their implementation. They liaise with the industry in developing guidelines and good practices (e.g., the UK Information Commissioner's Office (ICO) produced a CCTV Guidance for organisations aimed at promoting the proper and lawful use of CCTV).[398] They report to parliament on surveillance concerns.[399] They accept complaints from aggrieved parties and impose sanctions on companies violating privacy and data protection law. They conduct audits on surveillance practices and apply pressure on companies to comply with privacy and data protection law and conform to best practices. They also educate the public on surveillance concerns and their fundamental rights and freedoms.

There are several examples of how data protection authorities in Europe have prompted companies to comply with privacy and data protection law. For instance, Facebook has reportedly given up its automated face recognition feature in the European Union,[400] as a result of an audit conducted by the Irish Data Protection Authority (Office of the Data Protection Commissioner of Ireland, DPCI) in December 2011, assessing Facebook Ireland's compliance with European and Irish data protection law.[401]

Human rights commissions

Monitoring the surveillance industry comes within the scope of the objectives and activities of human rights commissions in the European Member States.[402] Human rights Commissions monitor human rights related developments, provide policy guidelines, resolve human rights disputes, educate public about human rights issues.

The Polish Human Rights Defender (independent constitutional authority safeguarding human rights) investigates whether actions undertaken or abandoned by the entities, organisations or institutions obliged to observe and implement human and citizen rights and freedoms have not led to infringement of the law or the principles of social coexistence and justice, and undertakes appropriate measures.[403]

---

[397] Reeve, Tom, "BSIA rejects surveillance camera commissioner's claims about CCTV", *Security News Desk*, 3 Oct 2012. http://www.securitynewsdesk.com/2012/10/03/bsia-rejects-surveillance-camera-commissioners-claims-about-cctv/

[398] Information Commissioner's Office, "CCTV". http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/cctv.aspx

[399] See Information Commissioner's Office, Information Commissioner's report to Parliament on the state of surveillance, November 2010.

[400] *Daily Mail*, "Facebook to switch off controversial facial recognition feature following data protection concerns", 22 Sept 2012. http://www.dailymail.co.uk/news/article-2207098/Facebook-switch-controversial-facial-recognition-feature-following-data-protection-concerns.html

[401] Office of the Data Protection Commissioner [Ireland], "Report of Review of Facebook Ireland's Implementation of Audit Recommendations Published – Facebook turns off Tag Suggest in the EU", 21 Sept 2012. http://dataprotection.ie/viewdoc.asp?DocID=1233&m=f

[402] A comprehensive list is available at the website of the Council of Europe Commissioner for Human Rights. http://www.coe.int/t/commissioner/links/omb_nhri_en.asp

[403] http://www.rpo.gov.pl/index.php?md=9118&s=3

Judiciary

The government also watches over the surveillance industry through the judiciary. One example of this is the judicial investigation into Finmeccanica's SELEX Sistemi Integrati SpA. The Public Prosecutor's Office attached to the Court of Rome investigated Finmeccanica's SELEX Sistemi Integrati SpA in connection with allegations of corruption and tax-related crimes relating to contracts awarded the company by ENAV SpA between 2008 and 2010.[404]

Monitoring motivations

Motivations of the various classes of government watchers vary. Some wish

- To protect the fundamental rights and freedoms of people
- To regulate the industry in response to changing societal attitudes on the development and roll-out of surveillance technologies
- To manage effects of the implementation of surveillance solutions

Effect upon industry and industry's response

Government watching actions have a diverse range of effects upon the surveillance industry. Companies themselves recognise this.

Enhancing transparency

Governments and regulators are increasingly expecting companies to implement "greater transparency".[405] In recognition of this, companies often implement measures to achieve this effect. For instance, Experian's Corporate Social Responsibility Report provides data on the scale on Experian's operations and impact upon consumers (i.e., how much data it holds),[406] impacts of its products and services,[407] and data management and compliance.[408]

Effects on operations and financial condition

Government legislation, regulations and policies affect business.[409] Changes in these could result in restraints upon business, acquisition of assets, tax and tariff burdens. Government inquiries and investigations can have a profound impact upon business. For instance, they could result in liabilities such as fines, financial penalties (cancellation of contracts, withholding of payments), suspension from contracts, loss of reputation, expropriation of

[404] Finmeccanica, 2011 Consolidated Annual Report. www.finmecannica.com
[405] Experian notes in its Annual Report: "There is a growing demand from governments, regulators and lenders for greater transparency." Experian plc, Annual Report 2012. http://www.experianplc.com/~/media/Files/E/Experian-V2/pdf/investor/reports/2012/experian-ar-2012.pdf
[406] Experian, Corporate Social Responsibility Report, 2012. http://crreport.experianplc.com/2012/our_global_performance/how_we_treat_consumers.aspx
[407] Experian, Corporate Social Responsibility Report, 2012. http://crreport.experianplc.com/2012/our_global_performance/impacts_of_products_services.aspx
[408] Experian, Corporate Social Responsibility Report, 2012. http://crreport.experianplc.com/2012/our_global_performance/managing_data_and_compliance.aspx
[409] Most companies, especially those with large government contracts, such as Honeywell International, Boeing and Northrop Grumman, recognise this effect in their Annual Reports.

assets and debarment from future business opportunities.[410] This can have an adverse impact on sales, profit margins and the future of the company.

Increase in performance and compliance costs

Greater government regulations and requirements mean an increase in performance and compliance costs for companies – thereby reducing their profit margins (e.g., Boeing recognises this explicitly in its Annual Report).[411]

Changes in demand and acceptance of products

This effect is explicitly recognised in Guidance Software's Annual Report:

> Laws and regulations are subject to drastic changes and these could either help or hurt the demand for our products. Thus, certain changes in the law and regulatory landscape, such as tort law or legislative reforms that limit the scope and size of electronic discovery requests or the admissibility of evidence generated by such requests, as well as court decisions, could significantly harm our business. Changes in domestic and international privacy laws could also affect the demand and acceptance of our products, and such changes could have a material impact on our revenues.[412]

Development of compliance strategies and best practices to meet government, regulatory requirements

Increasingly companies are actively pursuing compliance strategies and best practices to meet governmental and regulatory requirements. G4S, for instance, has a business ethics steering group "to develop a strategy to ensure compliance with the requirements of the UK Bribery Act and similar legislation" and helped develop the International Code of Conduct for Private Security Providers.[413]

Pressure upon industry to self-regulate

Companies feel pressure from governments to self-regulate. Experian acknowledges this in its annual report.[414]

Effectiveness analysis

This category of surveillance industry watchers has a greater potential (as compared to other watchers such as CSOs) to monitor the surveillance industry through a combination of regulatory, policy and judicial means. However, the government is currently is not a very effective watcher and organisations such as Privacy International believe that governments are

[410] Boeing, 2011 Annual Report. http://www.envisionreports.com/BA/2012/14427FE12E/5aeaf07f40c94540856bcbf8d53d7e39/Boeing_AR_3-9-12_SECURED_2-reduced.pdf
[411] Boeing, 2011 Annual Report. http://www.envisionreports.com/BA/2012/14427FE12E/5aeaf07f40c94540856bcbf8d53d7e39/Boeing_AR_3-9-12_SECURED_2-reduced.pdf
[412] Guidance Software Inc, Form 10-K Annual Report 2011. http://investors.guidancesoftware.com/secfiling.cfm?filingID=1104659-11-11808
[413] G4S plc, Annual Report and Accounts 2011. http://www.g4s.com/en/Investors/2011%20Annual%20Report/
[414] Experian plc, Annual Report 2012. http://www.experianplc.com/~/media/Files/E/Experian-V2/pdf/investor/reports/2012/experian-ar-2012.pdf

reluctant to regulate the surveillance industry.[415] Others such as the Centre for Irish & European Security (CIES) and Statewatch question whether governments are "out of their depth with new communications and surveillance technology" and no longer able to govern it.[416]

One reason might be because the government (and its various agencies), as shown in our analysis, is a **major customer of the surveillance industry**. The government also **collaborates** with surveillance companies in research and development in new technologies and in showcasing surveillance solutions. These public-private collaborations and partnerships are blurring the one strict role divisions between the two.

Data protection authorities are often unable to exercise effective control over the industry and find themselves at a disadvantage. The following excerpt outlines this concern:

> The Federal Data Protection Commissioner in Germany has complained that he cannot test how a spy computer programme used by German police works, because the firm that made it will not help him examine it, and the police do not have the source code. Peter Schaar had been asked by a Parliamentary Domestic Affairs Committee to look into the controversial spyware, but advised the Committee's Chairman, Wolfgang Bosbach, that he was being prevented from doing so. The programme allows security forces to monitor people's computers and, it is alleged, to engage in unconstitutional activities such as controlling the camera and microphone of someone's computer.[417]

3.8.2 Civil society organisations

This section examines key civil society organisations (CSOs) that watch over the European surveillance industry. CSOs perform a useful role as watchers of the surveillance industry. Hutter and O'Mahoney comment, "CSOs have the potential for significant influence over business and government regulatory agendas."[418] CSOs have been called "informal pressure groups" and "guardians of civil liberty".[419] There are a large number of civil society organisations in Europe that keep watch on the surveillance industry. This section introduces some of the key organisations, elaborates actions in relation to surveillance industry, identifies results and evaluates their effectiveness.

Key organisations

The table below lists the key CSOs watching the surveillance industry in Europe:

Organisation (country)	Nature of organisation	Surveillancefocus	Aims, vision	Website
Arbeitskreis Vorratsdatenspeiche	Association of civil rights	Data retention	To campaign against the introduction of data	http://www.vorratsdatenspeicherung.de/index.php?

[415] Privacy International. https://www.privacyinternational.org/blog/the-british-government-knows-more-about-surveillance-exports-than-it-is-letting-on

[416] Statewatch, "Are governments out of their depth with new communications and surveillance technology", Press release, 20 Sept 2012. http://www.statewatch.org/news/2012/sep/dublin-ep-surveillance-meeting.pdf

[417] *The Local*, "Data protector 'cannot check police spyware'", 12 Sept 2012. http://www.thelocal.de/sci-tech/20120912-44919.html

[418] Hutter, Bridget M., and Joan O'Mahoney, "The Role of Civil Society Organisations in Regulating Business", Discussion Paper No.ESRC Centre for Analysis of Risk and Regulation, 26 Sept 2004.

[419] UK House of Lords, Select Committee on the Constitution, 2nd Report of Session 2008–09, *Surveillance: Citizens and the State*, The Stationery Office, London, 2009, p. 192.

rung (Working Group on Data Retention, Germany)	campaigners, data protection activists and Internet users		retention in Germany.	lang=en
Arge Daten (Austria)	Non-profit organisation	Surveillance, security, privacy issues	The human and socially responsible use of information technology and telecommunications.	http://www.ad.or.at/
Association Electronique Libre (AEL, Belgium)	Non-profit organisation	Encryption, open software	To protect and defend fundamental rights in the information society.	http://www.ael.be/
Association for Technology and Internet (ApTI, Romania)	Non-governmental organisation	Online surveillance	To support and promote a free and open Internet where human rights are respected and protected.	http://www.apti.ro/
Associazione per la Libertà nella Comunicazione Elettronica Interattiva (ALCEI)/ Electronic Frontiers Italy	Non-profit, non-partisan organisation	Computer-based communication systems, data retention, privacy	To safeguard the freedom of expression and personal privacy of any person using electronic communication systems for personal, social, cultural, professional activities.	http://www.alcei.org/
Big Brother Watch (UK)	Campaign group	Variety of surveillance issues – CCTV, biometrics, databases, Internet surveillance	To give individuals more control over their personal data, and hold to account those who fail to respect privacy, whether private companies, government departments or local authorities.	http://www.bigbrotherwatch.org.uk/
Bits of Freedom (Netherlands)	Non-profit organisation	Big Brother Awards, ubiquitous surveillance	To defend civil rights in the information society.	https://www.bof.nl/home/english-bits-of-freedom/
Bulgarian Institute for Legal Development (Bulgaria)	Non-profit, non-governmental organisation	Data protection, human rights	To improve the legal sector in Bulgaria and promote the rule of law in Bulgaria.	http://www.bild.net/
Buro Jansen and Janssen (Netherlands)	Research organisation	Interception, security, personal identification, security control	To investigate police, justice and secret service activities dealing with all sorts of restrictive, preventive and disappearance measures against those in the margins (fringes) of society.	http://www.burojansen.nl/
Cyber-Rights & Cyber-Liberties (UK)	Non-profit civil liberties organisation	Communications interception, state	To promote free speech and privacy on the Internet and raise public	http://www.cyber-rights.org/background.htm

		surveillance	awareness of these important issues	
Deutsche Vereinigung für Datenschutz (DVD, German Association for Data Protection)	Non-profit association	Data protection, state surveillance, RFID, biometrics, etc.	To advise the public of the dangers of electronic data processing, restrictions of the right to informational self-determination and educate them.	http://www.datenschutzverein.de/vereinsprofil_dvd.html
Digital Rights (Denmark)	Non-profit civil organisation	Anti-terror legislation, data retention and exchange, camera surveillance	To raise awareness of rights in the digital world.	http://www.digitalrights.dk/
Digital Rights Ireland (DRI)	Digital rights advocacy and lobbying group	Data retention, ID cards, mass surveillance, RFID, passports	To defend civil, human and legal rights in the digital age.	www.digitalrights.ie/
Electronic Frontier Finland	Civil rights organisation	Big Brother Awards	To protect citizens' electronic rights.	http://www.effi.org/
Equipo Nizkor (Spain)	Human rights non-governmental organisation	Aerial, covert surveillance, state surveillance	To respect and promotion of human rights in different areas	http://www.derechos.org/nizkor/eng.html
European Digital Rights (EDRi, Belgium)	International non-profit association of 32 European privacy and civil rights organisations	Data retention requirements, telecommunica-tions interception	To defend civil rights in the information society	http://www.edri.org/
European Civil Liberties Network (ECLN)	Network	Security and intelligence, surveillance, biometric documents & databases	To create a European society based on freedom and equality, of fundamental civil liberties and personal and political freedoms, of free movement and freedom of information, and equal rights for minorities.	www.ecln.org/
Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIFF) Germany	Charitable association with 700 people from academia and industry	Data protection, monitoring, control	Inter alia, to fight against the use of information technology for control and surveillance.	http://fiff.de/
Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs	Privacy and digital rights non-governmental organisation	Annual Big Brother Awards, RFID, video surveillance, data retention, smart cards	To protect civil rights and privacy.	http://www.foebud.org/

(FoeBuD)Germany				
Förderverein Informationstechnik und Gesellschaft (FITUG) (Germany)	Association	Technological surveillance, surveillance laws, privacy	To promote the integration of new media in society, to educate about their techniques, risks and dangers and promote respect for human rights and consumer protection in computer networks.	www.fitug.de
Foundation for Information Policy Research (FIPR) (UK)	Independent non-profit organisation, think tank	Surveillance and security	To identify technical developments with significant social impact, commission and undertake research into public policy alternatives, and promote public understanding and dialogue between technologists and policy-makers in the UK and Europe.	http://www.fipr.org/
Humanist Union (Germany)	German civil liberties union	Security and surveillance laws, data protection law and policy	To protect human rights and civil liberties; liberate people from state authoritarianism.	http://www.humanistische-union.de/sprachen/english/
Hungarian Civil Liberties Union (HCLU, Hungary)	Non-profit human rights watchdog and NGO	Data protection, data retention, Internet surveillance	To educate citizens about their basic human rights and freedoms, and take a stand against undue interference and misuse of power by those in positions of authority.	http://tasz.hu/en
Imaginons un Réseau Internet Solidaire (IRIS, France)	Association	PNR, biometric ID, data retention, Internet surveillance	To influence the development of the Internet towards greater equality, sharing and solidarity.	http://www.iris.sgdg.org/
Internet Society (Bulgaria)	Non-governmental organisation	Privacy, data protection, assessment of surveillance in Europe	To function as the primary source of reliable information on the development of the information technologies in Bulgaria.	www.isoc.bg/index_en.html
Iuridicum Remedium (IuRe, Czech Republic)	Non-governmental non-profit organisation promoting human rights	Annual Big Brother Awards	To promote human rights.	http://www.iure.org/EN
Leave Them Kids Alone (LTKA)	Campaign group	Use of children's	To ensure that the widespread use of	www.leavethemkidsalone.com/

(UK)		biometrics	biometrics in UK schools is debated in Parliament, strictly regulated, closely monitored, and for statutory requirements for explicit informed parental consent where children's biometrics are taken.	
Liberty (UK)	Cross party, non-party membership organisation	State surveillance, surveillance society, CCTV and ANPR, ID cards, DNA database	To protect basic rights and freedoms through the courts, in Parliament and in the wider community.	www.liberty-human-rights.org.uk/
Metamorphosis (Macedonia)	Independent, non-partisan and non-profit foundation	Privacy, state surveillance	To contribute to the development of democracy and increase the quality of life through innovative use and sharing of knowledge.	www.metamorphosis.org.mk/
Netzwerk Neue Medien/Network New Media (NNM, Germany)	Networking organisation	Citizen surveillance	To preserve and promote civil liberties in the digital age.	http://www.nnm-ev.de/
NO2ID (UK)	Campaigning organisation	ID cards, database state	To publicise the case against state control of personal identity among the general public, in the media, and at every level in government.	http://www.no2id.net/
No-PNR.Org	Non-partisan and independent campaign	PNR, passenger data transfers	To inform the broader public about PNR data issues and concerns.	www.nopnr.org
Privacy International (UK)	International organisation	International trade in surveillance technologies, monitoring legal and policy developments across Europe. Projects – Global Surveillance Monitor; Big Brother Inc.	To defend the right to privacy globally, to fight unlawful surveillance and other intrusions into private life by governments and corporations.	https://www.privacyinternational.org/
Quintessenz (Austria)	Civil liberties advocacy organisation	Citizen surveillance, privacy	To restore civil rights in the information age.	http://quintessenz.at/

Statewatch (UK)	Non-profit-making voluntary group	Observatories on surveillance and related issues	To monitor the State and civil liberties in Europe.	http://www.statewatch.org/
Swiss Internet User Group (SIUG, Switzerland)	Initiative of / ch / open, an independent association	Monitoring surveillance concerns	Promotes open source software	http://www.siug.ch/
The Bureau of Investigative Journalism (UK)	Not-for-profit organisation	Government surveillance, surveillance industry, surveillance exports	To educate the public and the media on both the realities of today's world and the value of honest reporting	http://www.thebureauinvestigates.com/
The Chaos Computer Club (Germany)	Non-profit organisation	Biometrics, digital privacy, data retention	Transparency in government, freedom of information, and the human right to communication.	http://www.ccc.de/en/
The Irish Council for Civil Liberties (ICCL)	Independent human rights watchdog	State and police surveillance, data retention	To secure full enjoyment of human rights to everyone.	http://www.iccl.ie/
The Open Rights Group (UK)	Non-profit organisation	State surveillance, surveillance legislation, behavioural tracking	To promote and preserve rights in the digital age.	www.openrightsgroup.org
Verein für Internet Benutzer (VIBE!AT)/ Association for Austrian Internet Users) (Austria)	Non-profit organisation	RFID, data retention, privacy	To promote the responsible and self-determined use of the Internet	https://www.vibe.at/

Table: Major civil society organisations watching the surveillance industry in Europe

In addition to these Europe-based organisations, various CSOs based outside the European Union monitor the surveillance industry in Europe. These include: Amnesty International, the Australian Privacy Foundation, Electronic Privacy Information Center (EPIC), the Global Internet Liberty Campaign (GILC) International, Human Rights Watch, International Civil Liberties Monitoring Group (ICLMG), OpenNet Initiative (ONI), the Electronic Frontier Foundation (EFF) and the World Privacy Forum (WPF, USA).

Monitoring motivations

From the above research, the following monitoring motivations are evident:

- Promoting the rule of law
- Defending human rights and civil liberties
- Protecting privacy, freedom of expression and movement
- Fighting and deterring the abuses of surveillance practices and technologies
- Promoting the responsible use of surveillance
- Overseeing the surveillance industry

- Raising public awareness and education.

Actions taken

To realise their vision and objectives, CSOs may adopt one or a combination of the following actions.

Civil action and litigation

CSOs take civil action against surveillance practices and measures that directly or indirectly impact the surveillance industry. Digital Rights Ireland, for instance, sued the Irish government in relation to the new European and Irish laws promoting surveillance through data retention requirements.[420] Liberty UK also uses test case litigation to protect and preserve human rights and civil liberties.[421]

Campaigns

CSOs organise campaigns against the use of surveillance technologies. NO2ID[422] and Liberty[423] campaigned against ID cards. Bits of Freedom protested at Schiphol airport against the transfers of European passenger data to the US. Netzwerk Neue Medien/Network New Media (NNM) (Germany) and other CSOs demonstrated against increasing surveillance of citizens in Berlin.[424] LeaveThemKidsAlone campaigns against the "widespread use of biometrics in UK schools".[425] In a novel protest campaign against the use of biometric data, the Chaos Computer Club acquired and published the fingerprints of Wolfgang Schäuble, the German Home Secretary in the club's magazine Die Datenschleuder.[426] The Drone Campaign Network (DCN)[427] organised protests at various locations during a week of action from 6-13 October 2012 to protest the growing use of armed drones in the world. These campaigns have direct and indirect effects on the surveillance industry.

Defensive actions and countermeasures

CSOs such as the Electronic Frontier Foundation promote defensive actions and countermeasures against surveillance.[428] They educate people about managing surveillance

[420] *Digital Rights Ireland Limited v The Minister for Communication Marine and Natural Resource et al*, High Court, Record No. 2006/3785P. http://www.scribd.com/doc/30950035/Data-Retention-Challenge-Judgment-re-Preliminary-Reference-Standing-Security-for-Costs

[421] Liberty. http://www.liberty-human-rights.org.uk/about/index.php

[422] www.no2id.net/

[423] http://www.liberty-human-rights.org.uk/human-rights/privacy/index.php

[424] Netzwerk Neue Medien, "Demo against surveillance in Berlin on Saturday, 17 June", 14 June 2006. http://www.nnm-ev.de/show/158205.html
http://translate.google.com/translate?depth=1&hl=en&prev=/search%3Fq%3DNetzwerk%2BNeue%2BMedien%26hl%3Den%26rlz%3D1I7SVEA_enGB350%26prmd%3Dimvns&rurl=translate.google.co.uk&sl=de&u=http://www.nnm-ev.de/show/158205.html

[425] www.leavethemkidsalone.com/

[426] Kleinz, Torsten, "CCC publishes fingerprints of German Home Secretary", *Heise Online*, 31 March 2008. http://www.h-online.com/newsticker/news/item/CCC-publishes-fingerprints-of-German-Home-Secretary-734713.html

[427] https://dronecampaignnetwork.wordpress.com/2012/07/05/hello-world/. The organisation is a "UK-based network of organisations, academics and individuals working together to share information and coordinate collective action in relation to military drones". Membership is open to organisations and individuals on invitation basis.

[428] Electronic Frontier Foundation, The Surveillance Self-Defense Project. https://ssd.eff.org/

risks by using technologies such as secure deletion software, file and disk encryption software, and virtual private networks.[429]

Observatories

CSOs such as Statewatch maintain observatories such as the Observatory on EU-PNR (Passenger Name Record),[430] the Observatory on the Surveillance of Telecommunications in the EU[431] and UK: Surveillance Statistics: 1937-2011,[432] which function as information repositories for surveillance industry stakeholders.

Best practice collaborations

CSOs collaborate with industry to develop best practice for surveillance technologies. Liberty made best practice recommendations and was influential in getting the UK CCTV camera industry to rely upon voluntary codes of practice that addressed civil liberties concerns.[433]

Advice and training

Advice and training are important activities for many CSOs. Advice and training may be addressed to different stakeholders, e.g., government, industry or the general public.

The Open Rights Group (ORG) runs a Censorship and Surveillance Campaign Training to "equip activists to help stop the Snoopers' Charter and Mass Internet Blocking" and educate people across the UK about the interception and collection of their information.[434] The training includes a briefing on issues, overview of the campaigns and practical training on how to speak to one's Member of Parliament.

Networking and events organisation

One of the major activities of CSOs is networking, i.e., developing and facilitating relationships with fellow CSOs, governments, industry, academia and media. CSOs organise networking events such as specialist seminars, talks, conferences that bring together industry and other stakeholders, foster dialogue and partnerships.

Sharing of expertise

A major activity CSOs undertake is sharing their expertise. For instance, the Deutsche Vereinigung für Datenschutz (DVD) in Germany participates in parliamentary hearings on general and sector-specific privacy laws at the federal and state level.[435] The Foundation for

[429] Electronic Frontier Foundation, Defensive Technology. https://ssd.eff.org/tech
[430] EU-PNR (Passenger Name Record), 2011. http://www.statewatch.org/Targeted-issues/eu-pnr/eu-pnr-observatory.htm
[431] The surveillance of telecommunications in the EU (from 2004 and ongoing). http://www.statewatch.org/eu-data-retention.htm
[432] http://www.statewatch.org/uk-tel-tap-reports.htm
[433] Liberty, Liberty's Response to the Home Office Consultation on a Code of Practice relating to Surveillance Cameras, May 2011, p. 4. http://www.liberty-human-rights.org.uk/pdfs/policy11/liberty-s-response-to-the-consultation-on-a-code-of-practice-relating-to-sur.pdf
[434] Open Rights Group, Censorship and Surveillance Campaign Training. http://www.openrightsgroup.org/events/2012/censorship-and-surveillance-campaign-training
[435] http://www.datenschutzverein.de/vereinsprofil_dvd.html

Information Policy Research's (FIPR) Chair Ross Anderson is a Special Adviser to the UK House of Commons Health Committee inquiry into the Electronic Patient Record.[436]

Investigating and tracking the industry

A major means by which CSOs keep tabs on the surveillance industry is through focused investigations whose results aim to provide independent information about surveillance companies and their activities. The prime example is Privacy International's Big Brother Inc. which investigates the international trade in surveillance technologies.[437] The investigation had three objectives:

- To raise worldwide awareness of the dangers of surveillance technologies and the ethical failures of the surveillance industry.
- To ensure that export controls are put in place in Europe and the US to restrict the sale of surveillance technologies to repressive regimes.
- To seek redress for those who have suffered harm as a result of Western-manufactured surveillance technologies

CSOs track surveillance procurement and expenditures. Big Brother Watch produced a report[438] on how much Councils across the UK spend on CCTV.[439] OpenSpending.org, a project of the Open Knowledge Foundation (not strictly a surveillance-focussed CSO), monitors every (public) government and corporate financial transaction across the world, including surveillance companies.[440]

Big Brother Awards

Annually, Privacy International and its affiliates[441] present the Big Brother Awards,[442] judged by juries of lawyers, academics, consultants, journalists and civil right activists to government agencies, private companies and individuals who have egregiously violated privacy.

In Germany, 2012 recipients include Gamma International subsidiary FinFisher (for surveillance technology), video game company Blizzard Entertainment, Inc (for user surveillance), German-based frozen foods manufacturer Bofrost (employee surveillance), water filtration company Brita GmbH (for installing water vending machines in schools that dispensed water only to students who tapped them with RFID chipped bottles). The German judges reportedly criticised the latter practice thus:

> This water bottle system is a glaring example of the industry's attempts to establish a culture of overtechnisation, surveillance and blatant paternalism from early childhood."[443]

[436] www.fipr.org/achievements.html
[437] Privacy International. https://www.privacyinternational.org/projects/big-brother-inc
[438] Big Brother Watch, *The Price of Privacy: How local authorities spent £515 million on CCTV in four years*, February 2012.
http://www.bigbrotherwatch.org.uk/files/priceofprivacy/Price_of_privacy_2012.pdf#.T0OlbfI8Cd4
[439] http://www.bigbrotherwatch.org.uk/home/2012/02/price-privacy-councils-spend-521m.html
[440] http://openspending.org/
[441] Such as Bits of Freedom (Netherlands), Electronic Frontier (Finland), FoeBuD (Germany), Iuridicum Remedium (Czech Republic), Quintessenz (Austria) and Technika az Emberert Alapitvány (Hungary).
[442] Big Brother Awards International. http://www.bigbrotherawards.org/
[443] Electronic Frontier Foundation, "And the Privacy Invasion Award Goes To …", 11 May 2012.
https://www.eff.org/deeplinks/2012/05/and-privacy-invasion-award-goes-to

Facebook received the Dutch award for bad privacy practices[444]; MIVB/STIB (Brussels metro)[445] received the Belgian award for its Mobib card which raises personal data and anonymity concerns.[446]

Research projects

CSOs commission, undertake and/or collaborate in surveillance and security research projects. This activity enables them learn about, engage and influence the surveillance industry. The Danish Institute for Human Rights partnered in DETECTER, the Detection technologies, terrorism, ethics and human rights project.[447]

Dissemination of information

Perhaps the most crucial and universal activity of most CSOs is the dissemination of information. Equipo Nizkor, a Spanish CSO, intends "putting as much information as possible in the hands of as many people as possible".[448] Dissemination of information occurs through newsletters, media reports, press releases, articles, blogs, etc. Quintessenz publishes a free newsletter on electronic surveillance.[449] Bits of Freedom co-ordinates the publication of the *EDRi-gram*[450] and publishes a Dutch newsletter with digital and privacy related news. The German Humanist Union publishes the *Grundrechte-Report*, an annual report on the state of human rights and civil liberties in Germany and *vorgänge*, a journal for politics and critical societal analysis. The Open Rights Group blogs on surveillance-related topics such as behavioural tracking. Statewatch disseminates surveillance-related news, e.g., judicial enquiries into surveillance technology companies, technologies being implemented by companies and controversial surveillance technology exports.

Public awareness

CSOs undertake public awareness actions. In 2002, Bits of Freedom organised the *Spot the Cam* campaign aimed at creating public awareness of ubiquitous surveillance cameras. Under a project co-ordinated by the French League of Human Rights (LDH), in partnership with the European Association for the Defence of Human Rights (AEDH), European Digital Rights (EDRi), the Czech association Iuridicum Remedium (IuRe) and the Catalan association Comunicació per a la Cooperació (Pangea), a comic book "Under surveillance" was created to sensitise young European citizens about data protection.[451]

Effect upon industry and industry's response

CSOs and their actions have many effects upon the surveillance industry. CSOs and the industry are at odds with each other; they seek entirely different ends and often compete in relation to advancing their interests to other stakeholders (such as the government, other end

[444] *EDRi-gram*,, "Winners of the Dutch Big Brother Awards announced", 14 March 2012. http://www.edri.org/edrigram/number10.5/bba-netherlands-2012
[445] www.stib.be
[446] *EDRi-gram*,, "Belgian Big Brother Awards 2012", 1 Feb 2012. http://www.edri.org/edrigram/number10.2/belgian-bba-2012
[447] www.detecter.eu/
[448] Equipo Nizkor, About us. http://www.derechos.org/nizkor/about.html
[449] Quintessenz, What we do. http://www.quintessenz.at/cgi-bin/index?funktion=about
[450] *EDRI-gram* is a bi-weekly newsletter about digital civil rights in Europe. See http://www.edri.org/edrigram
[451] EDRi. http://www.edri.org/campaigns/comic-book-under-surveillance

users and the general public). Their relationship with each other is positive and negative at the same time.

CSOs influence industry (particularly in terms of their corporate social responsibility) and strengthen accountability. By raising concerns in relation to new and existing surveillance technologies, they enable the industry to keep an eye on the larger public and social interests. They thus help build and force the surveillance industry to be conscious of the societal effects of the technologies it develops and markets.

Using inputs and guidance from CSOs, a surveillance company might sensitise itself to human rights concerns of its business and technologies and demonstrate that its practices are in accordance with social values. CSOs can help companies identify, monitor and mitigate privacy and other risks, of surveillance technologies. Thus, they foster corporate social responsibility. By keeping a watchful eye on the industry in general and companies in particular, CSOs apply compliance pressures on surveillance companies.

Effectiveness analysis

Some argue that the role of civil society is little understood by the military and defence sectors, which have traditionally been resistant to public input. Others state that civil society doesn't have either the necessary expertise or interest needed to provide an informed input into what is a uniquely specialised policy area.[452] Many CSOs lack expertise to deal with ever developing surveillance technologies and threats.[453]

To a substantial extent, this might apply to the relationship between CSOs and the surveillance industry. The role of CSOs in regulating the surveillance industry, though it leaves much to be desired (particularly in terms of holding the industry to account and helping it discharge its human rights obligations), must not be downplayed.

3.8.3 Media

This section examines the relationship and role of the mass media in watching over the surveillance industry. The mass media play several important roles – they investigate, communicate and raise awareness. In performing these roles, the media monitor and, to a certain extent, regulate the surveillance industry.

The surveillance industry in turn recognises the importance of the mass media to promote their products, services and business and allocates human and financial resources to maintain a positive relationship with the media.

[452] Global Facilitation Network for Security Sector Reform, Civil Society and Security. http://www.ssrnetwork.net/topic_guides/civil_soci.php

[453] Ball, N., "Civil Society Actors in Defence and Security Affairs", in M. Caparini, P. Fluri and F. Molnar (eds.), *Civil Society and the Security Sector: Concepts and Practices in New Democracies*, DCAF, Geneva, 2006, Ch. 4; Caparini, M., and P. Fluri "Civil Society Actors in Defence and Security Affairs", in M. Caparini, P. Fluri and F. Molnar (eds.), *Civil Society and the Security Sector: Concepts and Practices in New Democracies*, eds. DCAF, Geneva, Ch.1.

Key organisations

Mass media include the different communication media such as the press, broadcast media (such as radio, TV,[454] films, documentaries,[455] advertising), online media (journals, webzines, blogs) that reach a large audience. We provide a few examples or snapshots of media coverage of the surveillance industry in Europe.

Der Spiegel (Germany)

Der Spiegel has carried reports of the practices of the surveillance industry and their customers (e.g., supermarket chain Aldi[456]) in Germany and controversial exports of surveillance technologies.[457]

TechWeekEurope (UK)

NetMediaEurope's TechWeekEurope has highlighted issues such as the use of surveillance powers by publicly funded organisations such as the BBC under the Regulation of Investigatory Powers Act (RIPA),[458] passenger surveillance by airline company British Airways,[459] VoIP surveillance by Skype[460] and aerial visual surveillance by Apple.[461]

Channel 4 (UK)

Channel 4 has sought to expose surveillance practices such as the installation of "black boxes" to monitor UK Internet and phone traffic, and decode encrypted messages.[462]

Radio Netherlands

Radio Netherlands has highlighted the expanding use of surveillance technologies,[463] increasing societal monitoring and securitization,[464] evolution/new developments in

[454] e.g., Panorama series. www.bbc.co.uk/programmes/b006t14n
[455] For instance, David Bond and Melinda McDougall (Directors), *Erasing David*, Green Lions, UK, 2009. http://erasingdavid.com/
[456] *Spiegel Online*, "Aldi Spied on Female Shoppers", 30 April 2012. http://www.spiegel.de/international/germany/aldi-spied-on-female-shoppers-with-hidden-cameras-a-830690.html
[457] *Spiegel Online*, "Siemens Allegedly Sold Surveillance Gear to Syria", 4 Nov 2012. http://www.spiegel.de/international/business/ard-reports-siemens-sold-surveillance-technology-to-syria-a-826860.html; Buse, Uwe, and Marcel Rosenbach, "The Transparent State Enemy Western Surveillance Technology in the Hands of Despots", *Spiegel Online*, 12 Aug 2011. http://www.spiegel.de/international/world/the-transparent-state-enemy-western-surveillance-technology-in-the-hands-of-despots-a-802317.html
[458] Brewster, Tom, "BBC Under Fire For Secret Use Of RIPA Surveillance Powers", *TechWeekEurope*, 22 Aug 2012. http://www.techweekeurope.co.uk/news/bbc-ripa-surveillance-bbw-big-brother-90086
[459] Jowitt, Tom, "BA Hits Privacy Turbulence Over Passenger Profiling", *TechWeekEurope*, 6 July 2012. http://www.techweekeurope.co.uk/news/ba-privacy-passenger-profiling-85310
[460] Brewster, Tom, "Skype Surveillance Claims Denied", *TechWeekEurope*, 27 July 2012. http://www.techweekeurope.co.uk/news/skype-sp-claims-denied-87703
[461] Smolaks, Max, "Apple Sends Out Spy Planes To Challenge Google Maps", *TechWeekEurope*, 11 June 2012. http://www.techweekeurope.co.uk/news/apple-spy-planes-google-maps-81842
[462] Channel 4 News, "'Black boxes' to monitor all internet and phone data", *Channel 4 News*, 29 June 2012. http://www.channel4.com/news/black-boxes-to-monitor-all-internet-and-phone-data
[463] Ford, Davion, "Dutch police look to expand spying powers", *Radio Netherlands Worldwide*, 27 Dec 2011. http://www.rnw.nl/english/video/dutch-police-look-expand-spying-powers

surveillance technologies,[465] usefulness of CCTV cameras,[466] the surveillance potential and behaviour of social media companies.[467]

Twitter, Wikileaks and blogs

Online social media play an important role in watching over the surveillance industry. These platforms not only expose (in the case of Wikileaks) but also facilitate a very broad discussion of surveillance industry practices, ethics and other concerns. One example is Jean Marc Manach, a journalist's Twitter feed sharing information and commentary on surveillance related issues.[468]

There are many other similar examples; and it is near to impossible to report all of these. A huge range of international, regional, national and local media report about surveillance industry, though the extent and nature of such coverage varies. For instance, some media specifically focus on surveillance issues and concerns regularly, while others report sporadically or casually. Some media function as the industry's voice; some adopt an anti-industry stance giving wide coverage to surveillance concerns and issues.

Monitoring motivations

A review of the mass media coverage of the surveillance industry reveals the following core monitoring motivations:

- To provide and disseminate information about the surveillance industry
- To influence policy and public opinions of the surveillance industry
- To raise public awareness of the surveillance industry
- To educate the public about surveillance.

Actions taken

As shown before, the mass media investigate surveillance companies, the industry, impact of surveillance technologies, report on the development of new surveillance technologies, key and upcoming players in the industry, the business and funding of surveillance, surveillance technology concerns and abuses, good practices, surveillance opportunities and the future of surveillance technologies.[469] The media publish articles, reports, reviews, opinions, editorials, commentary or commission and present films, broadcasts, interviews.

Effect upon industry and industry's response

The mass media is a very important watcher of the surveillance industry. If it plays its role effectively, it is a very powerful, visible industry regulator. Through exposing the surveillance

---

[464] Radio Netherlands Worldwide, "Earth Beat – Born free", *Radio Netherlands Worldwide,* 25 Dec 2011. http://www.rnw.nl/english/radioshow/born-free

[465] Ibid.

[466] Radio Netherlands Worldwide, "Dutch border police happy with CCTV cameras", *Radio Netherlands Worldwide*, 29 March 2011. http://www.rnw.nl/english/bulletin/dutch-border-police-happy-cctv-cameras

[467] Groot, Willemien, "Who's afraid of wiretap-friendly social media?" *Radio Netherlands Worldwide*, 11 May 2012. http://www.rnw.nl/english/article/who%E2%80%99s-afraid-wiretap-friendly-social-media

[468] http://twitter.com/manhack

[469] Gren, Martin, "Eyeing the future of video surveillance", *Technology Spectator*, 23 Aug 2012. http://technologyspectator.com.au/eyeing-future-video-surveillance (CCTV)

industry, its practices, concerns and abuses, it can regulate the industry's actions and pressure it to conform to legal and social obligations and values. For example, an extremely critical review of a surveillance company's technology or dealings with dubious clients (e.g., repressive regimes) might result in a public outcry that gets the technology banned and negative publicity and image for the company.[470] Therefore, surveillance companies devote financial and human resources to media and public relations (many surveillance companies have dedicated media liaison persons/and or departments).

The mass media are also a platform for other stakeholders such as the academia, civil society organisations and the public to express their views and share opinions on the surveillance industry. Thus, they enable surveillance industry stakeholders to engage and keep track of one another. For instance, the government can form opinion, take policy and legal action to regulate the surveillance industry based on media reports. Civil society organisations use the media to raise public awareness of social and ethical concerns (e.g., privacy, freedom of expression and movement) in relation to surveillance technologies. Thus, the mass media enable other watchers of the surveillance industry to play a more effective role in monitoring the surveillance industry.

Effectiveness analysis

A question arises as to how effective the mass media are in watching over the surveillance industry. The mass media have great potential as watchers of the surveillance industry but concerns and issues remain. One concern is how the media sometimes resort to surveillance technology scaremongering. Surveillance as a security measure is a necessary and real fact of the European security landscape. Biased scaremongering that portrays good surveillance technologies in a bad light might mean such technologies are rejected in favour of worse technologies (e.g., a privacy enhancing surveillance technology might be rejected in favour of a privacy reducing one).

Media carelessness in getting the facts right might tip the scales in favour of some surveillance technologies and companies. The mass media is often manipulated by large and medium-size surveillance companies and harnessed to their advantage. In such cases, these media cannot function as effective watchers of the surveillance industry.

3.8.4 Academia

Academia promotes and collaborates in research and events on surveillance technologies, their potential and actual effects, need for their regulation, etc. In this manner, they have an indirect watching effect over the industry.

Key organisations

The most noteworthy organisation is the Surveillance Studies Network (SSN), a charitable company registered in the UK dedicated to the "study of surveillance in all its forms, and the free distribution of scholarly information". [471]

[470] Silver, Vernon, "European Union Bans Exports to Syria of Systems for Monitoring Web, Phones", *Bloomberg News*, 1 Dec 2011. http://www.bloomberg.com/news/2011-12-01/european-union-bans-exports-to-syria-of-systems-for-monitoring-web-phones.html

[471] Surveillance Studies Network. http://www.surveillance-studies.net/

Monitoring motivations

According to the SSN's website, its key motivation is:

> The advancement of education for the public benefit by the promotion of the study of surveillance as a facet of contemporary social and technological change and its consequences for individuals, groups, organisations, nations and regions.[472]

Actions taken

The SSN undertakes the following activities:

- Supporting and promoting the free exchange of academic information about surveillance across academic disciplines and cultures;
- Promoting learning and the sharing of knowledge about surveillance between scholars, students, organisations and the public world-wide;
- Owning and publishing the journal *Surveillance & Society* and other online resources devoted to the publication of communications which advance knowledge concerning the study of surveillance and society.[473]

Effect upon industry and industry's response

Though the SSN might enable other stakeholders to watch over the surveillance industry, we cannot pinpoint the exact effect upon the industry.

Effectiveness analysis

The main advantage of the organisations such as the SSN and other academic watchers of the industry is that they present platforms for research and collaboration between stakeholders.

3.9 CONCLUSION

The global and European surveillance industry is developing at a rapid pace, stimulating and supplying increasing demands in the public and private sector, across a range of areas such as national defence and security, critical infrastructure, banking, employment, energy and utilities, entertainment, finance, government, healthcare, policing and justice, retail, telecommunications, travel and transport.

Various factors drive the industry: pro-surveillance policy and legislation, research and innovation, financial support and funding, profits, positive media coverage and public demand. On the other hand, inhibitors such as policy shifts, restrictive legislation, inadequate research, development and innovation, lack of finances/funding, losses, negative media publicity and lack of public demand or rejection curtail it.

The surveillance industry in Europe is characterised by a diversity of companies (based on organisational history, revenues, size, location, operation and organisational focus) providing a variety of surveillance solutions and a portfolio of expanding applications. The industry is a

[472] Surveillance Studies Network, Charitable Objects. http://www.surveillance-studies.net/?page_id=107
[473] Ibid.

profit-driven, profit-motivated industry. Investment in manufacture, integration, provision or sale of surveillance technologies is generating high levels of income for companies fuelled in particular by government public sector demand and expenditure. To boost their position and influence, surveillance companies are collaborating, making acquisitions and forming strategic partnerships and alliances and entering into joint ventures with other companies, academia and research institutions.

The surveillance industry in Europe is characterised by the presence of a large number of non-European companies, particularly from the USA. Conversely, European companies, driven by the economic downturn in Europe, huge potential of foreign market and their receptiveness to surveillance solutions, are investing heavily in non-European markets such as North and South America, Asia and Africa.

Surveillance companies have courted controversies such as unethical and even illegal business practices, illegal government subsidies, privacy and security concerns, sale of technologies to authoritarian and undemocratic regimes, human rights abuses, conflict zone profiteering, general surveillance-related profiteering and pro-surveillance thrusts, misleading consumers, and anti-competitive practices. Overall, this has affected the industry's reputation as a whole. The European surveillance industry (individual companies and industry associations) needs to take stock of this.

In sum, the future of surveillance is set. Most surveillance reports predict an increasing demand for surveillance solutions (stand-alone and integrated), rapid growth for the industry and strong market growth prospects. We identified the following trends: (1) a substantial growth of public sector demand for surveillance bolstered by the adoption of identity schemes, and terrorist detection technologies and markets, (2) an increase in the demand for civil and commercial surveillance, (3) development of a global industry in surveillance, (4) an increase in integrated surveillance solutions, (5) an increase in government use of cross-border surveillance solutions. Surveillance companies from Europe will face stiff competition from companies based outside the European Union.

Despite a generally positive outlook, the surveillance industry can expect to face challenges in the future. One challenge is the lack of security awareness and attitudes, resulting from a decreased demand for security and surveillance products and services. Another challenge is stricter government regulation which may stifle the development and growth of the industry. Financial challenges – higher duties and costs applicable to surveillance products – might deter the industry's future prospects and growth. Some surveillance technologies may be rejected by the public due to privacy, ethical and other human rights concerns. Competition is another challenge the surveillance industry in Europe faces; if the industry is to flourish, it must learn to deal with this.

Surveillance industry associations play an important role in the surveillance industry and in its interactions with other stakeholders. They promote and increase the use of their members' products and services, facilitate collaboration, promote research and development, establish policy, guidelines and standards, engage with the public and raise awareness of concerns such as security, safety, crime prevention and prosecution that ultimately drive and boost the demand for the surveillance industry's products and services. Industry associations also influence policy, particularly security policy at different levels – e.g., government, law and research. In addition, they organise and sponsor events, provide information and training, conduct networking activities, fund and disseminate research, encourage and develop best

practices, lobby government and policy-makers, develop strategic partnerships, maintain public and media relations. In any resilience-building exercise that needs to have deep impact, it would be advisable to harness the power of these associations.

Surveillance companies exert a great amount of influence through participation in security policy-related bodies such as the European Defence Agency (EDA), the European Organisation for Security (EOS) and European Security. Surveillance companies are increasingly intersecting with the public sector in the performance of traditionally public sector-restricted activities and are involved in many European research projects on security, information and communication technologies.

Some surveillance companies provide assurances that they act in conformity with legal and social obligations and values; however, these are inadequately expressed and followed through. A majority of companies neglect this aspect. Concerns have been expressed in relation to companies and fundamental rights – privacy, data protection, freedom of expression, freedom of movement. While some good practices exist, these are not enough; as stated before, they are inadequate in terms of the potential of some of the surveillance technologies the industry is developing and marketing.

No one entity (whether government, media, civil society, academia or individuals) can play a self-sufficient role in watching over the surveillance industry. Individually, each of these watchers is limited by their motivations and activities. Given the nature of the surveillance industry and its ever expanding potential to infringe upon fundamental rights and liberties, we recommend the formation and development of multi-stakeholder platforms and forums to monitor the industry (more collaboration is required between *all* stakeholders) to achieve a greater effect and ensure that the resilience of society is improved.

4 THE EFFECTIVENESS OF SURVEILLANCE IN PREVENTING AND DETECTING CRIME AND TERRORISM

Reinhard Kreissl, IRKS

4.1 INTRODUCTION

The idea that criminal or violent behaviours can be detected and/or prevented through surveillance practices emerges with modern law enforcement and police.[1] From the very beginning of the modern fight against crime, surveillance practices received mixed responses from the public, since it was always considered to be related to an illegitimate secrecy.[2] Surveillance practices have developed a long way since these early days, and contemporary law enforcement officials see a concept of "predictive policing" on the horizon.[3] This would enable crime prevention through prediction based on computer algorithms, processing historical and real-time data from surveillance systems and other sources.

Looking at the history of surveillance and crime prevention or detection, the co-evolution of technological development and law enforcement strategies becomes obvious. Most new technologies, developed for different applications, can be used for surveillance and fighting crime one way or another: from DNA to sensor technologies to advanced data processing technologies such as data-mining, each technological innovation is prone to function creep into the field of law enforcement and security work. And each new wave of surveillance technology receives mixed responses in public discourse. Whereas the critics taking a rights perspective point to the dangers that go along with new surveillance practices (such as loss of privacy, encompassing control, social sorting, loss of civil liberties, etc.), the supporters take a threat-based position, pointing to the damage caused by criminal or terrorist activities and the need to do whatever is technologically possible to prevent, detect or deter such activities.

Since the operational activities of law enforcement and police work are not openly discussed and typically are hidden from the general public, it is often difficult to assess the effects and effectiveness of individual strategies applied to detect and prevent criminal or terrorist acts. So in the first part of what follows, we briefly address key issues arising when talking about crime and crime prevention. The same is true for the surveillance practices and the technologies applied in the field of law enforcement and detection. We address these conceptual issues in more detail below.

After these brief introductory sections, we present and discuss some of the more important surveillance technologies, used in preventing crime and terrorism. This presentation has to be selective, since it would be beyond the scope of this report to give a comprehensive account of all of the different surveillance practices used by the police and law enforcement. After the discussion of selected surveillance practices, we look at the merging of different technologies

[1] Radzinowicz, Leon, *A history of English criminal law and its administration from 1750*, Vol. 4, Stevens and Sons, London, 1948.
[2] Shpayer-Makov, Haia, *The Ascent of the Detective: Police Sleuths in Victorian England*, Oxford University Press, Oxford, 2011. passim.
[3] Ferguson, Andrew Guthrie, "Predictive Policing and the Future of Reasonable Suspicion", *Emory Law Journal*, 2012 [forthcoming]. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2050001

and the emergence of surveillance assemblages. The chapter ends with a brief section trying to give an informed assessment of the effectiveness, the effects and side effects of surveillance in the fight against crime and terrorism.

4.1.1 Assessing the effectiveness of crime prevention and detection

"Crime" is not a natural phenomenon.[4] Crime is highly variable and context-dependent. The basic lesson learned from legal theory and critical criminology is that crime is a question of ascription (or labelling) and nothing to be read off behaviour.[5] This means to understand "crime" requires an understanding of the social processes that underlie the definition or negotiation of certain behaviours as criminal. Though there may seem to be clear cases of criminal, violent or terrorist acts or behaviours, a closer look reveals contingencies at all levels, micro, meso and macro. At the micro-level, behaviour is negotiated among police officers and potential suspects and whether an individual in a given situation is treated as a deviant, criminal or law-abiding citizen depends on how discretion is exercised in these local negotiations.[6] At the meso-level, local organisational cultures shape the handling of individuals as criminals, creating local cultures of control.[7] At the macro-level not only can terrorism be conceived as a politically motivated revolutionary strategy, but also within societies, we can observe negotiated shifts, definitions and re-definitions of what is conceived and treated as crime, as, e.g., with rape in marriage.[8]

When taking the notion of crime as a locally negotiated, socially defined and politically contested concept as a starting point, crime waves should be understood as effects of mutually reinforcing public (media) attention, mirroring power relations and law enforcement activity. When "crime goes up", one has to look at changes at the level of crime discourse and at behaviour simultaneously. Intensified media attention will increase public concern about crime and raise general awareness for crime problems. A typical example here is the case of sexually motivated abuse of minors. Looking at the figures of registered offences known to the police over a period of several years or at surveys,[9] the levels of registered offences has not changed significantly or even dropped. Comparing these figures with the media coverage of sexual offences and offenders, there is an obvious discrepancy, since media reporting has gone up dramatically. Similar effects have been observed in the field of drug abuse.[10]

From the perspective of the layperson, the increase in media attention creates the impression of sexual offenders or drug addicts as an imminent threat to the general public. This in turn motivates policy-makers to step up measures against these perceived threats, ask for higher

---

[4] Hacking, Ian, "A Tradition of Natural Kinds", *Philosophical Studies*, Vol. 61, No. 1-2, 1991, pp. 109-126.
[5] Hart, Herbert L.A., "The Ascription of Responsibility and Rights", in Anthony Flew (ed.), *Essays on Logic and Language*, Oxford University Press, Oxford, 1949, pp. 145-166. Becker, Howard, *Outsiders*, Free Press, New York, 1963.
[6] Klinger, David A., "Negotiating Order in Patrol Work: An ecological Theory of Police Response to Deviance", *Criminology*, Vol. 35, Issue 2, May 1997, pp. 277-306.
[7] Cicourel, Aaron V., *The social organization of juvenile justice*, New York, 1967. Kreissl, Reinhard and Lars Ostermeier, "Globale Trends und lokale Differenzen – Kulturen der Kontrolle und politische Steuerung in Hamburg und München", Kriminologisches Journal, Beiheft 9, 2007, pp. 137-151.
[8] Paetow, Barbara, *Vergewaltigung in der Ehe: eine strafrechtsvergleichende Untersuchung unter besonderer Berücksichtigung des Rechts der Vereinigten Staaten*, Max-Planck-Institut für ausländisches und internationals Strafrecht, Freiburg i. Breisgau, 1987.
[9] See Stadler, Lena, Steffen Bieneck and Christian Pfeiffer, *Repräsentativbefragung Sexueller Missbrauch 2011*, Forschungsbericht Nr. 118, KFN, Hannover, 2012.
[10] Beckett, Katherine, *Making Crime Pay: Law and order in Contemporary American Politics*, Oxford University Press, New York, 1997.

prison sentences and more surveillance (e.g., after release of sex offenders or drug addicts). What can be studied here is the self-propelled nature of a publicly perceived crime wave or "moral panic"[11] lacking clear evidence in the official crime statistics. "Crime" as social fact is not an entity existing independently of the observers' actions. When analysing crime as a social fact, a kind of uncertainty relation comes into play, i.e., the object under investigation is not independent of the observer investigating it.

As we know from the sociology of the media,[12] public awareness raises the number of incidents known to the police, which in turn raises the number of registered crimes, which in turn has an effect on media coverage, which in turn raises public awareness. The causal chain operative here can be typified like this:

(a) The most important source of information about crime for the media are police sources.

(b) Citizens' knowledge about crime is primarily based on media coverage of crimes known to the police.

(c) A very large proportion of crimes known to the police are based on citizens' reports (as victims or witnesses).

From a theoretical point of view, what we see here is a feedback cycle. Crime waves, i.e., rising rates of registered crimes and/or rising media coverage and public concern about crime problems in a society can emerge through such feedback cycles. Public concern can then trigger political activities (e.g., increased and extended surveillance measures), which in turn can have an effect on the registered crime rates.

With regard to surveillance, this means one has to look at what stage the issue of surveillance as a rational and effective strategy to combat crime enters public discourse (i.e., the feedback cycle between public awareness, police strategies and political projects). So drawing on official figures such as crime rates, reported by the police may seem only as a partly feasible solution when trying to assess the effectiveness of surveillance practices to prevent and fight crime and terrorism. Though these figures do have their limitations, they nonetheless can be taken as a somewhat better representation of crime compared to public arousal and media coverage. Starting with registered crime as an empirical basis has important consequences when looking at the problem of law enforcement. The effectiveness of the fight against crime can have two contradicting interpretations:

- Either policing can be seen as effective, when the rate of crimes known to the police is low, which then can be interpreted as a result of effective police work, deterring criminals.
- Or policing can be seen as effective, when the number of registered crimes goes up, since this can be understood as a proof of effective police work to identify and arrest criminals.[13]

Each interpretation has its plausibility and so the quantitative development of the registered crime rate is not easily interpreted when it comes to the problem of how effective the fight against crime is and how it is affected by surveillance measures.[14]

---

[11] Cohen, Stanley, *Folk Devils and Moral Panics*, Routledge, New York, 2002.

[12] Barak, Greg (ed.), *Media, Process, and the social construction of crime: studies in newsmaking criminology*, Garland Publishing, New York, London, 1994.

[13] On the controversial debates about the effects of the so called "Zero Tolerance" approach in New York, see, e.g., Bowling, Ben, "The rise and fall of New York murder: zero tolerance or crack's decline?", *British Journal of Criminology*, Vol. 39, No. 4, 1999, pp. 531-554. Greene, Judith A., "Zero Tolerance: A Case Study of Police Policies and Practices in New York City", *Crime & Delinquency*, Vol. 45, No. 2, April 1999, pp. 171-187.

A more general problem arises when analysing the effectiveness of crime prevention measures that could be termed the problem of the non-event.[15] Following the first line of reasoning listed above, i.e., conceiving of the fight against crime as effective when crime rates go down, it is very difficult to substantiate the evidence, particularly when it comes to serious threats such as terrorist attacks. The claim that a substantial number of terrorist attacks were prevented on the basis of massive surveillance is hard to verify independently.

Looking at the effectiveness of surveillance as an element in fighting crime and terrorism, we need to consider the kind of evidence produced to demonstrate this effectiveness. At the same time, it has to be kept in mind that different surveillance strategies and technologies can create an array of different effects.

On the one hand, there are effects that could be called first order: making behaviour more visible, identifying individuals more easily or improving panoptical control of individuals and their movements in public space. Following the rationale behind surveillance, this increased transparency of society facilitates the early identification of potential predators. This claim can be contested, when second order effects are taken into account.

Such second order effects comprise the creation of new categories of suspicious behaviour, producing information and data overload in the daily routine of law enforcement work, redirecting attention from observation of real-world events to analysis of data sets produced through surveillance technologies. What also often is ignored in the debate about the effectiveness of surveillance as a means to fight crime and terrorism is the impact of new technologies on the working routines and everyday knowledge of the field operatives in the domain of law enforcement and crime detection.[16]

Finally, there is a kind of consequence that could be termed tertiary effects. As Machado and Prainsack[17] have demonstrated, prisoners develop theories about the efficacy of DNA technology often over-emphasising their potential. This so-called CSI-effect can have a deterrent effect, when conceived in the frame of crime prevention, or it can trigger an attitude of "preventive paranoia" fostering conspiracy theories when seen from the perspective of the citizen, living in a surveillance society and being constantly monitored.[18]

Those criminal acts made visible to a larger public through surveillance become popularised in a specific way. Seeing footage from a CCTV camera showing a presumed burglary scene in action on TV creates a kind of reality effect far beyond any narrative or statistical information and supports the construction of urban legends about crime. The idea of crime made visible

---

[14] See, e.g., Phillips, Coretta, "A Review of CCTV Evaluations: Crime Reduction Effects and Attitudes towards its Use", *Crime Prevention Studies*, Vol. 10, 1999, pp. 123-155.

[15] Mackenzie, Simon, and Niall Hamilton-Smith, "Measuring police impact on organised crime: Performance management and harm reduction", *Policing: An International Journal of Police Strategies & Management*, Vol. 34, Issue 1, 2011, pp. 7-30.

[16] Rappert, Brian, "The Distribution and Resolution of the Ambiguities of Technology, or Why Bobby Can't Spray", *Social Studies of Science*, Vol. 31, No. 4, 2001, pp. 557-591.

[17] Machado, Helen, and Barbara Prainsack, *Tracing Technologies: Prisoners' Views in the Era of CSI*, Ashgate, Farnham, 2012.

[18] Bartlett, Jamie, and Carl Miller, *The power of unreason: Conspiracy theories, extremism and counter-terrorism*, Demos, London, 2010.

through CCTV has become part and parcel of modern media culture.[19] Establishing the idea of surveillance as a normal and effective element in fighting crime also increases public support for investing in ever more "sophisticated" or "intelligent" technology in this domain.

4.1.2 Different types of crime and changing paradigms of crime control

Crime covers a wide array of social phenomena: from visible forms of "street crime" to illegal forms of behaviour behind closed doors (e.g., corporate and financial crimes) and crimes with high symbolic political loading such as "terrorism".

With regard to the use of surveillance practices to combat and prevent different types of crime, there is evidence of a selective use of surveillance practices. As Coleman and McCahill[20] argue for the UK, surveillance measures are heavily used to control welfare fraud, while for corporate tax fraud, producing significantly higher economic and societal damage, surveillance is used to a much lesser extent.

As a general rule, street crimes lend themselves to massive surveillance that have a symbolically high loading in public discourse, while the overall damage caused by specific types of crimes does play a minor role. This explains why street crime and all types of behaviour that can trigger public anxiety are more heavily surveilled than other forms of crime. As Coleman and McCahill point out: "Surveillance, then, does not simply respond to 'crime' as such, but responds to socially constructed forms of public anxiety about particular social problems which may come to be defined as 'crime' without any necessary relationship to objective measurements relating to 'harms', 'costs', 'injuries' or 'damages'."[21] Looking at the differential use of surveillance practices to address (i.e., combat and prevent) different types of perceived criminal threats – from street crime to welfare fraud, corporate tax evasion and terrorism – it becomes obvious that surveillance is not a uniform and pervasive element in the area of law enforcement. Rather we see a selective use of surveillance technologies here. Taking the overall quantitative distribution of crimes as they are registered in official crime statistics, and taking into account the (economic) damage these different types of crimes – from vandalism through shoplifting, fraud, assault, terrorism and different types of white collar crime – create, it becomes obvious that surveillance is not targeted at the most damaging, dangerous or frequent crimes. Rather the use of surveillance practices seems to follow a different logic.

There are different interpretations for the spread of surveillance in the field of crime fight. On the one hand, an economic interpretation, looking at the emergence of a security-industrial complex[22] accounts for a number of developments. On the other hand, one might construe a kind of family resemblance between the logic of crime detection and policing and the logic of surveillance in a Foucauldian tradition. Both can be seen as cultural projects geared towards panoptical transparency, knowledge and control. Surveillance as practice goes well with

[19] Groombridge, Nic, "Crime Control or Crime Culture TV?", *Surveillance Studies*, Vol. 1, No. 1, 2002, pp. 30-46.
[20] Coleman, Roy, and Michael McCahill, *Surveillance and Crime*, Sage, London, 2011, p. 4 passim.
[21] Ibid., p. 5 passim. For similar developments in the US, see: Gordon, Diana R., *Justice Juggernaut: Fighting Street Crime, Controlling Citizens*, Rutgers University Press, New Brunswick, 1990.
[22] Kreissl, Reinhard, and Heinz Steinert, "Politik mit der Angst: Warum es keinen Widerstand dagegen gibt und was alltäglich aus ihr lernen", in Felix Herzog and Ulfried Neumann (eds.), *Festschrift für Wilfried Hassemer*, FS Hassemer, C.F. Müller, Heidelberg, 2010, S. 961-970. Hayes, Ben, *Arming Big Brother: The EU's Security Research Programme*, TNI, Amsterdam, 2006.

policing and crime detection, since it promises to provide instant and constant information about each individual in a population, based on a fixed set of universal categories.

Finally, when considering shifts in the general orientation of crime control and criminal justice, the spread of surveillance can be seen as an element in a new regime of actuarial justice[23] or flexible normalism.[24] What can be observed here is a reorientation from the focus on manifest norm-breaking behaviour to a focus on preventive risk assessment.[25] This shift of focus and the decoupling of norm and behaviour are paving the way for massive surveillance as the new gold standard of crime control. It nicely fits with a major societal trend that has been termed "dangerisation".[26] Others such as Niklas Luhmann[27] have accounted for this shift as a semantic recoding from danger to risk, where risk is a mode of perception of the social world that assesses choices to be made in the present from the perspective of future damages. Risk logic, dangerisation and actuarial justice can be seen as variation of a general theme that supports large-scale surveillance as a necessary strategy of crime control.

4.1.3 Crime, terrorism and surveillance

As pointed out above, surveillance resonates perfectly with certain socio-cultural sentiments and constitutes a profitable field of investment for private enterprises. But this does not imply that surveillance used in the fight against crime and terrorism lives up to the promises usually made by those who market technological solutions for surveillance practices. Very often new surveillance systems are introduced without any prior evaluation or assessment. System providers implement new technologies in local pilots without considering that changes in technology almost always imply an organisational change.[28] The problem is that law enforcement agencies operate in a strict legal context, defining duties, responsibilities and accountability of the agency. As opposed to private enterprises, organisational change is limited by these formal constraints. New surveillance technologies have to be integrated into the legal framework. At least three logics have to be integrated or considered here: the logic of law (giving citizens' rights to privacy and data protection, due process rights, etc.), the operational logic of the law enforcement organisations (as mediated by their organisational and occupational cultures) and the techno-logic of the surveillance system to be implemented. Frequently, rather than law determining the use of the technology, law is reactive and adapted post-hoc, and often legitimises current practice rather than shaping practice on the basis of a principled approach. Moreover, systems are particularly susceptible to function creep as the range of applications and use of surveillance technologies is gradually expanded.[29] Nor is the law often capable of regulating what could be called interaction or synergy effects, as different isolated technologies are integrated into a greater surveillance assemblage.

---

[23] Feeley, Malcom M., and Jonathan Simon, "The New Penology: Notes on the emerging strategy of corrections and its implications", *Criminology*, Vol. 30, Issue 4, November 1992, pp. 449-474.
[24] Link, Jürgen, and Mirko Hall, "From the 'Power of the Norm' to 'Flexible Normalism': Considerations after Foucault", *Cultural Critique*, No. 57, Spring 2004, pp. 14-32.
[25] Stenson, Kevin, and Robert R. Sullivan (eds.), *Crime, risk and justice: the politics of crime control in liberal democracies*, Willan Publishing, Cullompton, UK,2001.
[26] Lianos, Michaelis, and Mary Douglas, "Dangerization and the End of Deviance. The Institutional Environment", *British Journal of Criminology*, Vol. 40, No. 2, 2000, pp. 261-278.
[27] Luhmann, Niklas, *Soziologie des Risikos*, de Gruyter, Berlin, 2003.
[28] Tidd, Joe, John Bessant and Keith Pavitt, *Managing Innovation: Integrating Technological, Market and Organizational Change*, John Wiley & Sons, Chichester, 2005.
[29] Haggerty, Kevin D., and Richard V. Ericson (eds.), *The New Politics of Surveillance and Visibility*, University of Toronto Press, Toronto, 2006.

Obviously it is difficult to assess and evaluate new technologies in advance, before they are introduced as standard tools in the workings of law enforcement institutions. Assessments of the magnitude of threats or the structure of the problem to be addressed by surveillance are not always very well understood. Law enforcement agencies tend to operate with worst-case scenarios when they try to justify the introduction of new measures of control and surveillance or ask for extension of their legal powers. The key problem here is that other civil society actors are in a weak position when it comes to the assessment of the validity of the evidence presented by law enforcement agencies. These agencies have a privileged access to intelligence not available to others and so it is difficult to question the claims brought forward by the security agencies since counter expertise is not readily available. A further problem arises from the fact that threat scenarios as a basis for surveillance measures are projections of future events and the solutions suggested to counter these threats (i.e., increased surveillance) follow the logic of prevention. A strategy based on the idea on preventing security threats through surveillance has few natural limits on its expansion. This holds for mundane behaviours (such as driving under the influence of alcohol) and for serious and rare events (such as a major terrorist bomb attack) alike. In principle, surveillance can be expanded until the resources necessary are exhausted, since any criminal or terrorist act can be interpreted as the consequence of a number of preconditions or prior acts that can become the object of surveillance. Of course, legal constraints apply here, limiting the spread of surveillance, but the evidence suggests that these limits are flexible and extended over time in a process of what could be called "post-hoc legislation" where the law adapts to security needs and technology development instead of constraining the unlimited growth of surveillance.[30]

4.2 CONCEPTUAL ISSUES

Surveillance, as the scholars of Surveillance Studies point out, is a multifaceted phenomenon and not easily pinned down within a single conceptual framework. It can be approached from different theoretical angles.[31] Since here we are concerned with the use of surveillance to prevent and fight crime and terrorism, we focus on those instruments and technologies currently applied in the field of law enforcement. As David Lyon states, surveillance "always has some ambiguity".[32] This ambiguity arises from the interpretation of surveillance as being either for care or control, and rather than resenting surveillance, "Many seem content to be surveilled, for example by street cameras, and some appear so to relish being watched that they will put on a display for the overhead lenses, or disclose the most intimate details about themselves in blogs or on webcams."[33]

4.2.1 Surveillance

Before going any further on the efficacy of surveillance programs, some conceptual clarifications are necessary. Indeed, one of the main difficulties that arise about surveillance is that many concepts are often ill-defined and/or used as synonyms. Given the range of definitions and degrees of abstraction, confusion exists between key notions such as

[30] See, e.g., the discussion in Huster, Stefan, and Rudolph Karsten (eds.), *Vom Rechtsstaat zum Präventionsstaat*, Suhrkamp, Frankfurt/Main, 2008.
[31] Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2007.
[32] Ibid., p. 14.
[33] ibid.

instruments, tools, technologies, parameters and practices. While their precise meanings mostly remain underspecified in surveillance and security studies, this sub-section aims at offering some clarifications to facilitate a coherent and useful articulation of these concepts.

First, the growth of the modern, bureaucratic state and the implementation of "rational" methods are closely linked to the development of surveillance as a whole.[34] Regarding the association between surveillance and bureaucratic administration, Michel Foucault shows how governmental instruments have been used to both care for and control the population.[35] Instruments such as listings, mapping and taxation are implemented to "take measures, collect information or define behaviours on the basis of a reading of the relationship between the government and the governed".[36] According to this Foucauldian perspective, the notion of *instrument* can be defined as "a device that is both technical and social, that organizes specific social relations between the state and those it is addressed to, according to the representations and meaning it carries. It is a particular type of institution, a technical device with the generic purpose of carrying a concrete concept of the politics/society and sustained by a concept of relationship."[37]

Gilles Favarel-Garrigues et al.[38] attempt to couple this conceptualization of instrument with the notion of "dispositive" as broadly defined by Michel Foucault[39] as the particular assembly and relations between heterogeneous individual elements (objects and speech).[40] While a dispositive initially responds to an emergency and "therefore has an eminently strategic function",[41] it does not constitute a static arrangement to the extent that it tends to be reinvested by "a perpetual strategic elaboration".[42] Thus, in this perspective, Gilles Favarel-Garrigues et al. argue that "the instrument is a type of social institution that includes, on the one hand, a technical substrate (which objectifies a social fact and materializes it through the creation of synthetic artefacts) and, on the other hand, a cognitive dimension (which expresses a regulatory model within the framework of a power relationship, collecting information or guiding behaviour). Moreover, the instrument must have a generic vocation, meaning that it

[34] Lyon, David, Surveillance Studies: An Overview, Polity Press, Cambridge, 2007. Salter, Mark B., "Surveillance", in Peter J. Burgess (ed.), *The Routledge Handbook of New Security Studies*, Routledge, New York, 2010, pp. 187-196. Surveillance Studies Network, *A report on the surveillance society*, Information Commissioner's Office, Wilmslow, 2006.

[35] Foucault, Michel, *Naissance de la biopolitique : Cours au Collège de France. 1978-1979*, Hautes études, Gallimard, Seuil, Paris, 2004.

[36] Favarel-Garrigues, Gilles, Thierry Godefroy and Pierre Lascoumes, "Tools and securitization: the instrumentation of AML/CFT policies in French banks", in Karin Svedberg Helgesson and Ulrika Mörth (eds.), *Securitization, accountability and risk management*, PRIO, Routlege, Oslo, 2012, pp. 88-109, p.92.

[37] Lascoumes, Pierre and Patrick Legalès (eds.), Gouverner par les instruments, Presses de Sciences Po, Paris, 2005, p. 4. Lascoumes, Pierre, and Patrick Legalès, "Introduction: Understanding public policy through its instruments: From the nature of instruments to the sociology of public policy intrsumentation", *Governance*, No. 20, January 2007, pp. 1-22.

[38] Favarel-Garrigues, Gilles, Thierry Godefroy and Pierre Lascoumes, "Tools and securitization: the instrumentation of AML/CFT policies in French banks", in Karin Svedberg Helgesson, and Ulrika Mörth (eds.), *Securitization, accountability and risk management*, PRIO, Routlege, Oslo, 2012, pp. 88-109, p.92.

[39] Foucault, Michel, *Dits et écrits II. 1976-1988*, Gallimard, Paris, 2001.

[40] On the reasons for rendering the French term dispositif as dispositive rather than apparatus, see Bussolini, J., "What is a dispositive?", *Foucault Studies*, No. 10, 2010, pp. 85-107.

[41] Foucault, Michel, *Dits et écrits II. 1976-1988*, Gallimard, Paris, 2001. Bussolini, J., "What is a dispositive?", *Foucault Studies*, No. 10, 2010, pp. 85-107, p. 91. Agamben, Giorgio, *Qu'est-ce qu'un dispositif?*, Payot & Rivages, Paris, 2007.

[42] Favarel-Garrigues, Gilles, Thierry Godefroy and Pierre Lascoumes, "Tools and securitization: the instrumentation of AML/CFT policies in French banks", in Karin Svedberg Helgesson, and Ulrika Mörth (eds.), *Securitization, accountability and risk management*, PRIO, Routlege, Oslo, 2012, pp. 88-109, p.92.

must be applicable to very different situations."[43] Consequently, instruments such as listings, mapping and taxation are not programs to the extent that these instruments can be used for various purposes in different programs.[44] Listings, for example, can be used in the case of health programs or in the case of security-focused programs against "dirty money" and so on.[45] Moreover, social sorting[46] can be implemented by commercial companies in the case of consumer surveillance, to make profits[47] and social sorting can also be used for national security concerns regarding counter-terrorism programs.[48]

So it makes little sense to reconstruct surveillance from a law enforcement perspective, but rather one has to look at what kinds of instruments are available to be used by law enforcement agencies. The law-enforcement specific aspects or adaptations come into play when looking at the way a specific instrument is put to use through the application of tools.
The implementation of each instrument is based on one or several tools. In other words, at a micro-level, each instrument is operationalized by tool(s), such as one specific statistical classification (i.e. tool) for listing (i.e. instrument), one specific form of graphic representation (i.e. tool) for mapping (i.e. instrument) or one specific basis of calculation (i.e. tool) for taxation (instrument).[49] Finally, while each instrument is a particular combination of tools, each tool is based on specific parameters. "Thus, a statistical classification comprises pre-defined categories (age brackets, classification of professions and socio-professional categories); a mapped representation on a scale of definition;… the calculation of a tax on the basis of information bearing on the value of the relevant item (an estate, activity or economic transaction)."[50] With reference to contemporary surveillance, old instruments such as social sorting[51] are now highly computerised. That is, the classification and categorisation of populations are increasingly based on profiling and filtering software (i.e., tools). These data processing tools depend on parameters, which correspond to precise regulatory rules (thresholds and so on), "known patterns" or predetermined risk scenarios.[52]

---

[43] Ibid.
[44] Balzacq, T., "The policy tools of secuyritization: Information exchange, EU foreign and interior policies", *Journal of Common Market Studies*, Vol. 46, No. 1, January 2008, pp. 75-100.
[45] Amicelle, Anthony, and Gilles Favarel-Garrigues, "La lutte contre l'argent sale au prisme des libertés fondamentales: Quelles Mobilisations?", *Cultures & Conflits*, No. 76, 2009, pp. 39-66.
[46] Lyon, David (ed.), *Surveillance as social sorting: Privacy, risk and digital discrimination*, Routledge, London, 2003.
[47] Ball, Kirstie, Elizabeth Daniel, Sally Dibb and Maureen Meadows, "Democracy, surveillance and 'knowing what's good for you': the private sector origins of profiling and the birth of 'citizen relationship management'", in Kevin Haggerty and Minas Samatas (eds.), *Surveillance and Democracy*, Routledge, New York, 2010, pp. 111-126.
[48] Surveillance Studies Network, *A report on the surveillance society*, Information Commissioner's Office, Wilmslow, 2006.
[49] Woll, C., "Lectures: Gouverner par les instruments", *Pôle Sud*, No. 23, May 2005, pp. 200-202.
[50] Favarel-Garrigues, Gilles, Thierry Godefroy and Pierre Lascoumes, "Tools and securitization: the instrumentation of AML/CFT policies in French banks", in Karin Svedberg Helgesson, and Ulrika Mörth (eds.), *Securitization, accountability and risk management*, PRIO, Routlege, Oslo, 2012, pp. 88-109, p.92.
[51] Ball, Kirstie, Elizabeth Daniel, Sally Dibb and Maureen Meadows, "Democracy, surveillance and 'knowing what's good for you': the private sector origins of profiling and the birth of 'citizen relationship management'", in Kevin Haggerty and Minas Samatas (eds.), *Surveillance and Democracy*, Routledge, New York, 2010, pp. 111-126.
[52] Amicelle, Anthony, "Towards a 'new' political anatomy of financial surveillance", *Security Dialogue*, Vol. 42, No. 2, May 2011, pp. 161-178. Amicelle, Anthony, "The Great (Data) Bank Robbery: The Terrorist Finance Tracking Program & the SWIFT Affair", *Research Questions*, CERI, No. 36, May 2011, pp. 1-27. Amicelle, Anthony and Gilles Favarel-Garrigues, "Financial surveillance: Who cares?", *The Journal of Cultural Economy*, Vol. 5, No. 1, January 2012, pp. 105-124. De Goede, Marieke, "Risk, Preemption and exception in the war on terrorist financing", in Louise Amoore and Marieke De Goede (eds.), *Risk and the War on Terror*, Routledge, London, 2008, pp. 97-112.

Regarding security-focused programs with surveillance capabilities, the notions of "tool" and "technology" are commonly used as synonyms, at least implicitly. Indeed, at first glance, technologies (profiling software and so on) can be presented as inert and manufactured tools.[53] Hence, there is still a widespread belief today on the effectiveness of these tools to improve security.[54] Technologies – especially "new" technologies – often get promoted in political and some academic circles as *the* solution to facilitate the work of law enforcement and intelligence services to counter a specific set of threats in order to make citizens' lives safer.[55] Surveillance technologies constitute a strong priority for European industrial as well as research policies[56] and various sophisticated tools are proposed "on a rapidly evolving basis",[57] from new cameras to biometrics. While these technological fixes need further critical analysis, our understanding of technologies as material tools should also be discussed.

Growing academic contributions suggest going beyond material characteristics and understandings of technology as a neutral factor of implementation or a dependent variable that would determine outcome.[58] They insist on the necessity to also conceive technology as specific ways of knowing and doing, i.e., as practices[59] that can be conceived as "a routinized type of behaviour which consists of several elements, interconnected to one another: forms of bodily activities, 'things' and their use, a background knowledge in the form of understanding and know-how, states of emotion and motivational knowledge".[60] The understanding of technology as a set of social practices means that tools are socially fashioned and that the designing of specific technological tools "as well as their uses should be studied in relation to a political and social context".[61]

---

[53] Guittet, E.-P. and J. Jeandesboz, "Security technologies", in Peter J. Burgess (ed.), *The Routledge Handbook of New Security Studies*, Routledge, New York, 2010, pp. 229-239.

[54] Levi, Michael and David Wall, "Technologies, Security, and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society*, Vol. 31, No. 2, May 2004, pp. 194-220. Bellanova, Rocco, and Michael Friedewald (eds.), Deliverable 1.1: Smart Surveillance – State of the Art, FP7 SAPIENT Project, Brussels, 2011. http://www.sapientproject.eu/

[55] Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi, *Security technologies and society: A state of the art on security, technology, borders and mobility*, IN:EX, PRIO, Oslo, 2008. Ceyhan, A., "Enjeux d'identification et de surveillance à l'heure de la biométrie", *Cultures & Conflits*, No. 64, Winter 2006, pp. 33-47. Surveillance Studies Network, *A report on the surveillance society*, Information Commissioner's Office, Wilmslow, 2006.

[56] Preuss-Laussinotte, S., "L'Union européenne et les technologies de sécurité", *Cultures & Conflits*, No. 64, Winter 2006, pp. 97-108.

[57] Kroener, I., and D. Neyland, "New Technologies, security and surveillance", in Kirstie Ball, Kevin Haggerty and David Lyon (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, New York, 2012, pp. 141-148 [p. 141].

[58] Amoore, Louise, and Marieke De Goede, "Governance, risk and dataveillance in the war on terror", *Crime, Law & Social Change*, Vol. 43, No. 2, May 2005, pp. 149-173. Bellanova, Rocco, and Denis Duez, "A different view on the 'making' of European security: The EU Passenger Name Record System as a socio-technical assemblage", *European Foreign Affairs Review*, No. 17, 2012, pp. 109-124. Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi, *Security technologies and society: A state of the art on security, technology, borders and mobility*, IN:EX, PRIO, Oslo, 2008. Guittet, E.-P., and J. Jeandesboz, "Security technologies", in Peter J. Burgess (ed.), *The Routledge Handbook of New Security Studies*, Routledge, New York, 2010, pp. 229-239. Huysmans, Jef, The politics of insecurity: fear, migration and asylum in the EU, Routledge, London, 2006. Salter, Mark B., "Passports, Mobility, and Security: How smart can the border be?", *International Studies Perspective*, Vol. 5, No. 1, January 2004, pp. 71-91.

[59] Franklin, Ursula, *The real world of technology*, House of Anansi Press, Toronto, 1999.

[60] Reckwitz, A. "Toward a theory of social practices: A development in culturalist theorizing", *European Journal of Social Theory*, Vol. 5, No. 2, May 2002, pp. 243-263, p.249.

[61] Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi, Security technologies and society: *A state of the art on security, technology, borders and mobility*, IN:EX, PRIO, Oslo, 2008, p. 5. MacKenzie, Donald, and Judy Wajcman, "Introductory essay: the social shaping of technology", in Donald MacKenzie and

"In this sense, technologies are always involved in a range of what we might term social, political, and technical relations which contribute to any experience of that technology. It is only through an understanding of these relations that we can generate a detailed sense of the nature of a technology, its history and so on."[62] "Security technologies are more than the sum of manufactured objects devoted to protection, safety and surveillance: they combine ways of designing, undertaking and practicing security, and are both the support and the explanation of a certain doxa on security."[63] Consequently, the role, actions and transformative effect of security-focused technologies with surveillance capabilities have to be highlighted and closely studied to fully understand surveillance programs that increasingly rely on these sophisticated technologies.

As elaborated above a comprehensive understanding of surveillance requires a multidimensional approach, looking at instruments, tools and parameters and above all the analysis of surveillance practices has to consider the social embedded-ness of technologies (or tools). Surveillance as a techno-social practice in a sense creates or reconstructs the objects and subjects under surveillance since it establishes power relations linking and sorting individuals in a specific way. Since the question "Who are you?" can only be answered in a given social and cultural context, defining social relations, the emergence of surveillance can be reconstructed only when looking at the changes in these contexts.

4.2.2 Modern surveillance as naming and tracking

Modernity is about mobility.[64] In stable, village-type communities, no one ever raises the question of who is who with the exception of the stranger who enters from an unknown outside space. Deviant behaviour and deviant individuals are easily spotted and identified under these circumstances. Surveillance can be regarded as a practice to identify /name and locatetrack individuals and their movements when they are no longer tied to a narrow social and geographical space. Hence identifying/naming and locating/tracking are two of the main tasks for which surveillance practices are used.

Identify and name

In the context of the massive social and economic changes unleashed by the industrial revolution, the urban population was increasingly mobile, transitory and anonymous. The ability to identify those on the street based on a police officer's knowledge of a stable community was increasingly undermined. Moreover, 19th century social administrators were particularly concerned to differentiate the petty criminal from the habitual criminal, and this required a means of linking a person with their criminal history. Historically, this had been done by branding. A mark was burnt on to the skin with a red hot iron; as Thomas notes, in England, the letter "V" for vagabond, "T" for thief and even "M" for manslaughter ensured

---

Judy Wacjman (eds.), *The Social Shaping of Technology: How the refrigerator got its hum*, Open University Press, Milton Keynes, 1985, pp. 2-25.

[62] Kroener, I., and D. Neyland, "New Technologies, security and surveillance", in Kirstie Ball, Kevin Haggerty and David Lyon (eds.), Routledge *Handbook of Surveillance Studies*, Routledge, New York, 2012, pp. 141-148, p.145.

[63] Guittet, E.-P., and J. Jeandesboz, "Security technologies" in Peter J. Burgess (ed.), *The Routledge Handbook of New Security Studies*, Routledge, New York, 2010, pp. 229-239 [p. 238].

[64] Urry, John, Mobilities, *Polity Press*, Oxford, 2007.

due retribution for the second time offender.[65] With the demise of branding by the end of the 18th century, bureaucratic means for the identification of the habitual criminal were developed at the local level and by the latter part of the 19th century, police authorities in Paris and London sought to establish centralised registers of all convicted criminals.

However, a system that was based on matching records by name was soon found to be inadequate. In an age where many people could not read or write, when the spelling of a name was subject to phonetic interpretation and the more experienced criminal could falsify their name, the register was inherently unreliable for the purposes of identification. So much so that in the words of one contemporary commentator, "registration is of no use, and might as well be got rid of at once".[66]

Thus, even as late as the 1890s, one of the primary means of identifying the habitual criminal was still based on the face-to-face knowledge of a police officer and in London recently arrested prisoners were paraded, three times a week in front of detectives so they might be identified. In Paris, the same problem was exercising Alphonse Bertillon: how to devise a system that was not dependent on a person's name or a police officer's memory? As Sekula notes:

> Bertillon sought to break the professionals criminal's mastery of disguises, false identities, multiple biographies, and alibis. He did this by yoking anthropometrics, the optical precision of the camera, and refined physiognomic vocabulary, and statistics.[67]

Although the French records contained a photograph, the task of trying to match an individual photograph with the tens of thousands of records held in the files was formidable and could take weeks. Bertillon solved this problem by utilising a series of anthropometric measurements which, when combined, would allow the calculation of an individual reference point based on bodily dimensions. This number would be used to position the record in the system nearest to those who shared similar physical dimensions. To determine if a person already had an entry in the archive, the identification number on their new record could be checked against a small subset of existing entries, and a final comparison made between the photographs.[68]

At last, there was an efficient means of linking an individual to their record, which could now be used to differentiate the habitual from the petty criminal and, by 1893, about a dozen countries around the world had introduced the system. However, the system was not without its problems, the maturation of the criminal population, problems of obtaining accurate measurement and the rapid growth of the number of files, all undermined the efficiency of the system.

The pioneering work of Francis Galton, among others, demonstrated that each individual carries with them an almost unique and unchanging token of identity, and one that could be easily recorded – the fingerprint. By devising a simple system of classification, he made it amenable to systematic description and comparison. By 1901, in England, the fingerprint had replaced the Bertillon system of measurement and rapidly became adopted across the world as the primary means for the police to establish a suspect's identity.

---

[65] Thomas, Terry, *Criminal Records: A Database for the Criminal Justice System and Beyond*, Palgrave Macmillan, Basingstoke, 2007, p. 5.
[66] Hastings, G.W., *Address on the Repression of Crime*, Spottiswoode and Co., London, 1875, p. 13.
[67] Sekula, A. "The Body and the Archive", October (39) Winter: 3-64. 1986, p. 27.
[68] Ibid, p. 25-34.

The development of the criminal record, with the fingerprint as the unique marker of identity, allowing it to be linked with certainty to a named individual, provided the cornerstone of modern law enforcement. A person could now be linked with his history and his current self could no longer escape the impact of the official categorisation of the actions of his past selves; identity had been established.

Locating and tracking

As Lyon et al. point out: "Where you are, does matter".[69] So locating an individual or object in space-time is an important task of surveillance practices. As Bennett and Regan observe: "Surveillance is a means of determining who is where and what they are doing, either in the physical or virtual world, at a particular point in time. This is the basic purpose of surveillance and the most common goal of surveillance systems. These systems help answer the question of who is where, at what point in time, and what are they doing. The tracking of movements for such basic information is a fundamental component of the surveillance systems."[70]

Attempts to track and locate the movements of individuals and objects represent a key and ancient feature of surveillance that goes well beyond the fight against criminal and political violence. "There is nothing new, nor necessarily anything sinister, about wanting to know where others are at any given time. Parents may want to be sure their children are safe in the big city, trucking companies may wish to ensure that their drivers are taking breaks of sufficient length and emergency services may be able to do a better job if they can find accident victims whether or not they can speak clearly into a cellphone. New technologies make all these things possible, automatically, remotely and in real-time."[71] According to Olivier Razac[72], the wish to locate and to be located is partly related to the desire for security that is not only limited to the shift towards a "safety state".[73] Thus, the expectation to always know where we are and where our relatives are is increasingly normalised, especially with technologies such as mobile phones. Furthermore, the wish to locate and to be located can constitute a desire for efficiency[74] to the extent that entrepreneurs want to know in real-time where their products are and where they are going to manage their business. "Real-time visibility into exact locations of containers and cargo has never been as important as today with increased movement of cargo from offshore, the need to move it quickly to final destinations and new security requirements."[75] From a commercial perspective, mechanisms of tracking or tracing movements of consumers can also be implemented for marketing purposes.[76] Consequently, information such as where are/were you and when is increasingly considered as a valuable commodity for multiple uses.

Those desires of security, efficiency and profitability have led to a new impetus to tracking practices with the contemporary quest for location technologies. David Lyon et al. define

---

[69] Lyon, David, Stephen Marmura and Pasha Peroff, "Location Technologies: Mobility, surveillance and privacy", A report to the Office of the Privacy Commissioner of Canada, 2005, p. 5.
[70] Bennett & Regan 2004, p. 252.
[71] Lyon, David, Stephen Marmura, and Pasha Peroff, "Location Technologies: Mobility, surveillance and privacy", A report to the Office of the Privacy Commissioner of Canada, 2005, p. 5.
[72] Razac, Olivier, *Avec Foucault, après Foucault. Disséquer la société de contrôle*, L'Harmattan, Paris, 2008.
[73] Raab, Charles, "Governing the safety state", Inaugural Lecture at the University of Edinburgh, 7 June 2005.
[74] Razac, Olivier, *Avec Foucault, après Foucault. Disséquer la société de contrôle*, L'Harmattan, Paris, 2008.
[75] See the website of the Association for Automatic Identification and Mobility (AIM): https://aimglobal.site-ym.com/
[76] Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2007.

location technology as "an application that can provide continuous, real-time and accurate location information about an individual or item".[77] Hence, global positioning system (GPS) satellites represent one example of a location technology that can (1) pinpoint locations, (2) do so continuously and (3) do so in real time.[78] Although they do not meet these three criteria, other technologies such as RFID (radio frequency identification), CCTV (closed-circuit television) or credit card technologies can also be used for tracking individuals.[79] Indeed, the location of a person can be inferred from RFID tags, video images and financial transactions.[80]

"The shift of surveillance from fixed locations and 'enclosures' to mobile contexts is clearly a feature of the present."[81] The trend of mobile surveillance is associated with technological developments that would enhance surveillance by leaving "electronic traces"[82] in order to follow movements of people and goods in and out of specific spaces. According to official discourses,[83] traceability both contributes to ensuring systemic fluidity of mobility while knowing what happens and what/who is moving/crossing, to ultimately detecting unwanted movements. Regarding the location of goods, Didier Torny defines a "traceability instrument" as a set of tools that aims at ensuring in real-time the relocation of manufactured objects without obstructing the principle of their circulation.[84] The implementation of traceability consists of systematising the logic of the mark, which intends to attach to one moving item the trace of places, individuals and transformations that have been linked to this item.[85] Hence, this management of flows would tend to monitor without a priori interfering with the principle of "free movement". What becomes fixed is not the surveillance and control but the mark on mobile items, which registers their trajectory.

"What is important is not to stop mobility, to block it, but to manage the flow at the best pace.… The key word has been to 'trace' the movement, to analyze it and to anticipate its next trajectory (money, capital and human beings).… Then, surveillance, control and mobility are not antithetic elements, they are reunified as 'mobility controls', as 'management of flow'".[86] The intensification of surveillance operations has not introduced a back-to-borders strategy in the aftermath of 9/11 to the extent that "global circulation" mostly remains a referent object that is protected as a "quasi-transcendental" for liberal life.[87] This hypothesis is especially strong with reference to financial flows. "The world is a deliberately open and porous one, designed to encourage the free flow of capital, investment and economic

[77] Ibid, p. 14.
[78] Ibid.
[79] Levi, Michael, "Combating the Financing of Terrorism. A history and Assessment of the Control of 'Threat Finance'", *British Journal of Criminology*, Vol. 50, No. 4, Winter 2010, pp. 650-669.
Lyon, David, "Why where you are matters: Mundane Mobilities, Transparent Technologies and Digital Discrimination", in Torin Monahan (ed.), *Surveillance and security: Technological power and politics in everyday life*, Routledge, New York, 2006, pp. 209-224. Norris, Clive and Gary Armstrong, *The Maximum Surveillance Society: The Rise of CCTV*, Berg, Oxford, 1999.
[80] Bellanova, Rocco, and Michael Friedewald (eds.), Deliverable 1.1: Smart Surveillance – State of the Art, FP7 SAPIENT Project, Brussels, 2011. http://www.sapientproject.eu/
[81] Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2007, p.89.
[82] Levi, Michael, and David Wall, "Technologies, Security, and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society*, Vol. 31, No. 2, May 2004, pp. 194-220.
[83] Razac, Olivier, *Histoire politique du barbelé*, Editions Flammarion, Paris, 2009.
[84] Torny, D., "La traçabilité comme technique de gouvernement des hommes et des choses", *Politix*, No. 44, May 1998, pp. 51-75.
[85] Cochoy, F., "Les effets d'un trop-plein de traçabilité", *La Recherche*, No. 339, 2001, pp. 66-68.
[86] Bigo, Didier, Unpublished paper, 2007, p. 4.
[87] Lobo-Guerrero, L., "'Pirates', stewards, and the securitization of global circulation", *International Political Sociology*, Vol. 2, No. 3, September 2008, pp. 219-235.

development. To elect rules that intrude on that dynamic is to hand victory to the enemy."[88] Thus, the first European strategy against terrorist financing promotes programs "for improving traceability and transparency with respect to the movement of funds."[89] The preparatory Commission report on this strategy states that "real time data exchange between law enforcement/intelligence services and the private sector generally (financial transactions but also purchase of airline tickets, car hire) can play an essential role in both preventive and repressive law enforcement activity in the fight against terrorism and its financing. This could allow real time tracking of financial transactions".[90]

From this perspective, the Terrorist Finance Tracking Program (TFTP) exemplifies one of the forms taken by intelligence through databases and surveillance models based on the tracing of flows.[91] According to this form of surveillance understanding, security can only be promoted if the traces led by financial flows are followed. Contemporary financial intelligence is precisely associated to the willingness to take advantage of information technologies in order to identify, monitor and so manage flows. Hence, practices of control and surveillance feed on financial circulation rather than attempting to curtail it. Control and surveillance at a distance suppose mobility without which they would lose their critical enabler. Thus, the Terrorist Finance Tracking Program turns out to be one of the crucial pieces of an "assemblage" of mobility control. This surveillance program gets promoted to identify as well as to locate terrorist suspects and to monitor their relationships. Officials from the US administration and the European Union justify the TFTP by alleging that it enables the location of suspects and the finding of addresses or links between known and unknown terrorists.[92] Consequently, the TFTP deploys mobile forms of surveillance that can be conceptualised as a kind of location technology – tracking financial and physical movements of suspects – which would allow for "social network analyses"[93] to map individual connections. "Following the money" is one of the most valuable sources of information that we have to identify and locate the networks of terrorists and their supporters.[94] However, these tracking practices do not avoid tensions as

[88] Aufhauser, D., "Terrorist financing: foxes run to ground", *Journal of Money Laundering Control*, Vol. 6, No. 4, 2003, pp. 301-305 [p. 301]. David Aufhauser was the chairman of the US National Security Council's policy co-ordinating committee on terrorist financing.

[89] European Union, "Strategy on terrorist financing", Brussels, 2004a.

[90] European Union, "The prevention of and the fight against terrorist financing through measures to improve the exchange of information, to strengthen transparency and enhance the traceability of financial transactions", Brussels, 2004.

[91] Amicelle, Anthony, "The Great (Data) Bank Robbery: The Terrorist Finance Tracking Program & the SWIFT Affair", *Research Questions*, CERI, No. 36, May 2011a, pp. 1-27. Gonzalez Fuster, Gloria, Paul De Hert and Serge Gutwirth, "SWIFT and the vulnerability of transatlantic data transfers", *International Review of Law Computers & Technology*, Vol. 22, No. 1-2, May 2008, pp. 191-202. Kierkegaard, S., "US War on Terror SWIFT(ly) signs blank cheque on EU data", *Computer Law & Security Review*, Vol. 27, No. 5, June 2011, pp. 451-454.

[92] Bruguière, Jean-Louis, Second report on the processing of EU-originating personal data by the United-States Treasury Departement for Counter Terrorism purposes: Terrorist Finance Tracking Program, Brussels, 2010. US Treasury Department Office of Public Affairs, Testimony of Stuart Levey, Under Secretary, Terrorism and Financial Intelligence, US Department of the Treasury, Before the House Financial Services Subcommittee on Oversight and Investigations, Washington, 11 July 2006. US Treasury Department, Terrorist Finance Tracking Program – Factsheet. 23 June 2006. http://ebookbrowse.com/tftp-fact-sheet-revised-2-15-11-2-pdf-d328699617

[93] De Goede, Marieke, "Risk, Preemption and exception in the war on terrorist financing", in Louise Amoore and Marieke De Goede (eds.), *Risk and the War on Terror*, Routledge, London, 2008, pp. 97-112.

[94] US Treasury Department Office of Public Affairs, Testimony of Stuart Levey, Under Secretary, Terrorism and Financial Intelligence, US Department of the Treasury, Before the House Financial Services Subcommittee on Oversight and Investigations, Washington, 11 July 2006.
US Treasury Department, Terrorist Finance Tracking Program – Factsheet. 23 June 2006.
http://ebookbrowse.com/tftp-fact-sheet-revised-2-15-11-2-pdf-d328699617

well as criticisms regarding civil liberties, privacy issues, economic sovereignty and doubts on their efficacy.[95]

Contemporary programs against crime and terrorism such as financial surveillance and the Terrorist Finance Tracking Program aim at tracing the flows. The TFTP aims at locating suspects and visualising their relationships in following money in its context of movement without infringing on the principle of free movement of capital. Hence, this program does not corroborate the idea of any mobility or security dilemma whatsoever. Mobility precisely tends to be the crucial element through which practices of control and surveillance can be widely deployed. As a result, intelligence is enabled by technologies extracting information and monitoring electronic traces with the stated aim of prevention. This widespread belief on the use of tracking technologies to prevent crime and terrorism deserves further discussion.

4.2.3 Law enforcement and surveillance

Taking a social theory's perspective, law enforcement and surveillance practices are mutually reinforcing processes. As pointed out above, policing and surveillance can be "seen as cultural projects geared towards panoptical transparency, knowledge and control. Surveillance as practice goes well with policing and detection and prevention, since it promises to provide instant and constant information about each individual in a population, based on a fixed set of universal categories." As we tried to demonstrate, the co-evolution of policing and surveillance changes the perception of what is considered as criminal in a broader sense. Surveillance increases the database for law enforcement bringing not only norm-breaking behaviour into the focus of police. This leads to an uncoupling of crime and norm breaking, creating categories like the "pre-delinquent". Based on the analysis of massive amounts of data from different sources of surveillance, the abstract type of the pre-delinquent (or pre-delinquent behaviour) can be construed as a new category, traditionally beyond the reach (and the interest) of law enforcement. Analytically, the important point here is the gradual uncoupling of norm and behaviour through increased surveillance and the effects this has on the overall rationale of policing. While policing used to focus on events where reasonable evidence suggested that some sort of norm-breaking behaviour occurred, the new surveillance based on intelligence-led style of policing, a term introduced by the US Bureau of Justice Assistance after 9/11, signals a reorientation of policing and law enforcement practices. While at the surface, this new approach was justified with the need for closer co-operation between different branches of the law enforcement community to address the problems of terrorism, it signifies a fundamental shift in the strategy of policing:

> Intelligence-led policing is a collaborative enterprise based on improved intelligence operations, and community-oriented policing and problem solving, which the field has considered beneficial for many years. To implement intelligence-led policing, police organizations need to reevaluate their current policies and protocols. Intelligence must be incorporated into the planning process to reflect community problems and issues. Information sharing must become a policy, not an informal practice. Most important, intelligence must be contingent on quality analysis of data. The development of analytical techniques, training, and technical assistance needs to be supported.[96]

It is no longer the business of thief-taking that defines everyday police operation, but rather the pre-emptive identification of potential perpetrators and wrong-doers, based on massive

[95] Amicelle, Anthony, and Gilles Favarel-Garrigues, "La lutte contre l'argent sale au prisme des libertés fondamentales: Quelles Mobilisations?", *Cultures & Conflits*, No. 76, 2009, pp. 39-66.
[96] Bureau of Justice Assistance, *Intelligence-Led Policing: The New Intelligence Architecture*, US Department of Justice, Washington, D.C., 2005: VII. https://www.ncjrs.gov/pdffiles1/bja/210681.pdf

intelligence and data analysis gathered from large-scale surveillance operations. This again has massive consequences for the presumption of innocence, since this approach of intelligence-led policing widens the gaze of law enforcement beyond law breaking. What for the everyday citizen may appear to be normal behaviour can attract the attention of law enforcement under an intelligence-led strategy of policing as deviating from an abstractly defined standard of "normal" action. Policing normalcy is thus a complementary dimension of law enforcement activity made possible by the growth of surveillance. We will return to this problem later. First, we will describe a number of surveillance technologies used in detecting and preventing crime and terrorism.

4.3 SURVEILLANCE TECHNOLOGIES USED IN PREVENTING AND DETECTING CRIME AND TERRORISM

Looking at the different surveillance instruments, technologies and tools applied in the fields of the fight against crime and terrorism, different trajectories and dynamics can be observed. Fingerprinting has been around for quite some time and the relevant changes in the efficacy are due to improvements in the technology of data processing. Others such as CCTV are still lagging behind: reliable automated processing of huge data sets is in its infancy. While producing large amounts of data, the analysis of these data, the identification of relevant information and the matching with predefined stored profiles has not yet reached the level of perfection as in the field of fingerprinting. Also, the debate about the effectiveness and legitimacy of different technologies displays a wide array of dynamics. Whereas fingerprinting is accepted, CCTV and DNA are contested

In order to assess operational effectiveness, it is necessary to place the different technologies in context. We need to understand how they are integrated (or not) into the different working routines, administrative and legal frameworks of law enforcement work and how they perform in real-world settings as opposed to laboratory tests. Effectiveness not only involves effects on police work, but also indirect effects such as deterrence. The deterrent effects of a technology are not directly linked to effectiveness in a strict technical sense. Deterrence is based on beliefs held by citizens in general or potential perpetrators.

What makes surveillance technologies potentially more powerful in principle is the combination and integration of different systems (sensors, DNA, CCTV) into a comprehensive surveillance assemblage. An important difference is between those technologies that work at a distance and others that require physical contact (e.g., fingerprinting or drug testing). Advances in technology have created a third, hybrid version: devices requiring a physical contact but are read off from a distance (e.g., bracelets for remote alcohol testing).

Not all surveillance technologies applied for prevention and the fight against crime and terrorism have been explicitly developed for law enforcement purposes (e.g., ANPR was originally used for traffic control and road toll collection), but were adapted by police and other agencies.

The following presentation is selective and focuses on the most relevant surveillance technologies to give an overview over the efficacy of surveillance in the fight against crime and terrorism.

4.3.1 Fingerprinting

Contrary to the popular image of fingerprinting as a tool for forensic investigation, fingerprint identification was developed originally for purposes of administration and criminal record-keeping, rather than forensics. However, bloody or "latent" fingerprints – invisible finger impressions made visible by dusting with powder – had been used to investigate crimes as early as 1892 in Argentina, 1897 in India, 1903 in Britain and, although forgotten to history, in the late 1850s in Albany, New York.[97] Nevertheless, it was only after the First World War that fingerprints became the preferred method of identification and criminal record-keeping. However, manual searching was slow and cumbersome: especially as file sizes increased. It is only with computerised fingerprint identification that routine searching of unidentified latent prints and instantaneous national searching has become feasible. Data-processing technology was used to sort fingerprint cards as early as the 1940s and research into computer fingerprint imaging began in the 1960s. During the 1970s, the FBI developed an automated search and retrieval system but it was not until the mid-1980s that Automated Fingerprint Identification Systems (AFIS) were mature enough for local law enforcement agencies to begin investing in them. AFIS record prints use an optical scanner and store them as digital images.[98] Together with DNA samples, fingerprints have become the major source of forensic bio-information.

The technique of fingerprinting is known as dactyloscopy**.** Until the advent of digital scanning technologies, fingerprinting was done using ink and a card. Today, digital scanners capture an image of the fingerprint on an optical or silicon reader surface. The reader converts the information from the scan into digital data patterns. The computer then maps points on the fingerprints and uses those points to search for similar patterns in the database.

The UK has used fingerprints for identification and prosecution in judicial cases with automated data since 1987 and digital fingerprint scanners are now commonplace in police custody areas. Mobile scanners are being rolled out across the country for use at the roadside and are combined with drug testing technology to create simultaneous testing for fingerprints and substance use (Intelligent Fingerprinting[99]). Fingerprints can be checked with the UK Border Agency database and exchanged with EU Member States – and third countries – with ongoing developments to improve the quality, quantity and pace of transfer of data.[100] IDENT1 is used to compare fingerprints at crime scenes with fingerprints held in the National Fingerprint Collection and automated searching is supplemented by expert evaluation and decision-making. The national data for England and Wales in 2009 reflects the extent of use of fingerprint samples and are used to anticipate the expected use of DNA samples: "From April to October 2009, IDENT1 made 47,783 crime scene 'identifications', averaging 85,000 identifications a year. In addition, it verifies the identity of over 1.5 million arrestees per year. There are no data on the number of identifications that led to detections or convictions. Presently, there are 2000 identity checks being processed via mobile devices per month, and the UK Borders Agency uses IDENT1 to check over 4000 identities per week. However, no

[97] Although in early cases some trial judges and juries expressed scepticism about warranting a criminal conviction on the basis of a single fingerprint match, fingerprint experts testified that the latent print and the suspect's inked print were "identical", constituting a "fact" that they came from the same source finger, to the exclusion of all other fingerprints. Cole, S.A., *Suspect Identities: A History of Fingerprinting and Criminal Identification*, Harvard University Press, Cambridge, MA, 2002.
[98] Ibid.
[99] Intelligent Fingerprinting http://www.intelligentfingerprinting.com/applications.html
[100] McCartney, Carol, Robin Williams and Tim Wilson, *The Future of Forensic Bioinformation*, Nuffield Foundation, London, 2010.

data are centrally provided from IDENT1 on the uses made of these identifications to support the detection or prosecution of offenders."[101]

The US Integrated Automated Fingerprint Identification System holds all fingerprint sets collected in the country, and is managed by the FBI. Many states also have their own AFIS. AFISes have capabilities such as latent searching, electronic image storage, and electronic exchange of fingerprints and responses. Many other states, including Canada, the European Union, Israel, Pakistan, Argentina, Turkey, Morocco, Italy, Chile, Venezuela, Australia, Denmark, the International Criminal Police Organization, and various states, provinces and local administrative regions have their own systems, which are used for a variety of purposes, including criminal identification, applicant background checks, receipt of benefits and receipt of credentials such as passports.

Courts have accepted claims that no two fingerprints were identical and that such testimony was fundamentally scientific and reliable. This judicial acceptance offered fingerprint evidence its wider approbation and acceptance. Cole highlights that there is a significant lack of consensus between fingerprint identifiers and systems. "We may, therefore, conclude (1) that there is no clearly articulated standard for what constitutes a fingerprint match, and (2) the standard, whatever it is, is not uniform, across the United States, nor around the world. There is substantial disagreement between examiners and jurisdictions over what constitutes a fingerprint match."[102]

Despite high profile cases highlighting the dangers associated with fingerprint evidence within the criminal justice system, there is little doubt of the overall consensus as to the value of the technology as a part of the evidence base in criminal trials.[103] However, there is a clear basis for arguing against the historical view of fingerprint evidence as highly reliable – or even infallible – with the ability to establish identical matches. The legal guidance established in cases that have successfully challenged this view of "infallibility" is sound and measured: fingerprint evidence constitutes opinion and not fact. It should be weighed up by the jury alongside all the other evidence presented within a trial – and never relied upon as proof of an accused person's presence at a scene or action in a case – upon which to reach a verdict of guilt. However, reports indicate that experts continue to act outside that guidance.

---

[101] Ibid, p. 26.

[102] Cole, S.A., "The 'Opinionization' of Fingerprint Evidence", *BioSocieties* 3, 2008, pp. 105-113. USA v. Eric Robert Rudolph, CR 00-S-0422-S, 2005.
http://www.alnd.uscourts.gov/rudolph/PleaAgreement.pdf. The question of the validity of fingerprint evidence has become an important legal question. In a landmark USA case, the Supreme Court mandated that "proposed testimony must be supported by appropriate validation" (Daubert v Merrell Dow Pharmaceuticals 1993 p. 590). The Daubert ruling also required federal judges to ensure the reliability of evidence put to juries. It appears that this questioning approach has reaped results: as illustrated in the case of United States v Crisp (2003) in which Judge Michael dissented: "The government did not offer any record of testing on the reliability of fingerprint identification. . . . Indeed it appears that there has not been sufficient critical testing to determine the scientific validity of the technique. . . . The government did not introduce studies or testing that would show that fingerprint identification is based on reliable principles or methods." United States v Crisp 2003 p. 273–74. USA v. Patrick Leroy Crisp, No. 01-4953, 2003. http://bulk.resource.org/courts.gov/c/F3/324/324.F3d.261.01-4953.html

[103] Roth., Nelson E., "The New York State Police Evidence Tampering Investigation", Confidential Report to the Governor of New York, Ithaca, New York, 1997. Cole, S.A., "More than Zero: Accounting For Error In Latent Fingerprint Identification", *The Journal of Criminal Law and Criminology*, Vol. 95, No. 3., 2005. *The Guardian*, "Fingerprint evidence 'based on opinion rather than facts'", 14 Dec. 2011.
http://www.guardian.co.uk/uk/2011/dec/14/fingerprint-evidence-opinion-fact

> Public trust is an essential precondition for the effective use of forensic bioinformation. The government need trust to enable 'consensus' legislation. The police need trust in order to utilise the technologies and only trust can allay suspicions of 'Big Brother' futures. With trust in the institutions responsible for collecting, using, and governing forensic bio-information, individuals and communities can gain the benefits of these technologies yet still know that respect for human rights and the democratic process remain unchallenged. These are not simply matters of technology and science.[104]

4.3.2 CCTV

The use and expansion of CCTV in public spaces has only grown significantly – although varyingly across the globe – over the past 20 years. Despite having a public TV service in 1936, the UK only first used CCTV to assist with one-man operation of traffic lights in 1956. Even after this, its extension was limited: applied occasionally to crowd monitoring and used more widely across the retail sector. Following the IRA assassination attempt against the UK's Tory Government, large-scale use of CCTV was deployed in Bournemouth for the party's annual conference in 1985. Nevertheless, this did not signify a sea-change approach and in 1991 there were still only 10 cities operating open-street CCTV in the UK.[105] It was the Bulger child murder in 1993 that created widespread public and political reaction, with the CCTV image of Jamie Bulger achieving iconic status in the media. The Government initially announced £2 million in central funds for CCTV schemes across the country and when the response was high, this was raised to £5 million. By 1998, this had reached £31 million with 580 schemes and was continued by the new, Labour Government.

Despite an overall growth, the expansion of CCTV schemes across Europe has not been uniform. The 2004 URBANEYE project studied six EU capitals and concluded that although CCTV was common in public spaces – such as banks, shops, restaurants and transport terminals – the prevalence differed between states. Similarly, the organisational arrangements differed and this was important: as the system depends upon the people viewing and responding to CCTV images for its crime control function.[106] Overall, in Europe, 29% of public spaces were covered by CCTV, with 40% in London and 18% in Austria and in 2003, Denmark and Austria had no open-street schemes.[107] Meanwhile in the USA, the growth in CCTV schemes accelerated between 1990 and 2000 from a cost of $282 million to more than $1 billion. Following the 9/11 terrorist attacks in 2001, the USA saw an enormous expansion in CCTV in public spaces across its major cities. In a world-wide review, Norris noted that, "While the growth of open CCTV in the Nordic countries has been limited, in other countries, particularly France, Italy and the Netherlands, many cities now have open-street CCTV systems."[108]

From a technological viewpoint, the most interesting development in the area of CCTV surveillance over the past 10 years has been the move away from those very same defects that

---

[104] McCartney, Carol, Robin Williams and Tim Wilson, *The Future of Forensic Bioinformation*, Nuffield Foundation, London, 2010, pp. 107-108.
[105] Norris, Clive, Mike Mc Cahill and David Wood, "Editorial", *Surveillance & Society*, Vol. 2, Nos. 2/3, 2004, pp. 110-135.
[106] Norris, Clive, "A Review of the Increased Use of CCTV and Video-Surveillance for Crime Prevention Purposes in Europe", EU Policy Department C Citizens' Rights and Constitutional Affairs, PE 419.588, April 2009.
[107] Hempel, L., and E. Töpfer, *Urban Eye: Final Report to the European Commission*, 5th FP Urban Eye project, Technical University of Berlin, Berlin, 2004. http://www.urbaneye.net/results/ue_wp15.pdf
[108] Ibid, p. 3.

made CCTV look like a privacy-intrusive technology which was not cost-effective when it came to deterring and solving crime. Blurred, grainy images taken from the wrong angle were replaced or complemented by those from high definition (HD) pan tilt and zoom (PTZ) models, often with capacity for on-board video analytics. The most significant of the technological developments has been digitisation, which enables CCTV systems to be linked to computers, allowing for efficient storage and distribution of large amounts of data and for sophisticated algorithms to be applied for identification and categorisation purposes. Cost has been the main incentive for such developments with the reassessment of provision around cost leading to the integration of systems to reduce manpower costs and the introduction of second generation computerised surveillance systems where the actual monitoring is not done by a human operative, but by an automated digital process.[109] Where a dedicated or secure communications network is not immediately available, suppliers are now using cameras which can transmit and be controlled using Internet Protocol. Where a considerable number of analogue cameras already exist, the suppliers can insert a layer of software that can deal usefully with images from those cameras.

Finally, system designers no longer rely on video alone, but include in their analysis audio and other signals from every possible type of sensor imaginable. Within new project design work initiated by the EU FP7 SMART research project team,[110] this new phenomenon has been categorised as the massively integrated multiple sensor installations (MIMSI) approach to surveillance. MIMSI is the common denominator that can be observed in recent surveillance developments in Beijing, Chicago, New York and Shenzhen. However, the effectiveness of integrating data from several sensors into one system has been questioned. Some commentators point out that while using multiple sensorsand detectors can be effective, it is difficult to predict the number and kinds of detectors (e.g., are radiation detectors enough when terrorists resort to dynamite?) needed in any particular situation. Studies such as SMART may help determine which sensors and detectors would be less privacy-intrusive than others but more effective in countering real threats. These may then constitute a more preferable investment in high-risk areas. There is a delicate balance to be struck as integrating several types of sensors with PTZ CCTV through middleware linking up to multiple databases may be a powerful tool for law enforcement. A surveillance system that has developed in conjunction with developments in CCTV – and digitisation in particular – is that of facial recognition (see below).

There had been little evaluation of CCTV schemes prior to their expansion and what had taken place often showed limited, if any, effect on crime in city centres and transport networks.[111] Studies have been conducted into the use of open street CCTV across a variety of

[109] Surette, R. "The thinking eye: Pros and cons of second generation CCTV surveillance systems", *Policing*, Vol. 28, No. 1, 2005, pp. 152-173.

[110] SMART Project, "SMART Workplan Document", 2010. www.smartsurveillance.eu.org

[111] Ditton, J., and E. Short, "Yes, It Works, No, It Doesn't: Comparing the Effects of Open CCTV in Two Adjacent Scottish Town Centres", in K. Painter and and N. Tilley (eds.), *Crime Prevention Studies*, Vol. 10, 1999, pp. 201-224. Cameron, A., E. Kolodinski, H. May and N. Williams, "Measuring the effects of Video Surveillance on Crime in Los Angeles", Californian Research Bureau, University of Southern California: School of Policy Planning and Development, 2008.
http://www.cctvusergroup.com/Public%20Support%20for%20CCTV.htm. Gill, Martin, and Angelsa Spriggs, *Assessing the impact of CCTV*, Home Office Research, Development and Statistics Directorate, London, 2005.
King, J., D. Mulligan, S. Raphael, "Citris Report: The San Francisco Community Safety Camera Program", Berkeley School of Law, California, 2008.
http://www.citrisuc.org/files/CITRIS%20SF%20CSC%20Study%20Final%20Dec%202008.pdf. Ratcliffe, J., and T. Taniguchi, *CCTV Camera Evaluation: The crime reduction effects of public CCTV cameras in the City of Philadelphia, PA installed during 2006*, Temple University, Philadelphia, 2008.

countries: namely, in South Africa,[112] South Korea,[113] Norway[114] and Canada.[115] The URBANEYE project concluded that "next to the success stories, there are examples of mixed as well as of negative findings. The findings of the evaluations of the crime impacts of CCTV are disparate and not easy to summarise."[116] The crime prevention purpose of these systems was also limited to that of situational crime prevention, aiming to reduce opportunities for crime. They had no role to play in the wider, socio-structural causes of crime or individual interventions. However, some studies had shown evidence of the displacement – rather than the prevention – of crime, including geographical, tactical and target displacement.[117] Nevertheless, developments in technology and use of CCTV systems continue apace and are illustrated by the use of CCTV systems in schemes such as automated number plate recognition (ANPR) and, with less precise results, in conjunction with facial and behaviour recognition technologies.

Webster identifies five myths in relation to CCTV: that it works; is everywhere; citizens want it; citizens understand its technological capabilities; and CCTV is there for protection and to reduce crime.[118] He goes so far as to conclude, from his review of the evidence base, that "In the case of CCTV, the implementation of schemes seems to be at complete odds with the evidence base which in turn makes it difficult to provide a logical rational reason for installing CCTV surveillance systems so quickly and in so many public places."[119] The social impact of open-street CCTV has been found to include discrimination and exclusion based upon personal features unrelated to criminal behaviour per se. These findings have been found in studies across different countries.[120] Norris and Armstrong found that decisions to monitor individuals were formed on the basis of sociological categories, such as age, race and gender, rather than on the basis of behaviour by the individual and so unwarranted suspicion did not

---

http://www.temple.edu/cj/misc/PhilaCCTV.pdf

[112] Minnaar, Anthony, "The implementation and impact of crime prevention/crime control open street Closed-Circuit Television surveillance in South African Central Business Districts", *Surveillance & Society*, Vol. 4, No. 3, 2007, pp. 174-207.

[113] Park, Hyeon Ho, Gyeong Seok Oh and Seung Yeop Paek, "Measuring the crime displacement and diffusion of benefit effects of open-street CCTV in South Korea", *International Journal of Law, Crime and Justice*, Vol. 40, 2012, pp. 179-191.

[114] Lomell, Heidi Mork, "Targeting the Unwanted: Video Surveillance and Categorical Exclusion in Oslo, Norway?", *Surveillance & Society*, Vol. 2, Nos. 2/3, 2004, pp. 347-361.

[115] Walby, Kevin, "Little England? The rise of open-street Closed-Circuit Television surveillance in Canada", *Surveillance & Society*, Vol. 4, Nos. 1/2, 2006, pp. 29-51.

[116] Hempel, L., and E. Töpfer, *Urban Eye: Final Report to the European Commission*, 5th FP Urban Eye project, Technical University of Berlin, Berlin, 2004, p.16. http://www.urbaneye.net/results/ue_wp15.pdf

[117] Skinns, D., "Crime Reduction, Diffusion and Displacement: Evaluating the Effectiveness of CCTV", in Clive Norris, Jade Moran and Gary Armstrong (eds.), *Surveillance, Closed Circuit Television and Social Control*, Aldershot, Ashgate, 1998. Brown, B., "Closed Circuit Television in Town Centres: Three Case Studies", Crime Prevention and Detection, Series Paper 73, Home Office, London, 1995. Sarno, C., "The Impact of Closed Circuit Television on Crime in Sutton Town Centre", in M. Bulos and D. Grant (eds.), *Towards a Safer Sutton? CCTV One Year On, London Borough of Sutton*, London, 1996.

[118] Webster, William, "CCTV policy in the UK**:** reconsidering the evidence base", *Surveillance & Society*, Vol. 6, No. 1, 2009, pp. 10-22.

[119] Ibid, p. 20.

[120] Norris, Clive, and Gary Armstrong, *The Maximum Surveillance Society: The Rise of CCTV*, Berg, Oxford, 1999; Dubbeld, L., *The regulation of the observing gaze: privacy implications of camera surveillance*, PrintPartners Ipskamp, Enschede, 2004; Fonio, C., F. Pruno, R. Giglietto, L. Rossi, and S. Pedriol, "Eyes on You: Analyzing User Generated Content for Social Science", Paper presented at the Towards a Social Science of Web 2.0 conference, York, UK, May 2007; McCahill, M., *The Surveillance Web: The Rise of Visual Surveillance in an English City*, Willan, Devon, 2002; Lomell, H.M., 'Targeting the Unwanted: Video Surveillance and Categorical Exclusion in Oslo, Norway?', *Surveillance & Society*, Vol. 2, Nos. 2/3, 2004, pp. 347-361.

fall equally on all social groups.[121] Two thirds (65%) of teenagers were reported to have been surveilled for no obvious reason compared with only one in five (21%) of those aged over 30. Similarly, black people were twice as likely (68%) to be surveilled for no obvious reason compared to whites (35%) and men three times (47%) more likely than women (16%). This led Norris and Armstrong to conclude that these observations constituted discrimination[122] and, it has been found, these findings are repeated in studies across Europe.[123] Similarly, there have been reported cases of sexually inappropriate and unprofessional monitoring activities by male operators in relation to female subjects, resulting in calls for the adoption of training and licensing schemes for operating companies.

The effectiveness of CCTV in relation to claims concerning crime reduction and prevention remain inconclusive. As the early installations of the 1990s now require replacement or updating, the issue of cost raises its profile. It is clear that a sound basis of research data evaluating the effectiveness of CCTV systems for law enforcement purposes was never established and cannot now be drawn upon to justify renewed expenditure. There are cases cited in which CCTV footage undoubtedly assisted with the apprehension of suspects for particular – usually serious – crimes. However, available research studies demonstrate neither clear nor consistent evidence of success in crime reduction. Webster's myths remain pertinent[124] and cast a shadow of doubt over the purpose and effectiveness of the CCTV systems bearing down on many of our public spaces.

4.3.3 Facial recognition (FRT)

Unlike DNA and fingerprints, for which there needs to be a degree of suspicion – however minimal – before they are taken, the facial image is routinely taken on a daily basis for everyday activities such as transport passes, driving licences, gym membership and library tickets. This everyday use has rendered those who screen their faces even more suspicious.[125] As if they were disguising their identities for ulterior motives, media and public attention have been seen to focus on women wearing the burqa and youths in hoodies. Despite the fact that with the use of CCTV, facial images can be captured and decoded without the participation or consent of the individual, recognition can only be achieved through data matching. Nevertheless, as the Conservative *New York Times* columnist William Safire describes it: "to be watched at all times, especially when doing nothing seriously wrong, is to be afflicted with a creepy feeling .... It is the pervasive, inescapable feeling of being unfree."[126] Although surveillance has always been acknowledged as powerful, it is

[121] Norris, Clive, and Gary Armstrong, *The Maximum Surveillance Society: The Rise of CCTV*, Berg, Oxford, 1999.
[122] Ibid.
[123] Dubbeld, L., *The regulation of the observing gaze: privacy implications of camera surveillanc*e, PrintPartners Ipskamp, Enschede, 2004.
Fonio, C., F. Pruno, R. Giglietto, L. Rossi, and S. Pedriol, "Eyes on You: Analyzing User GeneratedContent for Social Science", Paper presented at the Towards a Social Science of Web 2.0 conference, York, UK, May 2007; von Hirsch, A., and C. Shearing, "Exclusion from Public Space", in A. von Hirsch (ed.), *Ethical and Social Perspectives on Situational Crime Prevention*, Hart Publishing, Oxford, 2000.
[124] Webster, William, "CCTV policy in the UK**:** reconsidering the evidence base", *Surveillance & Society*, Vol. 6, No. 1, 2009, pp. 10-22.
[125] Introna, Lucas, and David Wood, "Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems", *Surveillance & Society*, Vol. 2, Nos. 2/3, 2004, pp. 177-198.
[126] Safire, W., "The Great Unwatched", *The New York Times*, 18 Feb 2002.
www.nytimes.com/2002/02/18/opinion/18SAFI.htm

digitisation that has significantly increased its power, intensity and scope.[127] Digitisation enables the use of software algorithms for the automated recognition of human biometrics, and facial recognition systems are an illustrative example of that capacity. Facial recognition algorithms combined with smart CCTV provide a good example of what has been termed "silent technology". Furthermore, software algorithms are "operationally obscure" – what actually takes place through the chain of activities is not transparent – and are based on very sophisticated statistical methods: all of which can serve to create a sense of legitimacy that is more than is technically deserved.

There are two main categories of algorithms used in FRT: image template algorithms and geometry feature-based algorithms. Image template algorithms use a template-based method to calculate correlations between a face and one or more standard templates to estimate facial identity. The most commercially well-known of these is the "MIT Bayesian Eigenface technique", which uses a principal component analysis (PCA) method for calculating correlations. Geometry feature-based algorithms use methods that capture local facial features and their geometric relationships: measuring distances and angles to create a unique face "print". The local features analysis (LFA) method is less sensitive than the PCA to variations in light, skin tone, eye glasses, facial expression and hairstyle. Both categories use reduction – reducing the image size – which can lead to minorities being more easily recognised as "different" to standard templates or to many images in a database gallery.

The face recognition community has benefited from a series of US Government-funded technology development efforts and evaluation cycles, beginning with the FERET program in September 1993 through to the most recent evaluation in 2010.[128] Facial recognition vendor tests (FRVT) conducted in 2000, 2002, 2006 and 2010 evaluated the efficiency and effectiveness of the technology and have documented, roughly, three orders-of-magnitude improvement in performance from the start of the 1993 FERET. Although some scepticism was expressed over the fact that the research was funded by a US Government agency, the 2002 test was considered the best of that period as it had as large dataset of over 37,000 and included indoor and outdoor images with a probe image to test the database. The highest results achieved were a 73% match with a 1% false positive. Even though the outdoor images were better than one might ordinarily expect, performance dropped to 50% match for outdoor photos. The age of database images also affected performance with a drop of 10% over two years age of image. The larger the size of the database also decreased performance. This and other studies also reported biases in identification rates, which were higher for males than females, higher for older than younger and higher for Asians and African-Americans than whites.[129]

The American Civil Liberties Union has also commented that, "Facial recognition software is easily tripped up by changes in hairstyle or facial hair, by aging, weight gain or loss, and by simple disguises." [130] Nevertheless, developments in statistical and digital methods since over

[127] Introna, Lucas, and David Wood, "Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems", *Surveillance & Society*, Vol. 2, Nos. 2/3, 2004, pp. 177-198.
[128] Grother, Patrick, George Quinn and Jonathon Phillips, "Report on the Evaluation of 2D Still-Image Face Recognition Algorithms", NIST Interagency Report 7709, 2010.
[129] US Department of Defense, "Facial Recognition Vendor Test 2000 Evaluation Report", US Department of Defense Counterdrug Technology Development Program Office, 16 Feb. 2000 / 29 Nov. 2000. http://www.dodcounterdrug.com/facialrecognition/DLs/FRVT_2000.pdf
[130] American Civil Liberties Union, "ACLU Opposes Use of Face Recognition Software in Airports Due to Ineffectiveness and Privacy Concerns", ACLU, 29 Nov. 2002. http://archive.aclu.org/issues/privacy/FaceRec_Feature.html

a decade ago have contributed to improvements in technological performance and capacity. Interestingly, an area of biometric identification related to the FRS that has received increasing attention in recent years is that of the ear biometric. The French criminologist, Alphonse Bertillon, in the 1890s, pointed out that the ears – if not hidden by hair or hat – have a rich and stable structure that changes little with age. More recently Hurley, Abab-Zawar and Nixon[131] point out that "the ear does not suffer from changes in facial expression, and is firmly fixed in the middle of the side of the head so that the immediate background is predictable, whereas face recognition usually requires the face to be captured against a controlled background"[132] and this is an area of research that is ongoing.

The FRVT in 2006, sponsored by the National Institute for Standards and Technology (NIST), showed that performance was up tenfold since 2002. This rise in performance has been largely attributable to two areas of development: three-dimensional images and surface (or skin) texture analysis. three-dimensional algorithms improve accuracy and, using three-dimensional sensors, are not sensitive to lighting changes and can identify profile views. Nevertheless, even perfect three-dimensional matching techniques are sensitive to expression. Further improvements in performance have been achieved by the use of surface texture analysis (STA), which turns unique lines, patterns and spots into mathematical space. Tests have shown that the addition of STA can enhance performance by between 20 and 25%. It can even distinguish between identical twins. By combining the achievements and capacity of the original FRT with the developments in three-dimensional imaging and STA, companies such as Identix, with their product FaceIt, have greatly improved performance and achieved the best results to date. Nevertheless, identifying people in uncontrolled environments still presents the biggest challenge in FR reliability, which is still at only 50% or less. Alessandro Acquisti at Carnegie Mellon University has commented that facial recognition could soon become a casual pursuit as computers get smaller, more powerful and cloud computing costs come down. "Within a few years, real-time, automated, mass-scale facial recognition will be technologically feasible and economically efficient."[133]

FR systems have been developed and used to track employees' timing and attendance as well as verification for access within the workplacein French, US and Australian airports. They have also been used for biometric visas and passports. Although it has been used within law enforcement settings, the fact that FR in that context entails uncontrolled environments and one-to-many identification, vendors have been less keen to promote their products in this area than in more civilian and commercial settings. The UK National Police Improvement Agency published a report on automated FR in 2006, as part of its FR evaluation and demonstration strategy and academic collaboration programme, which outlines the FR technology, its uses and limitations in the policing context.[134] The report provides a comprehensive list of vendors operating at that time and areas of research and development for the future. It acknowledges the difficulties with reliability in the law enforcement context but nevertheless recognises that FRS offer potential benefits to policing with respect to prevention and detection.

[131] Hurley D.J., B. Abab-Zawarand and M. S. Nixon, "The Ear as a Biometric", in Anil Jain, Pat Flynn and Arun A. Ross (eds.), *Handbook of Biometrics*, Springer, 2007.
[132] Ibid, p. 1.
[133] Ars Technica, "Facial regonition tech is rocketing ahead of laws that can control it", 19 July 2012. http://arstechnica.com/business/2012/07/facial-regonition-tech-is-rocketing-ahead-of-laws-that-can-control-it/
[134] Great Britain National Police Improvement Agency, "Automated Facial Recognition: Applications within Law Enforcement", National Police Improvement Agency Report, London, 2006.

In their book evaluating developments in FR, Delac et al commented that most reports gave a recognition accuracy of more than 90% in controlled conditions.[135] However, when variations – such as pose, ageing and extreme illumination – were introduced, humans maintained remarkable accuracy whereas computers did not come even close. As Singh, Vatsa and Noore put it, "challenges in automatic face recognition can be classified into six categories: illumination, image quality, expression, pose, aging, and disguise". [136] Although disguise is a significant issue for FRS in the field of law enforcement and counter-terrorism, it has only recently been taken up by researchers and "existing face recognition algorithms may not be able to provide the desired level of security for such cases".[137] Singh, Vatsa and Noore conclude that "experimental results suggest that a careful and thorough investigation is required to develop a robust face recognition algorithm that can fulfil the operational needs of real world applications".[138]

The US National Institute of Standards and Technology commissioned a further FVRT study in 2010, with a population approaching 4 million, which comprises the largest public evaluation of face recognition technology to date.[139] Facial recognition algorithms from seven commercial providers and three universities were tested on one laboratory dataset and two operational face recognition datasets (one of which comprised visa images and the other law enforcement mug-shots). The project attracted participation from a majority of the known providers of FR technology including the largest commercial suppliers. Accuracy was measured for three applications: one-to-one verification (e.g., of e-passport holders); one-to-one verification against a claimed identity in an enrolled database (e.g., for driving licence renewal); and one-to-many search (e.g., for criminal identification or detection of driving licence duplication).

The study reported that, as with other biometrics, recognition accuracy depended strongly on the provider of the core technology and, broadly, there was an order of magnitude between the best and worst identification error rates.[140] They also found that, using the most accurate face recognition algorithm, the chance of identifying the unknown subject in a database of 1.6 million criminal records was about 92% and that, in all cases, a secondary – human – adjudication process is necessary to verify that the top-rank hit is indeed that hypothesized by the system. They conclude that, in criminal law enforcement applications, where recidivism rates are high and a pool of examiners is available to filter lengthy candidate lists, facial recognition algorithms offer high success rates. If the most accurate algorithm is used for identification in the population of 1.6 million, an examiner willing to review 50 candidates would only need to look at three, on average, before the match is found. For reasons that are not yet determined, this study confirmed the earlier research findings of differences in ease of identification between groups based on gender, age, build and race. In conclusion, the 2010 FVRT evaluation identifies that more accurate algorithms can significantly reduce the workload on examiners but, nonetheless, human observation and decision-making are

[135] Delac, Kresimir, Mislav Grgic and Marian Stewart Bartlett (eds.), Recent Advances in Face Recognition, In-teh, Croatia. 2008.
[136] Singh Richa, Vatsa Mayank and Noore Afzel, "Recognizing Face Images with Disguise Variations", in Kresimir Delac, Mislav Grgic and , Marian Stewart Bartlett (eds.), Recent Advances in Face Recognition, In-teh, Croatia, 2008.
[137] Ibid, p.149.
[138] Ibid, p.159.
[139] See http://www.nist.gov/itl/iad/ig/frvt-home.cfm
[140] Grother, Patrick, George Quinn and Jonathon Phillips, "Report on the Evaluation of 2D Still-Image Face Recognition Algorithms", NIST Interagency Report 7709, 2010.

indispensible in achieving the law-enforcement aim of a correct FR match between "real" and database images.

4.3.4 Behavioural recognition technologies (BRT)

Behavioural recognition technology and specific sectors – such as gait and voice recognition and polygraph tests – are used mainly for the identification of individuals and for identifying suspicious or risky activities. Only a decade ago, most of these human recognition technologies were considered to be in their infancy but have, since then, been the focus of on-going research and development. Strides in understanding artificial intelligence and the power of modern computers have enabled significant developments in behavioural recognition technologies. Whereas earlier surveillance equipment filming human activity relied upon specific and narrowly defined rules put in place by human operators, the new technology relies on "reason-based" software, allowing computers to autonomously learn behavioural patterns. From standard streams of camera data, the computer detects and tracks subjects, characterises their appearance and other properties, classifies them and learns their behaviour patterns. The system stores these patterns and, when a divergence is detected, an alert is issued. It is also possible now to send video data via digital networks instead of analogue videos or closed networks and system efficiency is improved with multi-location surveillance videos that can be controlled centrally.

Researchers have noted that behaviour modelling for crowds is usually much coarser than that for individuals. However, the crowd-tracking algorithm they used proved to be robust and gave reliable crowd movement vectors.[141] A similar system, Cromatica, developed by Sergio Velastin of King's College London, has been used to good effect on the London Underground to monitor crowd flow movements and control congestion. It has proved effective in identifying potential suicide incidents – by recognising patterns of behaviour that precede a person jumping from a platform – to which staff can then be directed to prevent or recover. Following the attacks of 9/11 and 7/7 in the US and UK, the definition of critical infrastructure has expanded to include a vast array of public and private locations, such as bridges, sports stadiums, national monuments and pharmaceutical companies. However, vast data needs evaluating and filtering for intelligence to be extracted from it and become useful. Humans must be alerted to real threats without becoming overwhelmed by the volume of normal activity.[142]

Challenges to developers have been posed by the need to differentiate effectively between humans, vehicles, birds, trees moving in the wind, reflections from marble, glass, wall mirrors, changing lighting conditions as well as rain and snow. Major developers and suppliers include Philips Research, who launched their "intelligent video" product ActivEye, in the US, and the Japanese company, Oki Electric, who provide a video coding technology product, VisualCast. Behavioural Recognition Systems (BRS) Labs launched their pioneering AlSight behavioural analytics technology in 2009 and their revenue rose from $20 million in that year to $200 million in 2010. In March 2012, BRS Labs were issued with a patent for new behavioural recognition technology involving the use of video surveillance and are working on other surveillance technologies for which patents are expected to be announced.

---

[141] Shobhit, Saxena, et al. "Crowd Behaviour Recognition for Video Surveillance", Proceedings of the 10th International Conference on Advanced Concepts for Intelligent Vision Systems, 2008, pp. 970-981.

[142] Yamada, Yoichi, Carolyn Ramsey, Richard Smolenski, "Behaviour Recognition: Does Someone Look Out of Place?" *Security World Magazine Online*, [n.d.].
http://www.securityworldmag.com/tech/tech_view.asp?idx=249&part_code=030160069&page=1

Another significant area of behavioural recognition work involves the identification of both speech and speakers. Speaker identification should be distinguished from speaker verification or authentication. The former involves establishing the identity of an unknown speaker, whereas the latter usually involves a gatekeeping function where the individual voluntary participates in an activity such as telephone banking. Speaker recognition technology uses the acoustic features of speech that differ between individuals and are based on anatomical differences (size and shape of mouth and throat) and individual patterns (voice pitch and speaking style). These differences form a voice-print or template unique to the individual. Over the past 50 years or more, security agencies such as NSA and GCHQ have been conducting and sponsoring research into speech recognition technologies. According to the EU Scientific and Technical Options Assessment Office,[143] reports indicated that attempts at developing techniques for speech or voice recognition were not sufficiently reliable to be used for intelligence purposes. Commercial PC systems usually required one or more hours of training in order to recognise a single speaker and, even then, such systems might mis-transcribe 10 per cent or more of the words spoken. US and Canadian research in the 1990s looked at word-spotting in telephone conversations and could only conclude that, regardless of environmental conditions, word-spotting remained a difficult problem. Even where continuous speech recognition systems were used, involving more conversations over time with large vocabulary sets, which was a better approach, researchers concluded that speaker identification was still not particularly reliable or effective.[144]

With an increased call for recognition technologies that operate at a distance, there has been growing interest in human gait recognition (HGR). HGR works from walking characteristics and includes visual cue extraction and classification. Generally, a gait is composed of a sequence of kinetic characteristics of human motion and most systems recognise it by the similarities of these characteristics. Research approaches to the development of HGR technology have largely been appearance-based and model-based.[145] The positive features of HGR as a biometric technology are that it is non-contact, non-invasive and can be conducted at a distance. However, gait factors have a high intra-personal variation in shape and are influenced by external factors. For example, gait features can vary with footwear, clothing, load carrying, mood, ground surface and time differences. Nevertheless, research has demonstrated that, and it is still considered to be, an effective biometric means of human identification at a distance.[146]

Another area of behaviour recognition technology, commonly associated with the USA but has gained increased use within the UK in the past decade, is that of the polygraph. The polygraph – often described as a lie detector – measures arousal associated with physiological changes of the autonomic nervous system. As described by the British Psychological

[143] European Union, Scientific and Technical Options Assessment, "Development of Surveillance Technology and Risk of Abuse of Economic Information", A Working Document for the S.T.O.A Panel, PE 168.184, Vol. 2/5, Luxembourg, 1999. http://www.europarl.europa.eu/RegData/etudes/etudes/join/1999/168184/DG-4-JOIN_ET%281999%29168184%28PAR01%29_EN.pdf
[144] Ibid.
[145] Pushpa Rani, M., and G. Arumugam, "An Efficient Gait Recognition System for Human Identification Using Modified ICA", *International Journal of Computer Science and Information Technology*, Vol. 2, No. 1, 2010, pp. 55-67.
[146] Nandini, C., and C.N. Ravi Kumar, "Comprehensive framework to gait recognition", *International Journal of Biometrics*, Vol. 1, No. 1, 2008, pp. 129-137.

Society,[147] the polygraph is a set of equipment that accurately measures various sorts of bodily activity such as heart rate, blood pressure, respiration and palmar sweating. In recent years, brain activity has also begun to be measured in this setting and the bodily and brain activity can be displayed via ink writing pens on charts or via a computer's visual display unit. Polygraph tests are currently used in criminal investigations in many countries including Belgium, Canada, Israel, Japan, Mexico, Singapore, South Korea, Pakistan, the Philippines, Taiwan, Thailand, Turkey, and the USA.[148] In the UK, it has been offered by private firms for voluntary testing purposes, but has not previously been applied within the UK criminal justice system. However, two pilot studies with sex offenders released on licence under supervision – the first involving voluntary participation and the second with offenders required to participate in order to be released on licence – have proved successful and the Government recently announced its intention to extend the scheme across the country.[149] The pilot study involving mandatory testing, which was evaluated by the University of Kent between 2010 and 2011, comprised 332 "polygraph offenders" and 303 "comparison offenders". The trials found that the benefits of using the polygraph were that offenders:

- were more honest with their offender managers, providing probation staff with more information about the potential risks they pose;
- made twice as many disclosures to probation staff, such as admitting that they had contacted a victim;
- admitted the tests helped them manage their own behaviour more effectively.

A 2009 trial conducted to identify fraudulent activity using voice risk analysis (VRA) with Job Centre Plus benefits applicants was shelved after results proved ineffective. Only 37 per cent of applicants, who, after conducting a telephone interview were deemed to be high risk of being fraudulent, were later found to be so. A third of applicants deemed to be low risk on the telephone interview using VRA, later, on further assessment, had their benefits reduced.[150] However, polygraph tests have also been used increasingly by employers to check applicants' CVs and other responses, on a voluntary basis: despite doubts expressed by occupational psychologists about their reliability and value to a selection process.[151] As the British Psychological Society has commented:

> Most published research on polygraphic deception detection has been concerned with its possible use in criminal investigations. The results of better quality research studies demonstrate that while the correct classification of deceivers can sometimes be fairly high, incorrect decisions about who is or is not being deceptive occur at rates that are far from negligible…. Use of the polygraph in employment and security screening is not justified by the available research evidence…. Over confidence in the ability of any procedure designed to detect deception can have serious consequences, especially if the deceivers are few among many non-deceivers. [152]

---

[147] British Psychological Society, "A review of the current scientific status and fields of application of Polygraphic Deception Detection", 2004. http://www.bps.org.uk/content/review-current-scientific-status-and-fields-application-polygraphic-deception-detection

[148] Ibid.

[149] *The Guardian*, "Sex offenders face mandatory lie detector tests", 20 July 2012. http://www.guardian.co.uk/society/2012/jul/20/sex-offenders-lie-detector-tests

[150] BBC News, "Genuine job seekers fail lie test", 2009. http://news.bbc.co.uk/1/hi/england/nottinghamshire/7938447.stm

[151] BBC News, "Employer lie detector use grows", 2012. http://news.bbc.co.uk/1/hi/england/west_midlands/8354559.stm

[152] British Psychological Society, "A review of the current scientific status and fields of application of Polygraphic Deception Detection", 2004, p. 4. http://www.bps.org.uk/content/review-current-scientific-status-and-fields-application-polygraphic-deception-detection

As outlined, the purposes of development of behavioural recognition technologies have been largely twofold: that of establishing identity and of identifying suspicious or risky activity. The research evidence appears to support the value of BRTs less with respect to the latter purpose than the former. As with facial recognition techniques, reliability with BRT remains questionable in achieving accurate matches of identity and results can be affected by personal and environmental changes as well as disguises. Nevertheless, as the information reviewed indicates, there has been some merit in the technologies developed and the ongoing work on further improvements continues to reap results. However, the assessments of BR technologies with respect to identifying dishonesty and fraudulent activity are far less optimistic, although some useful, secondary effects have been achieved, as with the use of polygraph tests with sex offenders released on licence. The ability to intervene in potential suicide bids – as seen in the work on the London Underground – also demonstrates a further merit to developments in BRT. In summary, the appraisal and the outlook can only be described as chequered. The achievements demonstrated by the developments in BRT cannot be dismissed but those technologies must be utilised with both a clarity of purpose and a measured grasp of their limits in terms of accuracy and reliability.

4.3.5 Electronic monitoring

Electronic monitoring (EM) has existed since the late 1960s. Originally conceived and developed by American psychologist Dr Ralph Schweitzgebel, EM was first employed as a "behavioural engineering" tool, that is, the application of electro-mechanical technology for the purpose of understanding, predicting and modifying human behaviour. EM came into widespread use in the 1980s with the explosion of the prison population in the USA. The UK was the next country to employ the use of EM in 1991, closely followed by Sweden. Today most European countries use EM in one form or another. As Renzema and Mayo-Wilson note, "Electronic Monitoring (EM) is either in routine use or has been piloted on every inhabited continent."[153]

In the UK, electronic monitoring technology is used as part of home detention curfews (HDC) and typically consists of a bracelet containing a transmitter worn around the ankle or wrist. This transmitter sends a signal to a monitoring unit (at the site of curfew) which in turn relays information via a mobile phone network or landline to a central computer system located at the service provider. If the bracelet moves beyond the range of the monitoring unit then the control centre is automatically alerted. More recently, Global Positioning System (GPS) combined with electronic monitoring enables continuous tracking in real time and offers the ability to set exclusion or inclusion zones with automatic alerts if an offender enters a prohibited area or comes into close proximity to someone deemed to be off limits. In many US states, there is a requirement to use GPS as a means of monitoring and tracking sex offenders. In some US states, there is a requirement to track certain sex offenders for life.[154] In their evaluation of the effectiveness of GPS on high risk sex offender parolees, Gies et al.

[153] Renzema, M., and E. Mayo-Wilson, "Can Electronic Monitoring Reduce Crime for Moderate to High Risk Offenders?", *Journal of Experimental Criminology*, Vol. 1, 2005, pp. 215-237 [p. 215]. http://ww.correcttechllc.com/articles/14.pdf

[154] Gies, S., R. Gainey, M. Cohen, et al., Maintaining high risk offenders with GPS technology: An evaluation of the California supervision programme, National Institute of Justice, Washington, 2012. https://www.ncjrs.gov/pdffiles1/nij/grants/238481.pdf

concluded that those parolees for whom GPS monitoring provided part of their programme exhibited low rates of recidivism and greater compliance.[155]

EM has also been combined with sobriety testing as a means of combating alcohol-related crime. In the UK, alcohol is said to be implicated in over one million violent crimes and 1.2 hospital admission each year.[156] Recently developed sobriety tags such as SCRAMx measure alcohol consumption by monitoring vapour emitted through an individual's skin (transdermal alcohol concentration). These sobriety tags have the advantage of being able to monitor alcohol consumption continuously and with little need for direct person-on-person supervision.[157]

Those supporters of EM assert that EM:

- Offers a cost effective way of addressing prison overcrowding;
- Enables offender rehabilitation and reintegration into the community, hence reduce recidivism;
- Relative to incarceration, has less of an impact on an offender's family and employment.[158]

Detractors point out its net-widening potential, drawing an increasing number of people into the formal criminal justice system for less serious offences.

Although EM technologies' popularity continues to grow globally, this growth has not been based on or driven by a large body of research. Following their meta-analysis of EM, Renzema and Mayo-Wilson conclude that existing data does not support the assertion that EM is an effective means of reducing crime.[159] More recent evaluations, however, such as that performed by Di Tella and Schargrodsky,[160] portray EM in a more positive light. In this evaluation, rates of re-arrest for those released early on EM (a total of 454 individuals) were compared with those prisoners who served the full term of their sentence (a total of 37,378 individuals). Recidivism rates were 13 per cent and 22 per cent respectively. Similarly, Padgett et al. evaluate the effectiveness of EM on serious offenders in Florida but differentiated between those subjected to home confinement without EM, those offenders with CS monitoring and offenders monitored via GPS.[161] The authors conclude that both GPS and RF EM were associated with lower rates of re-offending. Marklund and Holmberg's

---

[155] Ibid.

[156] BBC News, "Minimum alcohol price planned for England and Wales", 23 March 2012. http://www.bbc.co.uk/news/uk-17482035

[157] Jones, A.W., The relationship between blood alcohol concentration (BAC) and breath alcohol concentration: a review of the evidence, Department for Transport, London, 2010. http://assets.dft.gov.uk/publications/research-and-statistical-reports/report15.pdf

[158] National Audit Office (NAO), *The Electronic Monitoring of Adult Offenders*, Report by the Comptroller and Auditor General, HC 800 Session 2005-2006, 2006. http://www.nao.org.uk/publications/0506/the_electronic_monitoring_of_a.aspx. Ministry of Justice, *It's complicated: The management of electronically monitored curfews: a follow up inspection of electronically monitored curfews*, Her Majesty's Inspector of Probation, Criminal Justice Joint Inspection, (HMIP), 2012. http://www.justice.gov.uk/downloads/publications/inspectorate-reports/hmiprobation/joint-thematic/electronic-monitoring-report-2012.pdf

[159] Renzema, M., and E. Mayo-Wilson, "Can Electronic Monitoring Reduce Crime for Moderate to High Risk Offenders?", *Journal of Experimental Criminology*, Vol. 1, 2005, pp. 215-237 [p. 215]. http://ww.correcttechllc.com/articles/14.pdf

[160] Di Tella, R., and E. Schargrodsky, *Criminal Recidivism after prison and electronic monitoring*, US National Bureau of Economic Research, Working Paper No 15602, 2009. http://www.nber.org/papers/w15602.pdf

[161] Padgett, K., W. Bales and T. Blomberg, "Under Surveillance: An empirical test of the effectiveness and consequences of electronic monitoring", *Criminology & Public Policy*, Vol. 5, Issue 1, 2006, pp. 61–91.

Swedish study tracked two match groups released from prison (those released early on EM versus those who served the full term of their sentence) for a three-year period and monitored reconviction rates.[162] Irrespective of the risk group (high, medium or low) to which participants were assigned, reconviction rates were lowest amongst those who had received EM.

4.3.6 Drug testing and alcohol testing

Whilst countries such as the UK, Spain and Italy currently focus on proof of impairment others such as France, Belgium and Australia have opted for a zero tolerance per se approach where any illegal drug found in the body whilst driving is deemed to be a crime. In Belgium and Germany, the law differentiates between having traces of an illegal drug in the body verses being impaired by the presence of a drug. So whilst it is still a punishable offence to be operating a vehicle with traces of a drug in the body, a harsher penalty is awarded if it can be proven that a drug has impaired driving ability.[163]

An ingested drug can be tested for and measured by examining blood, urine, saliva and sweat. The testing process can involve actively attempting to identify the presence of the un-metabolised drug or its metabolites. Many of those roadside drug testing devices currently in use are concerned with testing saliva samples. Drug screening using saliva samples is particularly useful (relative to urine and blood samples) because testing procedures tend to be non-invasive, do not require the presence of a doctor (to draw a blood sample) and traces of the active drug in saliva tend to provide an indication of recent use. Roadside drug testing devices used across much of Europe tend to be based on immunoassay technology.[164]

Victoria's (Australia) roadside drug screening pilot, launched in 2004, is of particular interest because it represents the first time that motorists anywhere in the world have been randomly selected for roadside drug testing. Participants were breathalysed for the presence of alcohol above permissible levels. Drivers who failed two consecutive breathalyser tests were then charged with driving under the influence of alcohol. Those drivers testing negative in breathalyser tests were asked to undergo roadside drug screening. In this instance, the DRUG WIPE II (an immunoassay test) was used. If a driver tested positive at this point, a second test was performed using the Cozart DDS device (also an immunoassay test). Those drivers testing positive on the Cozart DDS test had a sample of their saliva sent to a laboratory for confirmatory testing.[165] During a 12-month period, a total of 13,176 roadside tests were conducted of which 330 saliva samples were sent to a laboratory for confirmatory testing. Of the 330 samples sent for confirmatory testing, a total of 313 were confirmed to be positive and 17 provided inconsistent results.[166]

---

[162] Marklund, F., and S. Holmberg, "Effects of early release from prison using electronic tagging in Sweden", *Journal of Experimental Criminology*, Vol. 5, No. 1, 2009, pp. 41–61.

[163] Jackson, P.G., and C.J. Hilditch, *A Review of Evidence Related to Drug Driving in the UK: A Report Submitted to the North Review Team*, Department for Transport, London, 2010. http://www.roadsafety.am/publication/pub_int/NorthReview-ReviewofEvidence.pdf

[164] Northern Ireland Assembly (NIA), "Drug Driving Testing Mechanisms Used Globally", Research Paper 34/10, Research and Library Services, Northern Ireland Assembly, 8 Jan 2010.
http://archive.niassembly.gov.uk/researchandlibrary/2010/3410.pdfAn immunoassay is a biochemical test used to detect or quantify a specific substance in bodily fluids using an immunological reaction (i.e., a reaction between antibodies and an antigen to form an identifiable antibody – antigen complex).

[165] Drummer, O.H., D. Gerostamoulos, M. Chu, et al., "Drugs in oral fluid in randomly selected drivers", *Forensic Science International*, Vol.170, Issues 2-3, 2007, pp. 105-110.
http://www.sciencedirect.com/science/article/pii/S0379073807005580

[166] Ibid.

Despite those benefits associated with saliva testing devices and Victoria's apparent success, it is interesting to note that the EU has yet to endorse the use of any single roadside drug-testing device for the detection of all the main drug types. The EU-funded DRUID (DRiving Under the Influence of Drugs, alcohol and medicine) project was designed to facilitate the development of a harmonised EU-wide approach to regulating driving under the influence of drugs and alcohol. The project evaluated eight on-site saliva screening devices. The testing devices were evaluated on the basis of sensitivity, specificity, accuracy, positive predictive value and negative predictive values for the individual substance test of the device. Desired performance values were set at 80% for all devices. Not one of the tested devices achieved the 80 per cent target for sensitivity, specificity or accuracy.[167]

Authors of the DRUID report note that theoretically on-site drug testing devices could act as strong deterrent to drug driving if they were deployed as part of large scale random on-the-spot drug tests. However, at the time of the evaluation, on-site drug tests using saliva were costly, time consuming and in some cases had low sensitivity to certain drug types.[168]

For more than a decade, the British government's Home Office has explored the use of surface-enhanced Raman spectroscopy (SERS).[169] This method of screening offers the potential to be rapid, cheap, non-invasive, sensitive and accurate.[170] SERS is capable of quickly identifying any substance (drugs, explosives, ammunition) and therefore potentially offers a valuable tool in combating crime and terrorism.

There are disadvantages associated with testing saliva. For example, a saliva sample can be adulterated by introducing substances into the mouth between drug use and testing. Also, some drugs actually dry out the mouth thus making the collection of a useable amount of saliva difficult, and saliva testing can be susceptible to contamination. The Intelligent Fingerprinting (IFP), hand-held unit analyses sweat and, according to its developers, removes the possibility of false positive test results and is virtually impossible to cheat.[171]

The IFP device combines fingerprinting with immunoassay technology. The device records a high definition image of a fingerprint and tests for metabolites in sweat produced from pores within the contours of a fingerprint. This technology therefore simultaneously links an

---

[167] Blencowe, T., A. Pehrsson and P. Lillsunde, "Driving under the Influence of Drugs, Alcohol and Medicine: Analytical evaluation of oral fluid screening devices and preceding selection procedures", FP7 DRUID project, 2010. http://www.druid-project.eu/cln_031/nn_107548/Druid/EN/deliverales-list/downloads/Deliverable__3__2__2,templateId=raw,property=publicationFile.pdf/Deliverable_3_2_2.pdf

[168] Ibid.

[169] When light (radiation) interacts with a transparent medium (e.g., a saliva sample), it can do so in different ways. Light can be reflected, absorbed or scattered. The energy and therefore frequency (wavelength) of scattered light is altered. This is referred to as the Raman effect. It is the change in wavelength of this scattered light which provides chemical and structural information about a sample. But Raman signals tend to be inherently weak. By introducing nano-sized roughen surface of gold or silver, the strength of the Raman effect is increased and therefore provides more information about the molecular structure of a sample.

[170] Jackson, P. G. and C. J. Hilditch, A review of evidence related to Drug Driving in the UK: a report submitted to the North Review Team, Department for Transport, London, 2010.
http://www.roadsafety.am/publication/pub_int/NorthReview-ReviewofEvidence.pdf.
Home Office, "Introduction to the Centre for Applied Science and Technology", 2011.
http://www.homeoffice.gov.uk/publications/science/cast/intro-to-cast

[171] Yates, Paul, "Intelligent Fingerprinting", *The Billboard*, Issue 26, 2012, pp. 44-45.
http://www.intelligentfingerprinting.com/news/billboard-article-26April2012.pdf

individual's identity to the presence of a drug.[172] At present, the IFP only exists as a prototype, but there are plans to develop the IFP so as to be able to store data on the hand-held device for further analysis at a later date and to develop the technology so that information can be relayed via wireless technology to relevant police computers. IFP developers claim that this device can be used on latent fingerprints at crime scenes where it can be used to identify not only drugs ingested but also traces of hormones (thus identifying the possible gender of a suspect).[173] Although this new technology could be applied to crime prevention and detection roles (e.g., quickly screening passengers boarding airliners), testing for metabolites as a means of identifying drug use should also account for the possible range of legal substances that can produce the same metabolites.[174]

Zero tolerance per se laws remove the burden of having to establish that the presence of a drug in a driver's system has impaired his or her driving and therefore this approach does not take into account variation in tolerance levels between individuals. As such, this approach runs the risk of criminalising those who do not pose a threat to public safety. This variation in tolerance levels along with the potential effects of polydrug use can mean that proving impairment can be challenging.[175]

Alcohol testing

In most countries, "drink driving" legislation tends to fall into two broad categories: behavioural based statutes and per se laws. Behavioural based statues date back to the turn of the 20th century and were designed to address what was referred to as drunk driving or driving whilst intoxicated (DWI).[176] These statutes demanded that in order to secure a conviction, law enforcement officials need to establish that an individual's driving has been impaired and that this decline in driving ability is attributed to having ingested alcohol.[177]

Ingested alcohol can be tested for and measured by examining blood, breath, urine, saliva and sweat. The testing process can involve actively attempting to identify the presence of ethanol (and ethanol vapour) or ethanol metabolites. Once ingested, alcohol is quickly degraded and after only a few hours, much of it can be broken down. Alcohol metabolites effectively act as biomarkers indicating that alcohol has been ingested and depending on the metabolite identified, can still be present in the body days or even weeks after first having been ingested.

---

[172] Yates, Paul, "Drug detection from fingerprints New technology tests drug metabolites in sweat", Royal *Canadian Mounted Police Gazette*, Vol. 74, No. 1, 2012.
http://www.intelligentfingerprinting.com/news/RCMPGazetteApril2012.pdf

[173] Yates, Paul,"Intelligent' Fingerprinting", *The Billboard*, Issue 26, 2012, pp. 44-45.
http://www.intelligentfingerprinting.com/news/billboard-article-26April2012.pdf

[174] Nutt, D., Written response to Department of Transport consultation paper on road safety compliance, Advisory Council on the Misuse of Drugs, London, 2009. http://www.homeoffice.gov.uk/publications/agencies-public-bodies/acmd1/DfT-road-safety-compliance-cons?view=Binary

[175] Ibid.

[176] OECD, Drugs and Driving: Detection and Deterrence, OECD Publishing, 2010.
http://dx.doi.org/10.1787/9789282102763-en

[177] Jackson, P.G., and C.J. Hilditch, *A Review of Evidence Related to Drug Driving in the UK: A Report Submitted to the North Review Team*, Department for Transport, London, 2010. http://www.roadsafety.am/publication/pub_int/NorthReview-ReviewofEvidence.pdf. In contrast to behavioural-based statutes, per se laws remove the need to prove that an individual's driving has been impaired or that this impairment was directly attributed to having ingested alcohol. Rather, per se laws focus on a scientifically established relationship between blood alcohol concentration (BAC), driving impairment and crash risk. A driver is deemed to have broken the law if his or her BAC exceeds a specified legal limit. These laws were first seen in Norway in 1936 and then in Sweden in 1941 where BACs were derived from blood testing.

By seeking to identify alcohol metabolites (rather than un-metabolised alcohol) "(t)he surveillance window, the period following exposure to a drug when traces can be detected, is substantially extended".[178]

First developed in the 1950s by Robert F. Borkenstein, breathalysers estimate the level of blood alcohol concentration (BAC) by measuring breath alcohol concentration (BrAC). Breathalysers were first used in the USA, and in the 1980s, table-top devices began to be used in Europe for evidential purposes with Britain leading the way in 1983 and followed by the Netherlands (1986), Austria (1986), Norway (1989) and Sweden (1989). Prior to the 1980s, European countries tended to rely on blood testing for evidential purposes.[179]

Modern breathalysers used by law enforcement either use spectrophotometer or fuel cell sensor technologies to detect and measure the presence of alcohol. Modern, table-top breathalysers used by law enforcement are highly accurate. As noted in the Department of Transport 2010 report on the relationship between BAC and BrAC, "The accuracy and precision of modern instruments for breath alcohol analysis are perfectly adequate for their intended purposes."[180]

The purpose of roadside breathalyser tests performed by law enforcement officials is to provide an estimate as to whether or not a driver is over the legal limit. Follow–up blood tests (performed in a laboratory) concretely indicate whether or not a driver's BAC is above the permissible legal limit.

Breathalysers are the most widely used means of performing roadside tests with drivers and have proved to be successful as part of the process of identifying those driving under the influence of alcohol. The need to enforce court orders [Drinking Ban Orders (DBOs) in the UK] has meant that there has been a need for devices capable of monitoring consumption remotely thus reducing the need for close person-on-person supervision. This has led to the development of remote electronic alcohol monitoring (REAM) technology. REAM devices determine alcohol levels via analysis of breath or sweat (vapour). During the metabolism of alcohol in the bloodstream, a small proportion of ethanol is lost as vapour through the skin. There are currently two electronic tags that are capable of monitoring the loss of ethanol vapour through the skin (transdermal alcohol concentration). These are Alcohol Monitoring Service's SCRAMx and Giner Inc's WrisTAS.[181]

The SCRAMx system comprises three parts, a bracelet, modem and remote server known as SCRAMNET. The bracelet consists of two halves worn on the ankle and held together by a robust plastic strap. One half of the bracelet contains sensors and an air pump and the second half of the bracelet houses a signal processing unit. Sensors within the bracelet monitor ethanol levels present in insensible perspiration. Ethanol levels are tested every 30 minutes and the results from these tests are uploaded daily via a modem to the SCRAMnet where data can be analysed. SCRAMx has been designed to meet the needs of law enforcement; therefore, the bracelet has been designed to be tamper-proof. Sensors within the bracelet not

[178] Marques, P., and S. McKnight, *Evaluating Transdermal Alcohol Measuring Devices*, National Highway Traffic Safety Administration, Washingon, DC, 2007, p. 6.
[179] Jones, Alan Wayne, The Relationship between Blood Alcohol Concentration (BAC) and Breath Alcohol Concentration: A Review of the Evidence, Department for Transport, London, 2010.
http://assets.dft.gov.uk/publications/research-and-statistical-reports/report15.pdf
[180] Ibid, p. 32.
[181] Ibid.

only measure ethanol levels, they also measure changes in skin temperature, and infrared sensors are able to identify any barrier placed between the wearer's skin and bracelet. Changes in skin temperature are indicative of changes in sensor distance from the skin, which in itself is an indication that the bracelet has been tampered with. Focus groups conducted with a sample of offenders who have worn the SCRAMx bracelet indicate that it is difficult to tamper with without being discovered. Past evaluations of SCRAMx's effectiveness have indicated that there have been issues around the production of false negative results. In addition, the sensitivity and accuracy of the bracelet have tended to decline over time.[182]

WrisTAS was not originally developed for use in law enforcement although Giner Inc have modified and are continuing to modify the WrisTAS for this purpose. WrisTAS functions in a similar way to the SCRAMx but the device continually monitors ethanol levels and data is transmitted via radio frequency to a computer for further analysis. As with SCRAMx, WrisTAS contains heat sensors and a conductance sensor both of which are capable of detecting whether or not the device has been tampered with.

Past evaluations of WrisTAS found that data was often lost or appeared not to have been captured by the system. In one study, as much as 38 per cent of data expected to be collected had been lost either at the point of data transmission from the device to the computer or during sample collection.[183]

Despite problems associated with sensitivity and accuracy over time, there are advantages to be gained by using Transdermal Alcohol Concentration (TAC) monitoring devices relative to other methods of alcohol monitoring such as breathalysers. In the case of SCRAMx and WrisTAS, data can be collected continuously, supervision is not required for sample collection and the cost of the devices is affordable. Despite these advantages, TAC monitoring is not as accurate a method as monitoring BAC.[184] Although SCRAMx has been commercially available since 2003, until recently its use has been limited to the USA. SCRAMx is currently being piloted in West Scotland and a similar pilot was conducted in London in the summer of 2012 as part of the new Sobriety Orders designed to tackle alcohol-related crime.[185]

Ignition interlocks or breath alcohol ignition interlock devices (BAIID) are in common use across most US states where they tend to be used for repeat DWI offenders.[186] BAIIDs are also used in Sweden, Netherlands and Finland. These systems consist of a hand-held breathalyser located close to the car's steering column with a unit attached to the vehicle's starter system. In order to start the vehicle, the driver must first complete a breathalyser test. If the levels of BrAC are above a prescribed limit, the vehicle simply will not start. These systems are able to record not only the level of BrAC but also record other information such as the number of times, the vehicle's engine was started, failed and aborted tests. Depending on the system used, data from an ignition interlock system can be manually downloaded or downloaded remotely via mobile phone or Internet-based technology. This type of technology has been investigated for more than 20 years, and there is evidence to suggest that BAIIDs are

[182] Ibid.
[183] Jones, Alan Wayne, The Relationship between Blood Alcohol Concentration (BAC) and Breath Alcohol Concentration: A Review of the Evidence, Department for Transport, London, 2010. http://assets.dft.gov.uk/publications/research-and-statistical-reports/report15.pdf
[184] Ibid.
[185] BBC News, "Sobriety orders to be piloted by government", 2012. http://www.bbc.co.uk/news/uk-17407493
[186] Voas, R.B., P.M. Marques and R. Roth, "Interlocks for first offenders: Effective?", *Traffic Injury Prevention*, Vol. 8, 2007, pp. 346-352.

effective at reducing recidivism amongst repeat DWI offenders.[187] The evidence for first-time DWI offenders is mixed. Current interlock fitting methods may not be possible with the next generation of cars.[188]

4.3.7 Automatic number plate recognition

At its most simple and automatic number plate recognition (ANPR) systems involve a roadside mounted digital camera, which can feed the images to a computer equipped with optical character recognition software that can extract the licence place information from the photograph. To enable accurate reading, high-speed infrared cameras are often used to ensure that images can be captured from fast moving vehicles even at night.[189] While the primary information collected by an ANPR system is images of vehicles and licence plates, often systems also attach date, time and location information to an image.[190] Once alphanumeric characters on each licence plate are rendered into an electronically readable format, it can then be subject to various forms of automated processing, which enable the licence plate to be checked against other databases. There are three main types of ANPR units, namely, (1) fixed, generally permanent static road-side cameras, (2) portable units, which police can use on an ad hoc for operations in particular locations, and (3) in-vehicle units, which are assigned to a particular patrol vehicle.

This history of automatic licence plate recognition is more bound up with road tolling schemes than law enforcement. In order to ensure a fast and efficient means to enable a vehicle to enter and leave a toll road without having to stop, the ability to identify a vehicle and match its details for the purposes of billing and detecting non-payers is highly desirable. ANPR offered one such solution. In 1986, Norway introduced one of the first ANPR-enabled electronic fee collections[191] and, since then, other systems have been introduced around the world most, including in Toronto and Melbourne.[192] The most ambitious scheme to date was introduction in 2003 of a congestion zone covering 21 square kilometres of central London with a total of 203 entry and exit points.[193]

ANPR systems have a wide range of applications in relation to the enforcement of traffic regulations, such as speeding, red light infringements, fatigue offences by commercial drivers and non-compliance of restrictions on provisional drivers, but also other illegal behaviours such as driving without a licence, driving without insurance and defaulting on traffic fines.[194]

---

[187] Marques, P., R. Voas and A. Tippetts, "Behavioral measures of drinking: Patterns in the interlock record", *Addiction*, Vol. 98, 2003, pp. 13-19.

[188] European Transport Safety Council (ETSC), *Drink Driving Monitor*, European Transport Safety Council, No. 16, June 2012. http://www.etsc.eu/documents/Drink_Driving_Monitor_June_2012.pdf

[189] Watson, B., and K. Walsh, "The Road Safety Implications of Automatic Number Plate Recognition", Centre for Accident Research & Road Safety, Queensland, 2008. http://eprints.qut.edu.au/13222/

[190] US International Association of Chiefs of Police Virginia (IACP), Privacy impact assessment report for the utilization of license plate readers, 2009.
http://www.theiacp.org/LinkClick.aspx?fileticket=N%2BE2wvY%2F1QU%3D&tabid=87

[191] See http://www.vegvesen.no/_attachment/109072/binary/187602

[192] Blythe, P.T., P. Knight and J. Walker, "The Technical and Operational Feasibility of Automatic Number-Plate Recognition as the Primary Means for Road User Charging", *The Journal of Navigation*, Vol. 54 , 2001, pp. 345-353.

[193] Transport for London (TfL), Congestion charging: Impacts monitoring, Second Annual Report, April 2004.
http://www.tfl.gov.uk/assets/downloads/Impacts-monitoring-report-2.pdf

[194] Queensland Parliamentary Travelsafe Committee (QPTC), Report No. 51: Report on the Inquiry into Automatic Number Plate Recognition Technology, Legislative Assembly of Queensland, Brisbane, 2008.

In the case of speeding, the ability of the system to record the time and location of a vehicle means that if a ANPR-enabled camera is placed at another location along a stretch of road, it is possible to calculate the time taken for the vehicle to have travelled between the two points. The other applications require linkage to an external database, such as a register of insured drivers or database of outstanding fine defaulters.

Recent policy initiatives in the UK, in particular, have sought to massively widen the scope of ANPR, from being concerned with traffic safety and enforcement to an all-encompassing tool of law enforcement. As Haines and Wells haves noted:

> The extent to which ANPR becomes an intelligence or surveillance tool depends primarily on the nature and scope of the databases used in conjunction with the designated cameras. In contrast to the 'basic' ANPR speed/traffic enforcement cameras which are linked only to the DVLA database, the ANPR systems used by the police are also linked to intelligence databases, including a single centralized National ANPR Data Centre. This is where the ANPR technology has the potential to become a powerful road surveillance tool. The NADC is configured to receive up to 50m reads per day, with the aim of enabling advanced analysis and enquiries at cross-border and national level, although the technology has yet to perform to its full potential. [195]

There are three main developments that have facilitated this. First, the system has been expanded to enable vehicles to be checked against numerous databases, not only those associated with road traffic, but also any other police and intelligence databases or even private sector databases, such insurance registers. When a vehicle is checked against the database, if it is matched against the "hotlist", an alert can be issued to indicate that the vehicle is of interest and recommend a course of action for local officers.[196]
Second, a national network of ANPR cameras has been established enabling the details of all car licence plates captured by the camera network to be stored on a centralised database. By 2010, there were more than 5,000 ANPR-enabled cameras in the network, and the National Data Centre was logging between 10-14 million ANPR reads per day. This creates an intelligence database of more than 3.5 billion per annum reads, which, in itself, can be exploited for intelligence and law enforcement purposes.

Third, the organisational capacity to act upon the information has been created. Each local police districted has established a dedicated intercept team, who at the local level can respond to "hits".

Typically, the system works in the following way: ANPR "reads" vehicle Registration Marks – more commonly known as number plates – from digital images, captured through cameras located either in a mobile unit, in-built in traffic vehicles or via CCTV. The digital image is converted into data, which is processed through the ANPR system. This system is able to cross reference the data against a variety of databases including the Police National Computer

---

http://rti.cabinet.qld.gov.au/documents/2009/apr/gov%20response%20to%20travelsafe%20report%20no%2051/Attachments/Travelsafe%20R51.pdf

[195] Haines, A., and H. Wells, "Persecution or protection? Understanding the differential public response to two road-based surveillance systems", *Criminology and Criminal Justice*, Vol. 12, 2012, p. 257.
http://crj.sagepub.com/content/12/3/257

[196] National Policing Improvement Agency (NPIA), National ACPO ANPR Standards, Version 4.12, November 2011, pp. 19-20.
http://www.acpo.police.uk/documents/crime/2011/201111CBANAAS412.pdf

(PNC), local force intelligence systems and other related databases, for example, that of the Driver and Vehicle Licensing Agency (DVLA). Once the data has been cross-checked against these databases – a process that takes around 1.5 seconds to complete – information about the vehicle, its registered owner and driver appears on a computer where it is evaluated by ANPR officers. If the information supplied via the ANPR system alerts officers to an offence or relevant intelligence on a vehicle, the vehicle will be stopped to allow officers to investigate further. ANPR officers acting as "interceptors" also use their observation to stop other offenders not highlighted by the system. ANPR systems are able to check up to 3,000 number plates per hour, per lane, even at speeds of up to 100 mph.[197]

In terms of the enforcement of traffic laws, particularly those associated with driving without a licence or insurance, by increasing the chances of detection, ANPR operates on a classic deterrence theory of crime reduction. The increased efficacy of automating the system for the identification of miscreants, coupled with dedicated intercept teams, should increase the chances of getting caught, and therefore act as both a specific deterrence to capture offenders and a general deterrence to potential offenders who are more likely to comply if they believe there is a stronger chance they will be caught.

However, as aid to criminal investigation, the aim of ANPR is to locate, identify, track and link vehicles and their occupants. In July 2009, the National Police Improvement Agency (NPIA) and Association of Chief Police Officers (ACPO) issued advice to police forces entitled *Practice Advice on the Management and Use of Automatic Number Plate Recognition* which detailed the extensive data mining potential of the new database.[198] It is now possible for UK police forces to interrogate in excess of 3.5 billion records per year lodged on the system.[199] The main ways that the data can be exploited through data-mining are outlined as: vehicle tracking: real time and retrospective; vehicle matching: identifying all vehicles that have taken a particular route during a particular time frame; geographical matching: identifying all vehicles present in a particular place at a particular time; incident analysis: can be used to refute or verify alibi statements, to locate offenders, to identify potential witnesses to specific incidents by identifying vehicles in the location at the time of an incident; network analysis: by identifying the drivers of vehicles and their network of associates, ANPR can be used to indicate vehicles that may be travelling in convoy; subject profile analysis; by creating a in depth profile of the suspects by integrating information from a variety of data sources such as "crime reports, incidents reports, witness testimony, CCTV, other surveillance, communications analysis, financial analysis, as well as existing intelligence, to define a pattern of behaviour for a subject of interest"[200]. This relies on the capture and storage of historical ANPR data so that the previous movements of a vehicle can be analysed. It can also identify if there is any association between the movements of the subject's vehicle and a crime that has been committed.

There is no reliable data to determine the extent to which ANPR systems are in use throughout the world for law enforcement purposes. In 2008, the Travelsafe Report documented that ANPR was being used in 25 different national state agencies, particularly for

[197] UK Motorists, Automatic Number Plate Recognition, 2012. http://www.ukmotorists.com/anpr.asp
[198] http://www.acpo.police.uk/documents/crime/2009/200907CRIANP01.pdf
[199] http://www.timesonline.co.uk/tol/news/uk/crime/article7086783.ece. If the National data centre is recording between 10 and 14 million reads per day, that equates to a minimum of 3.6 billion per year.
[200] National Police Improvement Agency (NPIA), Practice Advice on the Management and Use of Automatic Number Plate Recognition, 2009, p. 46.

border security, road tolling and general traffic monitoring. However, Canada, France and Ireland were using ANPR to target prohibited drivers, and detect untaxed, uninsured or stolen vehicles.[201] In the United States, Lum et al. reported that one-third of larger police agencies[202] were using LPR technology and that, as interest in the technology was growing, it was expected this would increase to 50 per cent by the end of 2010.[203] Lum et al. found that "the most common function of LPR was detecting stolen motor vehicles and license plates (91%) and also motor vehicle violations (40%)", but in addition 40 per cent of agencies were also accessing non-vehicular databases. These included databases detailing open warrants, violations of child support, convicted sex offender registries, and those found guilty of selling drugs around schools.[204]

The intensification of surveillance of the motorist is set to expand rapidly over the next few years. By coupling the camera to a computer, it is possible to automatically read the licence plates of passing cars and check them against the records held by the Drivers and Vehicle Licensing Centre (DVLC) and databases held on the Police National Computer (PNC). In 2003, the Home Office announced a national pilot of the ANPR schemes as part of its general crime reduction initiatives. The pilot involved 23 police forces setting up 50 ANPR enabled intercept teams typically consisting of six officers operating from either cars or motorcycles who would stop vehicles that are flagged on various police databases as of police interest. In their first nine months of operation, more than 20 million vehicle registration marks were read and 900,000 of these were flagged on police databases as being of interest to them. As a result more than 130,000 vehicles were stopped and more than 10,000 people arrested, three quarters for non-driving related offences.[205]

The scientific bases for an assessment of the effectiveness of number plate recognition technologies for law enforcement is scant. "Most agencies only evaluate the process of tactics or the efficiency of technologies, concluding "success" if an arrest is made or if the technology works faster. Of the 35 agencies that use LPR, only five (four large and one small) conducted any type of assessment of LPR use, and none conducted impact evaluations."[206]
There have also been few formal evaluation studies. The PA consultancy evaluation of the UK pilot scheme concluded that it had been very successful; however, their criteria of success was the increase of the arrest rate per officer, rather than whether the system led to a reduction in the crime rate or an increase in detections.

In Australia, in 2008, the parliamentary committee looking at road safety noted that "Despite what appears to be promising efficiency gains from the use of ANPR-assisted enforcement compared to traditional enforcement approaches, the committee and others have noted a lack

[201] Queensland Parliamentary Travelsafe Committee (QPTC), Report No 51: Report on the Inquiry into Automatic Number Plate Recognition Technology, Legislative Assembly of Queensland, Brisbane, 2008. http://rti.cabinet.qld.gov.au/documents/2009/apr/gov%20response%20to%20travelsafe%20report%20no%2051/Attachments/Travelsafe%20R51.pdf
[202] Larger police departments were defined as having more than 100 officers.
[203] Lum, Cynthia, Linda Merola, Julie Willis and Breanne Cave, "License Plate Recognition Technology, (LPR) Impact Evaluation and Community Assessment", Center for Evidence-Based Crime Policy, George Mason University, 2010, p.19. http://gemini.gmu.edu/cebcp/lpr_final.pdf
[204] Ibid., p.21.
[205] PA Consulting 2004.
[206] Lum, Cynthia, Linda Merola, Julie Willis and Breanne Cave, "License Plate Recognition Technology, (LPR) Impact Evaluation and Community Assessment", Center for Evidence-Based Crime Policy, George Mason University, 2010, p.23. http://gemini.gmu.edu/cebcp/lpr_final.pdf

of rigorous evaluations in Australia or overseas demonstrating the effectiveness of ANPR technology in reducing road crash rates."[207]

This situation has been somewhat remedied by the publication of the evaluation of the Queensland ANPR trials, although the evaluation did not measure a reduction in road crash deaths but the number of licence plates the systems read in an hour and the number of unlicensed drivers that were detected. Even so, they concluded: "The ANPR system affords substantial improvements over the current technology for detecting unlicensed drivers, both in terms of the detection ability and the operational efficiency and the deterrence value of the technology has the potential to positively impact on road safety."[208]

The most rigorous evaluation conducted so far on the impact of number plate recognition on general crime rates, rather than licence violations, concluded that "there appeared to be no discernible difference in the levels of crime during or after the intervention period between experimental and control hot spots."[209] Neither could they discover a "statistically significant specific deterrence effect of LPR deployment in hot spots on auto theft or auto-related crimes".[210]

4.3.8 Communication interception

Eavesdropping is a surveillance strategy that has gained momentum with the growth of global electronic communication and the increase of communication channels. Messengers were stopped, letters opened and spies had been listening at closed doors since ancient times to get access to secret information. But these activities were the exception not the rule. Present technologies operating with wireless data transmission allow for the massive interception of communication in a way that leaves no visible traces and is difficult to detect by those individuals whose communication is intercepted.[211] While technical standards have been implemented to protect mobile communication from being intercepted, there is evidence that these safeguards are far from safe.[212] What complicates the matter is the global nature of communication. With the emergence of satellite-based transmission, communication interception enters a new realm, since it is no longer linked to individual devices or one-to-one communication lines.[213] While national jurisdiction may pose constraints on communication interception, it is now possible to start such operation from an offshore base where this jurisdiction is irrelevant.[214]

---

[207] Queensland Parliamentary Travelsafe Committee (QPTC), Report No 51: Report on the Inquiry into Automatic Number Plate Recognition Technology, Legislative Assembly of Queensland, Brisbane, 2008. http://rti.cabinet.qld.gov.au/documents/2009/apr/gov%20response%20to%20travelsafe%20report%20no%2051/Attachments/Travelsafe%20R51.pdf

[208] Armstrong, K., A. Wilson, B. Watson, J. Freeman and J. Davey, "Evaluation of ANPR trials for Traffic Policing in Queensland, Report to the Queensland Police Service", State Traffic Support Branch, The Centre for Accident Research and Road Safety, Queensland, 2010, p. 30.

[209] Ibid, p.50.

[210] Ibid., p. 55.

[211] PRISE Project, Deliverable 2.2, Overview of Security Technologies, 2006/2007, p. 25. http://www.prise.oeaw.ac.at/docs/PPRISE_D2.2_Overview_of_Security_Technologies-Revision1.pdf

[212] Borisov, Nikita, Ian Goldberg and David Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11", Published in the proceedings of the Seventh Annual International Conference on Mobile Computing and Networking, 16-21 July 2001.

[213] Swire, Peter, "From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud", *International Data Privacy Law*, Vol. 2, No. 4, 2012. http://idpl.oxfordjournals.org/content/2/4/200.full.pdf+html

[214] Schmid, Gerhard, Rapporteur,

With regard to communication interception at the national level, conducted by intelligence and law enforcement agencies and based on formal orders by courts or other relevant bodies, the figures have been rising over the last years. In the wake of the 2005 London bombing, the EU Data Retention Directive was enacted requiring the "providers of fixed and mobile telephony and internet services to retain details of the communications, including the physical location (for mobile operators), of all citizens – even those never suspected of committing a crime – for 6- to 24-month periods".[215] According to the European Parliament's evaluation report, law enforcement agencies have been keen to access the data, and the volume of both telecommunications traffic and requests for access to traffic data is increasing. Statistics provided by 19 Member States for either 2008 and/or 2009 indicate that, overall in the EU, more than 2 million data requests were submitted each year, with significant variance between Member States.[216]

The report concluded that the "Member States generally reported data retention to be at least valuable, and in some cases indispensable, for preventing and combating crime, including the protection of victims and the acquittal of the innocent in criminal proceedings." In the UK, for example, one of the highest users of intercept data, there were 494,078 requests in 2011, and although there is no statistical evidence to back up the view, one United Kingdom police agency described the availability of traffic data as "'absolutely crucial…to investigating the threat of terrorism and serious crime".[217]

However, an analysis by the German privacy rights group AK Vorrat of national criminal statistics suggests that the overall value of data retention in preventing crime concluded that there is no proof that the number of cleared cases, the crime rate or the number of convictions, acquittals or closed cases significantly depends on whether a blanket data retention scheme is in operation in a given country or not. There is no evidence that countries using targeted investigation techniques clear less crime or suffer from more criminal acts than countries operating a blanket communications data retention scheme.[218]

The Data Retention Directive does not give law enforcement officers access to the content of communications data, however, wire, or phone, tapping (which does) has been a key feature of the investigation of serious crime, and tends to be the subject of high level judicial scrutiny, which limits it usage. Even in the USA where the average number of judicially authorised wiretaps has risen from 1,491 in 2001 to 2,732 in 2011, the absolute numbers are relatively small.[219] In 2011, the 2,092 intercepts resulted in 3,547 arrests and 465 convictions.[220] In the UK, the total number of lawful intercept warrants issued in 2011 was 2,911; no statistics are

---

European Parliament, "Report on the existence of a global system for the interception of private and commercial communications", ECHELON interception system, (2001/2098(INI)), European Parliament, 11 July 2001. http://www.statewatch.org/news/2001/sep/echelon.pdf

[215] European Digital Right Institute, EU Surveillance: A summary of current EU surveillance and security measures, Digital Right Institute, Paper No 2, 2012, p. 5.
http://www.edri.org/files/2012EDRiPapers/eusurveillance.pdf

[216] European Parliament, Commission to the Council and the European Parliament, "Evaluation report on the Data Retention Directive", (Directive 2006/24/EC), 2011, p.21. http://www.statewatch.org/news/2011/apr/eu-com-data-retention-report-225-11.pdf

[217] Ibid., p.23.

[218] Arbeitskreis Vorratdsatenspeicherung, Germany (Working Group on Data Retention), "Serious criminal offences, as defined in sect. 100a StPO, in Germany according to police crime statistics". 2011. http://www.vorratsdatenspeicherung.de/images/data_retention_effectiveness_report_2011-01-26.pdf

[219] http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2011/Table2.pdf

[220] http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2011/Table6.pdf

provided as to the outcome of these intercepts. Although it is difficult to find comparative statistics for other European countries, according to the DETECTOR project, "it can be said that this technology is widely used in the EU" and "According to the Max Planck Institute Italy leads the way in the number of intercepted phone calls, with 76 intercepts per 100.000 of the population", compared with Sweden (33) Germany (23.5) and England and Wales (6).[221]

Law enforcement authorities can exploit vast amounts of data available on social media through both overt and covert surveillance methods, as a number of high profile events have highlighted. The quantity of data is now termed '"ig Data", and is measured in quintillions of bytes (a billion billion), since it is only with numbers this large that one can capture the data flows involved in the estimated 250 million photos added to Facebook, 200 million tweets on Twitter and 4 billion video views per day on YouTube. A variety of research projects is currently assessing the value to law enforcement agencies of being able to plot a suspect's on-line network or contacts through their Facebook page, gauging the public moods in time of crisis through Twitter traffic and profiling their political view from the videos that they download. As a recent DEMOS report on SOCMINT[222] as the monitoring of social media sites has come to be called, reported:

Police forces in the UK and elsewhere are trialling various types of automated social media collection and analysis to collect information to help criminal investigations and gauge the "temperature" of communities with which they are working. Police constabularies have used Flickr to crowdsource identifications of suspects from photographs. Underlying this has been significant public investment in the capabilities to generate SOCMINT. In the UK, the Ministry of Defence's Cyber and Influence Science and Technology Centre has released calls for research to develop capabilities including "cyber situational awareness", "influence through cyber" and "social media monitoring and analysis: crowd sourcing".[223]

Looking at the overall effects of communication interception to prevent and fight crime and terrorism, it appears that a targeted use of this technology can produce results in some cases by producing evidence for a specific case, whereas the dragnet type of large-scale screening of traffic on different channels of communication is more or less ineffective in identifying individual suspects. To what extent the attempts to produce intelligence from analysing new social media will produce any effects cannot be assessed at the present state of development. Nonetheless, substantial investments in technologies of data mining from new social media are taking place, though not primarily in a law enforcement context. However, this does not mean that function creep into this domain will take place once these technologies have reached a mature state.

4.3.9 DNA profiling

Deoxyribonucleic acid (DNA) is found in virtually every cell in the body and contains the genetic instructions that determine physical characteristics. An individual inherits half their DNA from their father and half from their mother and individuals who are closely biologically related to each other will have more DNA in common than unrelated individuals.

[221] Detector Project, "Human Rights Risks of Selected Detection Technologies Sample Uses by Governments of Selected Detection Technologies", University of Birmingham, 2009.
http://www.detecter.bham.ac.uk/documents.html
[222] SOCMINT - social media intelligece
[223] Omand, David, Jamie Bartlett and Carl Miller, #Intelligence, Demos, London, 2011, p. 17.
http://www.demos.co.uk/files/_Intelligence_-_web.pdf?1335197327

With the exception of identical twins, each person's DNA is unique. In the context of law enforcement, DNA profiles are derived from samples such as semen, saliva and blood, which may be left at a crime scene. It is usually claimed that the chance of the DNA profiles of two unrelated individuals matching is on average less than one-in-one-billion. However, the discriminatory power of the analysis decreases for related individuals.[224]

DNA fingerprinting was first developed in the UK by Professor Sir Alec Jeffreys and his team at the University of Leicester in 1984. Jeffreys was quick to understand the potential of DNA in linking individual to crime scenes, and in 1986, the Leicester police asked Jeffreys to help them in a case in involving the rape and murder of two young girls: "Comparing forensic samples from the two victims with blood from the suspect, the forensic analysis revealed that both girls had indeed been raped by the same man, but that that man was not the suspect they were holding in custody."[225] The first DNA fingerprinting techniques were time consuming and required a significant quantity of biological material left at crime scenes to enable the technique to be used successfully, which considerably limited its use in criminal investigation. By the late 1980s, new techniques were invented that could obtain a profile from just a few cells left at a crime scene and new procedures developed which reduced the processing time from weeks to hours. Most significantly, the new "technique allows a numerical designation to be assigned to each piece of DNA, which makes the process highly suitable for integration with a searchable database".[226] DNA samples from suspects are generally collected from cells on the inside of the mouth and taken by means of a swab.

DNA profiling, databasing, searching and matching provide the law enforcement officer a means to establish presence of an individual at a particular location, if there is a biological trace left, and the potential, if their DNA is held on the database, of establishing their identity. If they are not on the database, it allows for suspects who come into the frame through other forms of investigation, to be positively matched or eliminated.

The Interpol Handbook on DNA lists the following as the main ways that a DNA database can contribute to the criminal justice system:

- Different crime scenes can be linked and old cases solved when there are matches between crimes.
- Hits (matches) enable investigators to identify serial offenders and perpetrators.
- It ensures early identification, arrest of serial offenders and prevention of criminal activities.
- DNA can provide important investigative leads to help resolve issues of human identification.
- It serves deterrence (i.e., "you should not commit a crime as we have your DNA profile; we'll catch you!").
- Familial searches can result in the identification of the offender through links with their biological relatives.[227]

[224] National Policing Improvement Agency, "The National DNA Database (NPIA)", Basic Facts, 2012. http://www.npia.police.uk/en/13340.htm

[225] Human Genetics Commission (HGC), *Nothing to Hide, Nothing to Fear*, London, November 2009, p. 23. http://www.hgc.gov.uk/Client/document.asp?DocId=226&CAtegoryId=8

[226] Ibid, p.19.

[227] Interpol: Interpol Handbook on DNA data exchange and practice,2009, available at http://www.interpol.int/contentinterpol/search?SearchText=dna&x=4&y=0

To this list, we should also add the potential to undertake mass "voluntary" DNA screens of a "suspect" population, so individuals can rule themselves out of the frame, thus focusing the investigation on a smaller number of suspects. Between 1995 and 2005, the British Police resorted to this tactic 292 times with the largest screening involving the analysis of more than 4,500 samples taken from local men after the recovery of a body quarry in 1996.[228]

Williams and Johnson argue that DNA profiling is different to other technologies as a form of surveillance as:

> DNA profiling is not targeted at bodies (although it relies on "traces" left by the body) and does not seek to differentiate between individuals through direct observation of their activities. Nor do DNA databases work through the observation of the actions of known or unknown individuals as they happen. Rather, they allow investigators to capture past actions through the artefactualisation and informatisation of the residual presences of individuals at what are designated "crime scenes".[229]

At the heart of this artefactualisation and informatisation is the database, for it is the database, as much as the chemical processing of the samples, that transforms a speck of blood into usable information. The world's first National DNA Database was set up in the UK in 1995. It consists of three sets of data: profiles of samples found at crime scenes; profiles of samples obtained compulsorily from people who are arrested by the police, and samples provided by volunteers, for instance, samples from those known to have been legitimately at a crime. The database consists of the 20 numbers that make up a person's DNA profile along with the result of the gender test. Alongside the DNA information, and details of a person's name, date of birth, ethnic appearance and gender are recorded. Most importantly from an investigatory perspective, there is also a link to the person's file on the Police National Computer.

Originally, entry into the database of suspects was restricted to criminals involved in the most serious crimes such as rape and murder. However, in 1993, the Royal Commission on Criminal Justice,[230] which was set up in the wake of a string of miscarriages of justice resulting from police investigatory malpractice, recommended the setting up of an extension of the DNA testing programme, that the category of serious arrestable offences be redrawn to include assault and burglary and, most importantly, "that the obtaining of samples should be decoupled from their usefulness to a particular investigation (and therefore, implicitly, that they should be obtainable for the sake of future reference)".[231] In the event, the government went further and the Public Order Act of 1994 provided the legislative base to allow swabs to be taken in the investigation of any "recordable" (rather than "serious") offence. Recordable offences are those that may be recorded on the PNC as convictions, including any offences punishable by imprisonment and others such as drunkenness, prostitution and even taking a pedal cycle without the owner's consent.

In 2003, the Criminal Justice Act further extended police powers, allowing them to take samples from anyone arrested for a recordable offence. This meant that even though a person

---

[228] McCartney, C., "The DNA Expansion Programme and Criminal Investigations", British Journal of Criminology, 46 (2), 2006, pp. 175-192, p.179.

[229] Williams, R., and P. Johnson, "Circuits of surveillance", *Surveillance & Society*, Vol. 2, No. 1, 2004, pp. 1-14 [p. 7].

[230] Runciman, W.G., Report of the Royal Commission on Criminal Justice, Cm 2263, The Stationery Office, London, 1993.

[231] Human Genetics Commission (HGC), *Nothing to Hide, Nothing to Fear*, London, November 2009, p. 30. http://www.hgc.gov.uk/Client/document.asp?DocId=226&CAtegoryId=8

may subsequently not be convicted of an offence, or even released without charge, they would be permanently recorded on the DNA database. As the HGC reported noted, in effect, "suspicion (on reasonable grounds) by any police officer became a sufficient condition for permanent and involuntary retention of a DNA record on the NDNAD".[232]

The British government was clearly convinced that the database could not only help solve the most serious crimes, but also play a major role in the investigation of volume crime such as burglary and auto-crime[233] and therefore could play a significant part in their crime reduction programme. Between 2000 and 2005, the Government invested an additional £240 million in the DNA expansion programme. Then Prime Minister Tony Blair announced that "every known offender will have their DNA recorded and evidence from any crime scene will be matched with it".[234]

It was estimated that this would require three million profiles of the arrested population, and by the end of 2005, the database had 2.9 million profiles. By 2012, the national database for England and Wales held profiles on 5,570,284 million individuals, 37,175 volunteer samples and 386,841 crime scene samples. Males made up 78 per cent of the samples. The database had profiles on about 10 per cent of the population, although some sections of the population are more likely to be profiled on the database than others; for example, nearly 40 per cent of black males are now profiled on the database compared with 9 per cent of white males.[235]

In 2011, according to the Council for Responsible Genetics, 56 countries worldwide operate national DNA databases from Asia to Europe and the Americas.[236] This picture confirms an earlier Interpol survey conducted in 2008 which found that 54 countries were operating DNA databases, and that there had been a dramatic increase in their use over the previous decade with a 126 per cent increase (from 53 to 120) in the number of countries using DNA profiling for law enforcement purposes and a 238 per cent increase (from 16 to 54) in the number of member countries with a national DNA database.[237] However, there is also wide variation in the size of the databases: of the 15 million profiles held by law enforcement agencies, 76% of them were held by just two countries, the United Kingdom and the United States. The US seems to be following the UK trajectory, with the FBI database now containing more than 5 million profiles, as individual states pass legislation to widen the net as to who may be entered into the database:

> Forty-four states collect DNA from anyone convicted of a felony, thirty-nine states collect DNA from those convicted of certain misdemeanours, twenty-eight collect DNA from juvenile offenders, six states collect DNA of all individuals arrested and some states (such as California) have started to retain DNA from individuals identified as "suspects".[238]

---

[232] National DNA Database, Basic Facts, 2012. http://www.npia.police.uk/en/13340.htm

[233] Home Office, "DNA Expansion Programme 2000–2005: Reporting achievement", Home Office Forensic Science and Pathology Unit, London, 2006.

[234] Ibid.

[235] Derived from http://www.npia.police.uk/en/13338.htm

[236] Council for Responsible Genetics (CRG), National DNA Datebases, 2011. http://www.councilforresponsiblegenetics.org/dnadata/index_high.html

[237] Interpol, Interpol Handbook on DNA data exchange and practice, Lyon, 2009, p. 52. http://www.interpol.int/content/download/10460/74503/version/7/file/HandbookPublic2009[2].pdf

[238] Council for Responsible Genetics (CRG), National DNA Datebases, 2011. http://www.councilforresponsiblegenetics.org/dnadata/index_high.html

The logic of expansion, and the case to expand DNA profiling from the most serious cases is clearly articulated in the Interpol handbook:

> The more crime types and suspects there are in a national DNA Database, the higher a country's crime detection rate will be. National databases often have match rates for linking a crime scene profile with a previously stored person (between 20-50%). It is therefore clear that DNA Databases can be used to solve high-volume crimes such as burglary or car thefts which are traditionally very difficult crimes to solve by other means.[239]

Interpol and Europol have developed platforms to facilitate the international sharing of DNA profiles. The enactment of the Prüm treaty has enabled automated cross-border searches by the police and criminal justice agencies of each Member State's national database of DNA profiles, fingerprints and vehicle registration data. However, such cross-border searches have run into considerable technical, financial and political difficulties.[240]

The value of DNA profiling to criminal investigators is, in part, due to its successful use in high profile cases. However, evaluating its overall contribution to investigation and detection is more difficult due to the lack of data. As the NPIA, the custodians of the UK national databases, has written:

> It is hard to say how many detections have resulted from the use of DNA as every case is different and other forms of evidence will also contribute to detections. However, we are able to provide figures for the number of detected crimes in which a DNA match was available from profiles loaded to the NDNAD. In 2008/09, 17,607 crimes were detected in which a DNA match was available, including 70 'homicides' (this includes murder and manslaughter) and 168 rapes.[241]

With recorded crime at 4.7 million offences, this means that DNA played a role in detecting under 0.5% of all crimes. Even for more serious crimes such as murder, a DNA match was only available in 11% of cases, and for rape in less than 2% of cases. However, such statistics although useful in contextualizing the limitations of DNA profiling in contributing to detection rates, do little to help us evaluate it in comparison with other investigative strategies. Unfortunately, there are few studies that assess the contribution of DNA profiling with scientific rigour. In the Campbell Collaboration Meta-evaluation of the use of DNA testing in police investigative work for increasing offender identification, arrest, conviction and case clearance , Wilson et al.[242] could only identify five such studies, and even then four of those were described as having "clear methodological weakness". The most rigorous was the US National Institute for Justice evaluation of DNA profiling in high volume crime. This research found that:

> Property crime cases where DNA evidence is processed have more than twice as many suspects identified, twice as many suspects arrested, and more than twice as many cases accepted for prosecution compared with traditional investigation ... (and) ... that DNA is

[239] Interpol, Interpol Handbook on DNA data exchange and practice, Lyon, 2009, p. 53. http://www.interpol.int/content/download/10460/74503/version/7/file/HandbookPublic2009[2].pdf

[240] Töpfer, E., "Network with errors. Europe's emerging web of DNA databases", *Statewatch Journal*, Vol. 21, No. 1, 2011, pp. 1-3. http://www.statewatch.org/analyses/no-134-dna-databases.pdf

[241] National DNA Database (NPIA), Basic Facts, 2012. http://www.npia.police.uk/en/13340.htm

[242] Wilson, David, David Weisburd and David McClure, "Use of DNA testing in police investigative work for increasing offender identification, arrest, conviction, and case clearance", *Campbell Systematic Reviews*, Vol. 7, 2011. https://www.ncjrs.gov/App/Publications/Abstract.aspx?id=258407

at least five times as likely to result in a suspect identification compared with fingerprints.[243]

4.4 MERGING TECHNOLOGIES – THE EMERGENCE OF SURVEILLANCE ASSEMBLAGES

In the previous section we described different technologies applied by law enforcement agencies to combat and prevent crime, to identify, track and locate suspects or criminals and to produce evidence for cases brought to court. Looking at these different technologies and their historical trajectories, they all were embedded in a specific period of technology development, matched to a specific type of policing (and often changing the way policing was done) and many of these technologies reflect historically specific cultural problematics reaching far beyond law enforcement and the fight against crime. Each of these technologies began as stand-alone solutions creating new knowledge, producing information and at the same time displaying limitations of use and application. Limitations often were based on limited information processing capacities and communication capabilities.

This can be demonstrated in the use of fingerprints. In the early days of this technology, the prints were made and kept on paper and a sophisticated set of rules was applied to compare different prints to find matches so as to identify a specific individual. Fingerprints constitute the principal paradigm of an identification technology, answering the question: "Who are you?" A recorded fingerprint is linked to written information about an individual kept in police files and if a print, sharing a significant number of defined features with recorded prints, is found on a crime scene or taken from an individual held by the police, this is seen as proof that this individual is identical with the person registered in the files. Identification means matching physical features (such as fingerprints) found in vivo with bureaucratic information stored in vitro. With finger printing as a stand-alone technology in its early days, this identification was strictly limited to a local context. Having fingerprinted a person at location X, it can be time-consuming to find a match for the prints at location Y. A physical copy has to be sent from X to Y, this copy has to be matched with the prints available at Y and the results have to be communicated back to X. A similar problem emerges when the number of stored fingerprints increases. It may take a very long time to check an individual's fingerprints i with the information stored in police files.

What can be observed here is a fundamental problem: that of information retrieval and analysis. This problem affects all surveillance technologies and different solutions have been developed to cope with it. The solution for the problem of information retrieval and matching developed for fingerprints is to "informate" or digitalise the analogue information contained in the physical image of the print. This tremendously increases the capacities of search procedures. A digital representation of a fingerprint makes it is easy to search huge databases and to communicate this information across long distances to other organisations (or to create a central database as a hub to which all local police offices have remote access). So the step from "isolated" to "informated" use of information created through surveillance technologies is a quantum leap in their range of applicability. Once information is informated or transferred into a digital format and the adequate communication channels and algorithms for matching the data are available, the costs for using this technology in a single case are close to zero.

[243] Roman, John K., Shannon Reid, Jay Reid et al., The DNA Field Experiment: Cost-Effectiveness Analysis of the Use of DNA in the Investigation of High-Volume Crimes, Urban Institute, Justice Policy Centre, Washington, 2008, p. 3.

Here a more general point can be made: as long as high thresholds prevail (in terms of costs, time, etc.) to use a certain technology, this technology will be applied only in cases where the effort seems justified. At the same time, modern legal systems also produce such thresholds. As soon as fingerprinting, for example, becomes an easy-to-use and cheap technology, law enforcement agencies tend to use it for all purposes and limitations have to be introduced at the level of legal regulations (When is it legal to fingerprint an individual? What can be done with the fingerprints? Who is entitled to use them for what purpose?).

The consequence of "informating" surveillance can also be seen in the field of surveillance practices focussing on tracking and/or locating an individual. Whereas in the pre-digital era, tracking and locating a suspected criminal required a policeman, physically following and watching this individual, in the age of electronic communication tools, it is easy to access the mobile phone or any other device regularly used and carried by almost everyone to create profiles of an individual's movements and to locate this person in physical space. Again, there is a tremendous lowering of thresholds for application of these surveillance technologies, and hence legal constraints have to be imposed to limit the use of these easily available tools for law enforcement. The problem of information overload emerges here. With millions of cell phones or mobile gadgets carried by millions of individuals, it may be difficult to filter out the relevant information as long as the targets of surveillance are not known. The envisaged solution is the definition of suspicious patterns to be extracted from protocols created automatically by service providers.

Informating the data produced by different surveillance technologies not only increases the range and ease of application, but also is a precondition to integrate data from different sources in an overall assemblage. As Lianos and Douglas have observed, encounters in modern societies are mediated by institutions and based on a number of information technologies.[244] The paradigmatic case is the interaction with an ATM. The machine identifies the person asking for service by a numerical code, a PIN, before delivering the required service. This interaction is recorded and stored in a database that may be accessed for different purposes – from marketing to law enforcement. Living in a technology-soaked "PIN-culture", each individual is leaving data traces, and produces what David Lyon has aptly called a "data double"[245] or what Sheila Brown has called a "techno-social hybrid".[246]

Moving from isolated to informated to integrated surveillance technologies or practices, forming assemblages and creating data doubles open up new ways of policing and control for presumed illegal behaviour. Creating a maze of what could be called "fictions of normal events", the data traces produced by all different kinds of mundane actions, processes and events can be screened for deviations from an institutionally defined standard of normality.

A good example for this strategy is the set of surveillance measures applied by law enforcement agencies in the fight against financial crime to combat terrorism. All current strategies for combating terrorism and crime include financial measures increasing the

[244] Lianos, Michaelis, and Mary Douglas, "Dangerization and the End of Deviance. The Institutional Environment", *British Journal of Criminology*, Vol. 40, No. 2, 2000, pp. 261-278.
[245] Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2007.
[246] Brown, Sheila, "The criminology of hybrids: Rethinking crime and law in technosocial networks", *Theoretical Criminology*, Vol. 10, No. 2, May 2006, pp. 223-244.

surveillance of capital movements.[247] The measures that have been implemented take various forms, including the imposition of targeted economic sanctions ("blacklists"), transnational communication of personal data[248] and the delegation of policing prerogatives to commercial actors.[249] As with the fight against terrorism more generally, financial surveillance practices have officially assumed functions that are at once investigative, analytical and proactive.[250] More than simple evidence allowing illicit capital to be confiscated, financial information now constitutes a key intelligence-gathering element in the fight against erratic violence. The UK Treasury, for example, emphasises the "key role" played by financial information, which is not limited to "looking backwards" after a terrorist attack, but also includes "looking sideways" as well as "looking forward" in order to identify "the warning signs of criminal or terrorist activity in preparation".[251]

More than 180 national jurisdictions are now involved in combating money-laundering and terrorist financing. In each of these jurisdictions, governmental action relies on the vigilance of regulated institutions, which are responsible for detecting suspicious transactions and clients and passing relevant information on to the competent intelligence services.[252] Banks are foremost among these institutions but many other professions are also involved (insurance companies, public notaries, lawyers, etc.). Banking establishments have thus had to devise and implement procedures for keeping watch over their clientele on behalf of the tasks that governments ask them to perform. They have to operate within normative constraints such as "Know Your Customer" (KYC) rules and specified standards for reporting and record-keeping. They are obliged to verify the identity of their clients, to report "suspicious transactions", to keep detailed records of their business relationships for a specified amount of time, and to respond to enquiries from competent authorities (mainly the national financial intelligence unit of each individual Member State). The security-conscious management of financial flows is based on the identification of at-risk categories and the pre-emptive exclusion of illegitimate players.[253] The surveillance of capital flows belongs to a "governmentality of mobility"[254] that establishes banking institutions as protective filters of

[247] Amicelle, Anthony, and Gilles Favarel-Garrigues, "Financial surveillance: Who cares?", *The Journal of Cultural Economy*, Vol. 5, No. 1, January 2012, pp. 105-124. Levi, Michael, "Combating the Financing of Terrorism. A history and Assessment of the Control of 'Threat Finance'", *British Journal of Criminology*, Vol. 50, No. 4, Winter 2010, pp. 650-669. Gilmore, William C., *L'argent sale: L'évolution des mesures internationales de lutte contre le blanchiment des capitaux et le financement du terrorisme*, Editions du Conseil de l'Europe, Strasbourg, 2005.

[248] Wesselin, Mara, Louise Amoore and Marieke De Goede, "Datawars, Surveillance and SWIFT: Opening the Black Box of SWIFT", *Journal of Cultural Economy*, Vol. 5, No. 1, January 2012, pp. 49-66.

[249] Naylor, Robin T., *Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy*, Revised edition, Cornell University Press, Ithaca, 2004.

[250] Biersteker, Thomas, and Sue Eckert (eds.), *Countering the Financing of Terrorism*, Routledge, London, 2007.

[251] Her Majesty's Treasury, *The financial challenge to crime and terrorism*, London, 28 Feb. 2007, p.10. http://www.hm-treasury.gov.uk/d/financialchallenge_crime_280207.pdf

[252] Favarel-Garrigues, Gilles, Thierry Godefroy and Pierre Lascoumes, *Les sentinelles de l'argent sale : les banques aux prises avec l'antiblanchiment*, La Découverte, Paris, 2009. Mitsilegas, Valsamis, "New Forms of Transnational Policing: The Emergence of Financial Intelligence Units in the European Union and the Challenges for Human Rights: Part 1", *Journal of Money Laundering Control*, Vol. 3, No. 2, May 1999, pp. 147-160. Mitsilegas, Valsamis, "Countering the Chameleon Threat of Dirty Money: 'Hard' and 'Soft' Law in the Emergence of a Global Regime against Money Laundering and Terrorist Finance", in Adam Edwards and Peter Gill (eds.), *Transnational Organised Crime: Perspectives on Global Security*, Routledge, London, 2003, pp. 195-211. Sheptycki, James, "Policing the virtual launderette: Money laundering and global governance", in James Sheptycki (ed.), *Issues in Transnational Policing*, Routledge, London, 2000, pp. 135-176.

[253] Aradau, Claudia, Luis Lobo-Guerrero and Rens Van Munster, "Security, technologies of risk, and the political: guest editors' introduction", *Security Dialogue*, Vol. 39, Nos. 2-3, September 2008, pp. 147-154.

[254] Bigo, Didier, Ricardo Bocco and Jean-Louis Piermay, "Introduction. Logiques de marquage: murs et disputes frontalières", *Cultures & Conflits*, No. 73, 2009, pp. 7-13.

the international financial architecture. These filters have to freeze the assets of blacklisted persons and entities and they perform differential risk assessment and management intended to result in the exclusion of illegitimate flows without obstructing the systemic fluidity of movements of money.[255]

Banks have had to fulfill their obligations by elaborating sophisticated programs for managing risks related to money-laundering and terrorist financing.[256] Such programs include, in particular, the routinised use of specialised data processing tools, the market for which has ceaselessly grown over the course of the past decade.[257] Although the principal motivation of banking establishments in developing these tools has to do with securing auditability [258] – they need to show evidence of scrupulous respect for compliance in order to avoid governmental sanctions – it remains the case that they help professionals forge their suspicions. Today's data processing tools tend to offer a collection of functionalities. In the first place, they allow screening operations to be carried out relating to the development of blacklists in the fight against transnational crime and terrorism. Second, data mining tools are used to create "profiles by collecting and combining personal data, and analyzing it for particular patterns of behaviour deemed to be suspicious".[259]

Risk managers in the banks are critical of the performance and contribution of screening and profiling tools. The frequency of false positives – that is, alerts triggered by homonymy – particularly concerned them. They regularly express doubts concerning the relevance of these tools, in particular, concerning the validity of the data used and the correlations established in order to define profiles. In other words, information processing might be based on official and commercial sources that do not take sufficient steps to maintain its accuracy.[260]

Although this situation is acknowledged across the European level, the official discourse continues to argue that "the fight against the financing of terrorism is aimed at preventing attacks", and that financial information have to be proactively used to identify "terrorist networks" and to develop counter-terrorist intelligence.[261] The solution is then linked to new public–private arrangements in the field of financial intelligence – that is, new forms of co-operation between professionals of security and professionals of finance to manage the risk of terrorist financing. In UK, this has resulted in the establishment of a vetted group to enable the sharing of intelligence between security agencies and the regulated sector (mainly banks)

[255] De Goede, Marieke, *Speculative security: The politics of pursuing terrorist monies*, University of Minnesota Press, Minnesota, 2012. Power, Michael, *Organized Uncertainty: Designing a World of Risk Management*, Oxford University Press, Oxford, 2007.
[256] Hood, Christopher, Henry Rothstein and Robert Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes*, Oxford University Press, Oxford, 2001. Levi, Michael and David Wall, "Technologies, Security, and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society*, Vol. 31, No. 2, May 2004, pp. 194-220.
[257] Taylor, Geoffrey and Martin Gill, "Preventing Money Laundering or Obstructing Business ? Financial Companies' Prespectives on 'Know your Customer' Procedures", *British Journal of Criminology*, Vol. 44, September 2004, pp. 582-594.
[258] Favarel-Garrigues, Gilles, Thierry Godefroy and Pierre Lascoumes, *Les sentinelles de l'argent sale : les banques aux prises avec l'antiblanchiment*, La Découverte, Paris, 2009.
[259] Solove, Daniel, "Data mining and the security-liberty debate", *University of Chicago Law Review*, Vol. 14, February 2008, pp. 745-772.
[260] Ibid.
[261] European Union, Stratégie révisée de lutte contre le financement du terrorisme, Bruxelles, 11778/1/08, 17 July 2008, p. 4.

in relation to money laundering and terrorist financing.[262] The main function of this vetted group is to create a security-cleared environment in which information can be exchanged about sensitive cases or the confidential typologies used to produce alerts.[263]

Thus, members of the reporting sector would learn either directly from the provision of intelligence on specific individuals or indirectly through the communication of confidential typologies what should be regarded as unusual activities for the purposes of defining the parameters of the computer software that carries out their sorting processes. The routinization of these forms of exchange leads to a degree of co-production of surveillance and intelligence. This ongoing process continues what R.T. Naylor[264] has referred to as a "quiet revolution" and illustrates the "complex new spaces of governing in which public and private authorities, knowledges and datasets cooperate closely, and sometimes become practically indistinguishable".[265] Nevertheless, although various actors are placed in a position of informational interdependency, the efficacy of this so-called public-private partnership needs to be balanced.

Given that the regulated sector has a considerable degree of autonomy regarding decision-making within the risk management approach, banking actors prefer to submit defensive reports to the UK financial intelligence unit – without substantiated suspicion – just to protect themselves and their institutions from their regulators in the name of the risk averse.[266] The officials from the UK financial intelligence unit acknowledge this situation of "defensive reporting" and the uselessness of many of the suspicious activity reports they receive; yet the reports are almost invariably stored on their database for 10 years.[267] The storage of these reports is justified on the grounds that such information might be useful in the future for intelligence and investigative purposes. Indeed, the financial intelligence unit does not simply receive and disseminate the suspicious activity reports: it also carries out proactive analysis of the existing stock of SARs (Suspicious Activity Report) to "identify interesting links" through an increasing use of data-mining tools. In addition, one of its official priorities is to assemble an integrative electronic network for data analysis by cross-matching suspicious activity reports with other state databases and other sources of information.[268]

At the end of the day, the results in terms of combating "dirty money" and preventing crime and terrorism remain hypothetical, or at least difficult to assess. One can assume the existence of effective policies (i.e., concrete implementation of regulations), but that does not mean that they achieve their stated aims.

---

[262] Amicelle, Anthony, "Towards a 'new' political anatomy of financial surveillance", *Security Dialogue*, Vol. 42, No. 2, May 2011, pp. 161-178.
[263] Serious Organised Crime Agency (SOCA), *The suspicious activity reports regime annual report*, London, 2007.
[264] Naylor, Robin T., *Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy*, Revised edition, Cornell University Press, Ithaca, 2004.
[265] Amoore, Louise, and Marieke De Goede (eds.), *Risk and the War on Terror*, Routledge, London, 2008.
[266] Amicelle, Anthony, "Towards a 'new' political anatomy of financial surveillance", *Security Dialogue*, Vol. 42, No. 2, May 2011, pp. 161-178
[267] Ibid.
[268] Serious Organised Crime Agency (SOCA), *The suspicious activity reports regime annual report*, London, 2007.

4.5 ASSESSMENT

We have witnessed a gradual transformation of surveillance practices over the course of the 20th century. Developed in the 19th century, and perfected in the early years of the 20th century, the fingerprint and the photograph provided the first reliable means of identification for an increasingly anonymous urban population. The suspect's photographs and fingerprints could be checked against those held on file to authenticate a suspect's identity. The fingerprint also promised another benefit: it could be used to link a person to a locale. The discovery of a fingerprint mark left at a crime scene could then be matched against the files of those who have been entered into the system, or with those just arrested and suspected of the crime. In reality, however, for much of the 20th century, the routine uses of fingerprint evidence was limited by the difficulty of recovering acceptable prints from the crime scene and the labour intensive process of matching. However, in public space, it was the photograph, or its heir, the video image, that has provided a more readily accessible means of locating a person in public space, either contemporaneously, or historically from the images left on the taped archive. With the development of sophisticated pan-tilt-zoom cameras with powerful lenses, it is possible to track a person as they move around the city streets. DNA is also set to replace the fingerprint as the primary means of linking a suspect with a crime scene, as there is a much stronger chance of retrieving a viable sample from the crime scene. Locating and tracking suspects has also been greatly facilitated by the coupling of video cameras to automatic licence plate readers allowing vehicles to be tracked across large distances. For those already identified as criminal, electronic tagging has provided a means of monitoring an individual's whereabouts in space and time, and enabling the enforcement of curfews and restrictions on movements.

The surveillance technologies of the later part of the 20th century were not just employed to identify, locate and track the suspect population but increasingly to monitor their behaviour. The breathalyser introduced in the late 1960 sought to deter drink driving by monitoring the contents of the body, to provide evidence of past drinking behaviour. CCTV operatives now increasingly monitor the streets to locate behaviours that they view as suspicious and worthy of further monitoring or even deployment of security or police personnel to curtail. And drug testing has become a routine feature of many jurisdictions' attempts to break the links between their illegal drug use and a range of acquisitive crimes.

If the quantity of surveillance in criminal justice has increased incrementally over the 20th century, towards its end, there was a radical qualitative shift as the digital revolution began to transform information processing by law enforcement agencies. The fingerprint and the photograph were no longer tied to their material bases of film, paper and graphite. Digitalisation rendered them both mobile, capable of being transmitted freely to any and all points in the system and of being processed by computers. Fingerprint matching no longer required laborious and time-consuming manual analysis, and the new automated systems reduced the time taken to perform a search from hours to minutes. Moreover, digitalisation allows for suspects to be instantaneously checked on the spot, against the criminal record indices by placing their fingertips to be read by a portable handheld device. The same devices are also capable of receiving digital photographs or video images, which can also be used in the process of identification.

Digitalisation does more than just compress space and time, by allowing information to appear at any location on a national or global network almost instantaneously, it also allows for new sorts of analysis to be undertaken. This is particularly the case with photographic

data. Once the photographic image is digital, it can be subject to a raft of pattern recognition algorithms which have the potential, if not yet the operational reality, of allowing the automated recognition of faces, behaviours and events. Although the analysis of complex scenes is still beyond most systems, simpler tasks such as detecting objects moving the wrong way or unattended luggage are now being perfected. Even the elusive goal of being able to recognise a face in crowd is moving closer with the development of algorithms that create a three-dimensional model of the face to compare a likeness. The power of the video camera coupled to the computer is nowhere better illustrated than with automated licence recognition systems. The digital image of the licence plate is capable of being read to extract the number plate and then used to link to a variety of other databases. But it also exponentially increases the power of the state to locate and track vehicles in space and time and potentially create a vast database of vehicle movements and by proxy the driver, which can be later used for retrospective analysis. Digitalisation also brings with it the practical possibility of the full-enforcement of law. For example, this has happened in some jurisdictions with the policing of traffic violations such as speeding and red light infringements are no longer hampered by limitations of wet film technology and expensive manual processing.

The digital revolution has also generated new forms of data that can be exploited for the purposes of crime control. Communications data in the form of logs of telephone and Internet activity are now routinely available to police for investigative purposes. Although the content of communication is not routinely monitored for policing purposes, the use of speech and text recognition systems is employed by some intelligence agencies to monitor vast amounts of intercepted communications.

The ascendancy of the database has come to symbolise the changes to surveillance practice at the beginning of the 21st century, whether the database be of faces, DNA, fingerprints, licence plates, telephone calls or criminal records systems, with their subsidiary databases of sex offenders, those wanted on warrant and so forth. The logic of databases is always expansive, databases rarely get smaller. In the case of identity matching such as DNA, finger printing or facial images, because the operational effectiveness increases as a greater number people are held on the system, there are always sound operational reasons for calling for ever larger categories of inclusion.

The impact of digitalisation is not just making available vast new bodies of data that can be exploited for law enforcement practices in ways that are only just starting to emerge. It is also allowing for the integration of different sensors and systems, for instance, electronic monitoring with sobriety testing. At the larger scale, there is the potential to develop massively integrated multiple sensor inputs (MIMSIs). This is the approach being developed by companies such as IBM in their “Big Data” programmes, which foresee all data held by government departments, police and the private sector being integrated into centralised urban control centres.

Despite the proliferation of surveillance practices to detect and prevent crime, one common theme to emerge from this review is that it is extremely rare for surveillance measures to be properly evaluated before they are widely implemented. Even when they are evaluated, they are often judged in terms of their processual efficiency rather than their impact on outcomes. This is of particular significance in the context of law enforcement where the primary goal of crime reduction is often displaced by evaluations with proxy measures such as the number of licence plates read or the number of arrests made. Where properly conducted evaluations have been carried out, the confident claim of success boasted by industry and practitioners

often vanish. This is not to say that surveillance measures have no effect or have not contributed to the detection and prevention of a number of serious acts of crime and terrorism. However, in the absence of rigorously conducted evaluation studies, it is difficult to assess the overall impact on crime rates, offending behaviour or acts of terrorism. This is compounded by the fact that we are not just talking about a technology. We are describing socio-technical systems that are embedded in a particular organisational and operational context. This means that even when the technology can be shown to have worked in one place, unless the new environment mirrors the previous setting there is no guarantee of that success will be repeated. This is perhaps one of the reasons that when new surveillance technologies are introduced to different contexts, many evaluation studies show contradictory results.

5 SOCIAL AND ECONOMIC COSTS OF SURVEILLANCE

5.1 INTRODUCTION

Johann Čas, OeAW-ITA

Describing the social and economic costs of surveillance is entering a largely unknown territory with soft grounds and quickly changing landscapes. First, surveillance itself is quickly changing, and sometimes hiding its face. Technical progress in information technologies in general is not only increasing the capabilities of surveillance technologies, it is also transforming practically all kinds of information technologies and services into devices and applications which, as a by-product, can be used to extend surveillance to completely private spheres a few decades ago. The different forms of surveillance, the intensity and intrusiveness, the outreach and the range, the duration and permanence, the context in which surveillance is applied are but a few of the many factors influencing the costs of surveillance.

Second, social costs and, in many aspects, even economic costs are far away from being well-defined, broadly understood and easily applied concepts. And this vagueness holds even more if these concepts are to be applied to quickly evolving and multifaceted societal phenomena like surveillance. The manifold difficulties involved in identifying and determining the social and economic costs of surveillance – let alone quantifying these costs – should not , however, serve as an excuse for not dealing with these costs when debating and deciding on the development and implementation of surveillance technologies and measures. On the contrary, neglecting the social impacts and related costs does not imply that they do not exist and that our society does not have to carry them but that we risk to create large and potentially irreversible damage to the economy and society.

We need, however, to be aware that considering social and economic costs doesn't automatically guarantee bringing about the best solutions. There are several reasons why such a promise would be misleading: the social and economic costs comprise to a large extent categories which exclude monetary quantification. The identification and determination of social costs also depends on the evaluation of social values, implying that personal subjective judgements influence the evaluation schemes and their outcomes. It is therefore very likely that the importance and magnitude of the specific social impact resulting from surveillance are not only to be evaluated differently by different persons but also that the algebraic sign might reverse, i.e., that what is regarded as a cost by one person might be regarded as a benefit by another.

Nevertheless, all these limitations do not imply that the intention to take social and economic costs into consideration is futile as such. On the contrary, it demands taking this endeavour seriously as some kind of, at least implicit, evaluation of costs and benefits is taking place anyway. Making this process explicit does not guarantee finding the optimal solution – if such a "best solution" exists at all– but initiating such a process should constitute a safeguard against the implementation of obviously suboptimal measures from a social or economic cost of point of view.

The aim of using the concept of social and economic costs to achieve as much as possible a comprehensive consideration of costs and damages caused by surveillance, or in other words,

to identify the “real price” that has to be paid for the intended benefits of using surveillance to prevent crime and terrorism, discussed in the previous chapter. These costs are not restricted to cost that can be transferred into and expressed as monetary units. This holds even for economic costs, where the calculation and the expression of the costs as financial units is at least in principle possible. In reality, however, it might be impossible to put concrete figures to these costs for several reasons.

Reasons for these difficulties range from missing information, e.g., due to business secrets, unjustifiable efforts needed to get this information to uncertainties about future developments having an impact on the costs involved. More fundamental methodological difficulties relate to the determination of so-called opportunity costs. Opportunity costs are the lost benefits that would have been generated by the second-best alternative to the measure under consideration. In the context of surveillance and security both elements determining the opportunity costs are much more challenging than in usual economic decision-making. Whereas it might not be trivial to calculate the forgone profits when manufacturing product A instead of project B, the determination of the sacrificed security gain due to selecting a specific surveillance measure might in comparison prove utterly impossible; the same holds for the identification of the second-best alternative. It would first require that the selected surveillance measure is accepted as the best solution, then that a general agreement is available about what this is second-best alternative. Both assumptions could be disputed and contested.

The obvious obstacles of applying economic costs concepts to surveillance-related decision-making again do not imply that such decision-making shall be performed without taking such costs into account. On the contrary, the contested nature and the gravity of the potential consequences of increasing surveillance demand comprehensive consideration of “costs” and exploration of alternatives. However, to overcome these obstacles, an adjustment and improvement of applied methods appears to be indispensable to cope with the complexity of the task. In addition to complete and concise assessments of core economic costs, i.e., investment, implementation, operation and maintenance costs, an adequate representation of different interests and perspectives in the assessment process is even more important for an adequate consideration of social costs caused by surveillance.

The request for a participatory approach is supported by the fact that the boundaries between the different cost categories are overlapping and may change over time. So-called externalities or external effects are one example of this blurred relationship. They describe costs or benefits of an economic activity or transaction which are not reflected in prices. A prominent example for negative externalities is environmental pollution caused by an economic activity, which has costs in the form of reduced quality of life and increased costs for the health system carried by a neighbouring population or society as a whole. Another example could be implementation of a specific surveillance technology measure at a specific place, which could be seen as a positive externality, on the one hand, because it increases the objective security of the concerned neighbourhood, but it could also be seen as a negative externality on the other hand because it causes feelings of insecurity by giving the impression that one is living in a particularly endangered area.

The latter example touches on another relevant distinction in this context, namely, that between tangible and intangible costs. Intangible costs, such as increased subjective insecurity, are often difficult to identify, and even when they are specified, difficult or impossible to quantify. A further degree of complexity is that this cost may change character

over time. Short-term intangible costs can turn out as tangible costs over longer term, e.g., decreased property prices in the concerned area.

In the following sections on the social and economic costs of surveillance, the different cost categories will be illustrated and discussed in more detail, based on specific aspects and impacts as well as on concrete examples of surveillance technologies. The specific sections on social and economic costs are preceded by a brief taxonomy of social and economic costs related to surveillance and summarised in a subsequent section discussing the relevance of cost considerations for deciding on the implementation of surveillance measures and technologies. The assessment and evaluation of different cost categories should be an indispensable precondition to be fulfilled before any investment and implementation decision is taken, simply to avoid measures with an overall negative cost benefit ratio or to ensure the selection of the most efficient measure from a set.a of alternatives. However, assessing the social and economic cost criteria is only one of the necessary conditions involved in decision-making. Before the implementation of any such measure, the principles of necessity and proportionality from a human rights perspective need to be fulfilled as a core criterion (see Chapter 6 for more on this).

5.2 TOWARDS A TAXONOMY OF SOCIAL AND ECONOMIC COSTS

Stefan Strauß, OeAW-ITA

Economic aspects play an important role in the implementation of security and surveillance systems and technology. The global growth of security and surveillance modalities is strongly influenced by new economic mechanisms and markets that the OECD has termed the security economy.6.[1]. Surveillance here is mostly seen as a necessary means to foster security which also stimulates new markets and innovation. This assumption follows a simple rational choice formula claiming more surveillance leads to more security and wider use of related technologies creates new markets without considering benefit-cost ratios and assessing its economic and social costs. As a consequence, surveillance is mainly driven by economic objectives that neglect the negative impacts on economy and society in a wider sense. This document aims to fill this gap by analysing costs of surveillance on the economic as well as on the social scale.

Surveillance costs as brake on efficiency and effectiveness of government functions

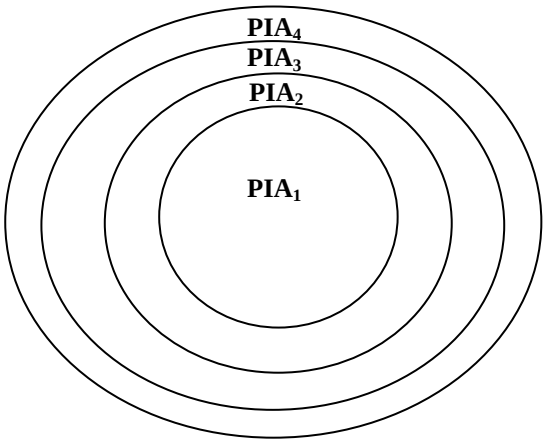
Opposed to the opinion of some technologists that see the conduct of privacy impact assessment as a drag on technological progress and innovation, the costs of neglecting privacy by design and the costs of surveillance are great barriers to efficiency and effectiveness of government functions in the realm of national security. Security and surveillance measurements cannot be placed over “the rule of law, the living legacy of human rights and the workings of the system of justice which are equally central to the national interest”.[2] PIA and the measurement of surveillance costs are thus to be understood as means to reduce the risks of sprawling surveillance to come to a deliberate concept of security and related actions in accordance with fundamental rights.

[1] OECD, *The Security Economy*, Organisation for Economic Co-operation and Development, Paris, 2004. http://www.oecd.org/futures/16692437.pdf.

[2] Raab, Charles, and David Wright, “Surveillance: Extending the limits of privacy impact assessment”, in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012, pp. 363-383.

Privacy impact assessment and framing the costs of surveillance

Privacy impact assessment (PIA) is a means to investigate the impact of surveillance on privacy and provides a way to examine whether technologies are in accordance with privacy and data protection laws or not. Raab and Wright[3] provide an improved model on privacy impact assessment to extend its limits and widen its analytical dimensions to assess the impacts of surveillance in a wider sense. They distinguish between four stages or circles of PIA:



Cycles of PIA[4]

PIA_1 focuses on individual privacy, **PIA_2** on PIA_1+other impacts on individual's relationships, positions and freedoms; **PIA_3** on PIA_2+impacts on groups and categories and **PIA_4** on PIA_3+impacts on society and political system.

This model provides a useful heuristic for developing a (layer-based) taxonomy about the costs of surveillance with four overlapping layers: individual (**L_1**), relational (**L_2**), group (**L_3**), social and political layer (**L_4**).

Costs at individual layer L_1

Layer 1 related costs are linked to the perspective of an individual affected by surveillance. Costs include different aspects of restriction to individual behaviour such as

- mainstreaming or normalising behaviour and conformity,
- inhibition of actions,
- self-censorship and, as a consequence,
- loss of privacy, autonomy and limited freedom.

These costs could also be subsumed as social costs of avoidance.[5] At first glance, from an observer's point of view, these costs might be in accordance with the aim of surveillance to

[3] Ibid.
[4] Ibid., p. 379.
[5] Song, Andrew, "Technology, Terrorism, and the Fishbowl Effect: An Economic Analysis of Surveillance and Searches", The Berkman Center for Internet & Society Research Publication, No. 5, September 2003, pp. 1-26.

alter behaviour. However, this would overlook the fact that these costs can lead to mid- and long-term costs in a wider range such as prolonged loss of trust in security authorities, non-compliance and increasing resistance against surveillance modalities. This undermines the aim of increasing security and might trigger a misleading process for fostering surveillance which leads to a further increase in its costs.

Costs at relational layer L_2

Costs on the second layer are based on layer 1 and include wider impacts as they include the costs of surveillance to the individual's social and political interactions and relationships with others, such as

- decrease in trust,
- self-censorship and fear of sharing one's opinion (reduction in freedom of speech). This also affects
- anxiety to participate and engage in public issues and leads to
- reduction of the willingness to political participation and civic engagement

This layer also addresses the so-called "chilling effect" of surveillance which describes the infringement of individual freedoms and the fear of being in contact with persons who are under observation. This then becomes further costly at the wider layers.

Costs at group layer L_3

This layer incorporates the prior layers and extends them by the negative effects of surveillance on the groups and categories of which the individual is part. The costs are related to surveillance actions on how individuals are treated and include

- social sorting and classification in different groups of customers, passengers, social or ethnic groups that entail
- categorical suspicion and reinforce
- various forms of discrimination (racial, ethnic, social exclusion) which leads to
- reinforcement of social inequalities, mistrust among different social groups and racism

Costs at social and political layer L_4

This layer rests on all prior layers and includes the costs for the functioning of society and the political-administrative system:

- loss of privacy as a public good,
- loss of freedom of speech,
- reversal of the presumption of innocence,
- increasing mistrust in political-administrative system that
- undermine social and democratic activities and lead to
- erosion of democracy.

Economic costs

While the cost categories discussed above are mainly social ones that frequently cannot be simply expressed by figures in the sense of a cost-benefit analysis, they are very likely to

increase if there is no assessment of the economic costs of surveillance before its realisation. Economic costs can be distinguished in

Direct economic costs for acquiring a surveillance system such as

- investment in surveillance, implementation
- installation, operation (including special staff and training costs, data analysis)
- maintenance (updating technologies used, adapting systems to changed security requirements, etc.) and
- additional costs such as increased transport and travel costs including waiting times.

These costs are often passed on to the customers or citizens via additional service fees (e.g., in the case of data retention and related interception interfaces) that lead to a situation where those being monitored have to pay for their own surveillance in an economic and a social sense.

An essential requirement of economic costs assessment is to take opportunity costs into consideration. As mentioned above, these are the lost benefits that would have been generated by the second-best alternative to the measure under consideration.

Indirect economic costs include

- welfare reducing changes in behaviour
- reductions in innovation due to increased conformity and normalised behaviour
- reductions in individual responsibility for security due to reliance on surveillance systems
- increasing dependency of governments on security economy and surveillance providers
- costs of judicial errors (which also trigger social costs such as erosion of trust in the political-administrative system)

False positives and costs of errors

These can be understood as a particular category, demonstrating the associations between social and economic costs (see also section below). Modern surveillance systems increasingly tend to have embedded automated functions aimed at exploiting the benefits of computing for data mining and recognition of behavioural patterns to identify suspect and criminal actions. At first glance, this might be seen as a strong benefit to improve efficiency and thus to reduce economic costs of surveillance. However, this assumption is a fallacy as this also automatizes the occurrence of false positives and proneness to errors of surveillance systems. The high complexity of such modalities triggers a wide range of both economic and social costs. In addition to the operational costs for analysing data, they trigger social costs such as a surveilled individual being repressed in some way. They entail higher economic costs for correcting errors in the surveillance system (if they are even recognised!), they reinforce the problem of social sorting and discrimination, and can lead to judicial errors that further boost economic (process costs) and social (erosion of trust) costs on a larger scale.

The quality of data is an important aspect to avoid false positives. However, the attempt to improve quality by gathering more detailed data may not achieve the desired result because it leads to an increase in complexity and can even foster proneness to error. As Hamacher and

Katzenbeisser demonstrate, the practice of pre-storing data for surveillance such as fostered by data retention to gather more data and improve predictability of crimes does not lead to better results.[6] On the contrary, the more data is gathered, the more complex the systems become and the higher the costs for correcting failure. The handling of surveillance data is a costly task. While pre-storing and collecting data are rather simple, filtering useful information is tricky and prone to errors.

5.3 SOCIAL COSTS OF SURVEILLANCE

5.3.1 Exclusion and discrimination

Anthony Amicelle, PRIO

The current centrality of security-focused technologies with surveillance capabilities is partly related to the belief that "monitoring the future of human beings is possible".[7] The aim to manage (in)security as well as to prevent criminal violence and political violence through databases increases the use of technologies that often get promoted as the solution to anticipate worst-case scenarios and to prevent catastrophic events from happening. The list of technologies is now huge, to the extent that one of the key issues at stake has been the contemporary "turn to data"[8] in favour of increasing the routine registering and mining of personal data to detect deviant behaviours and illegitimate actors. There are passenger name records for airports, electronic visas, biometric passports, communication technologies in financial services and so on. "The reduction of data storage costs and the increased ability of computer systems to analyze and integrate data mean that preemption is also applied to the gathering of intelligence: it is never clear what information might be useful, and so as much information as possible is collected."[9]

While the scope of surveillance is extremely broad, from telecommunication monitoring to drones, contemporary programs of surveillance mostly share the "preventive dimension". This dimension is also pervasive regarding consumer surveillance and customer relationship management.[10] With reference to the actors within the institutions of business and government, Oscar Gandy argues that the "sensory infrastructure" of surveillance is "no longer primarily oriented toward the production of an accurate impression or representation of the present or the recent past. Its lens is increasingly being focused on a strategic representation of the future. It is this distinction that makes all the difference between old and new forms of surveillance".[11] Although the appetite for personal data and this preventive

[6] Hamacher, Kay, and Stefan Katzenbeisser, "Public Security: Simulations need to replace conventional wisdom", in Proceedings of the New Security Paradigms Workshop (NSPW11), ISBN 978-1-4503-1078-9, ACM, 2011, pp. 115-124.
[7] Bigo, Didier, "Security, Surveillance and Democracy", in Kirstie Ball, Kevin Haggerty and David Lyon (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, New York, 2012, p. 283.
[8] Amoore, Louise, and Marieke De Goede, "Introduction. Data and the War by Other Means", *Journal of Cultural Economy*, Vol. 5, No. 1, January 2012, pp. 3-8.
[9] Salter, Mark B., "Surveillance", in J. Peter Burgess (ed.), *The Routledge Handbook of New Security Studies*, Routledge, New York, 2010, p. 191.
[10] Ball, Kirstie, Elizabeth Daniel, Sally Dibb and Maureen Meadows, "Democracy, surveillance and 'knowing what's good for you': the private sector origins of profiling and the birth of 'citizen relationship management'", in Kevin Haggerty and Minas Samatas (eds.), *Surveillance and Democracy*, Routledge, New York, 2010, pp. 111-126.
[11] Gandy, Oscar, "Statistical Surveillance: Remote Sensing in the Digital Age", in Kirstie Ball, Kevin Haggerty and David Lyon (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, New York, 2012, p. 128.

claim have been sometimes associated with illegal practices,[12] that is the logic of these new forms of surveillance which is related to potential social costs. "Such a [preventive] stance is all the more problematic as the contemporary orientation of existing and developing security technologies strongly leans towards the 'monitoring of the future', i.e. the privileging of pro-activity, prevention and profiling stance in the management of insecurity, to the detriment of the practices of criminal investigation and criminal justice, including the presumption of innocence, the right to a private life and so forth."[13] Consequently, there are numerous potential social costs from negative impact on the presumption of innocence to various forms of discrimination, social exclusion, social inequalities, self-censorship and inhibition. Social costs of surveillance can affect individuals and society more generally, as we indicate in the following paragraphs.

False positives and social damage

First, the issue of "false positives" represents a significant problem regarding counterterrorism policies based on watch lists and profiling. In connection with the use of watch lists, the category of false-positives covers individuals and entities that are not blacklisted but there is confusion between them and official suspects of terrorism, mainly with alerts triggered by homonymy.[14] Therefore, the false-positives can be affected by irrelevant restrictive measures. Potential errors are acknowledged at the European and United Nations level regarding the development of official blacklists[15] and assets freezing measures.[16] A false positive's bank account and financial transactions can be blocked until the end of the confusion between her and the "real" blacklisted individual.

The frequency of false positives particularly concerns risk managers in the banking sector. They do not hesitate to complain to the team of UN officials who follow the work of the UN Sanctions Committee and object to the lack of identification data for some entries on the UN list of terrorist suspects. Expressing their frustration during the implementation of sanctions (the freezing of funds), they underscored the fact that these lacunae increased "the risk that individuals whose names figure on the list not be identified and that sanctions be applied to individuals who were not targeted".[17] Moreover, some lists include erroneous information. According to a report from the American Justice Department, 24,000 individuals wrongly figure on the FBI's consolidated anti-terrorist list, which includes around 400,000 individuals, corresponding to more than one million names and aliases.[18] Some governments are also

[12] Bigo, Didier, and Pierre Piazza, "Les conséquences humaines de l'échange transnational des données individuelles", *Cultures & Conflits*, No. 76, December 2009, pp. 7-14.
[13] Jeandesboz, Julien, Didier Bigo, Philippe Bonditti and Francesco Ragazzi, *Security technologies and society: A state of the art on security, technology, borders and mobility*, INEX Deliverable D.1.1, PRIO, Oslo, 2008, p. 5.
[14] Ericson, R., "Ten Uncertainties of Risk-Management: Approaches to Security", *Canadian Journal of Criminology and Criminal Justice*, Vol. 48, No. 3, September 2006, pp. 345-357.
[15] Guild, E., "The Uses and Abuses of Counter-Terrorism Policies in Europe: The Case of the 'Terrorist Lists'". *Journal of Common Market Studies*, Vol. 46, No. 1, February 2008, pp. 173-193. Hayes, Ben, and Gavin Sullivan, *Blacklisted: Targeted sanctions, preemptive security and fundamental rights*, ECCHR: 10 years after 9/11 Publication Series, 2010.
[16] EBIC (European Banking Industry Committee), *Recommendations for improvements to EC regulations in the field of embargo measures and financial sanctions*, Brussels, August 2004. European Union, *Meilleures pratiques de l'UE en ce qui concerne la mise en œuvre effective de mesures restrictives*, Bruxelles, 15115/05, Novembre 2005. United Nations, *Recommandations figurant dans le huitième rapport de l'Équipe d'appui analytique et de surveillance des sanctions: position du Comité*, S/2008/408, New York, June 2008.
[17] Ibid., p. 8.
[18] US Department of Justice. Office of the Inspector General Audit Division, *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Process*, 2009.

aware of the problems with the commercial lists used by banks to screen their client relations and to detect financial transactions that are related to blacklisted individuals: "For a bank, investigation and evaluation are expensive things, thus very often if a name appears on a commercial list such as World Check, it will refuse this client's transaction without looking into it further. The problem is that the supplier of tools has no obligation to exercise vigilance vis-a-vis the information they draw from more or less trustworthy public sources and they do not regularly verify their data. For example, someone who had been removed from an official list can remain on the World Check list. There is a potential risk connected with the quality of information of those who sell these tools."[19]

In connection with official EU and UN "terrorist lists", the negative consequences are not only limited to financial mobility and economic problems. The damage to reputation and human mobility can also be affected to the extent that targeted sanctions include travel bans. Although there is no European nor UN official statistics on "collateral damages" of the blacklisting, the social cost of this approach is largely acknowledged.

> Of course, some individuals have been affected by false-positives cases because they have the same name as blacklisted persons; and it is not only true for the UN list, it is also true for the OFAC [US] list, may be less for the EU list but there are many people who have had some difficulties to register themselves to the high school or to the university in order to continue their studies. Some of them also have had problems on a daily basis to simply live their life because they have the name of a blacklisted individual. As you know, there are much more Mohamed than Jean-Paul on the 'terrorists blacklists'. This situation can lead to discrimination and that is a significant issue. We have some problems with names, with the complete names of individuals and the 'nicknames' that are used in the Middle East. In Afghanistan, most of the people have only one official name and many of them have the same name. We often do not know their date of birth, their address and there are some problems of translation. Of course, that is a real problem for banks. Let me clarify, the problem is not the blacklisted individual who tries to open a bank account in Los Angeles. The problem is the innocent individual who has the same name of the blacklisted individual, may be not exactly the same age or the same address but you cannot be sure that he is not the blacklisted.[20]

Furthermore, EU officials underline that further identification data on blacklisted individuals can reduce negative consequences on false positives, but it cannot completely eradicate potential errors.[21]

Similarly, airline no-fly lists have been publicly criticised for apparent racial profiling and numerous false positives – both Nelson Mandela and the late Senator Edward Kennedy were inclused on no-fly lists, for instance.[22] The problem of false-positives at airports also exists with profiling and data mining tools designed to detect suspicious behavior patterns. "The problem is that even if data mining identifies some terrorists correctly, it is effective only if it doesn't have too many false positives – people who fit the profile but who aren't terrorists. More than two million people fly each day worldwide. A data mining program to identify terrorists with a false positive rate of 1 percent (which would be exceptionally low for such a

[19] Interview with a British official, London, January 2009.
[20] Interview with a UN official, April 2009, New York.
[21] European Union, *Meilleures pratiques de l'UE en ce qui concerne la mise en œuvre effective de mesures restrictives*, Brussels, 15115/05, November 2005.
[22] Adey, P., "Facing Security Airport: Affect, Biopolitics, and the Preemptive Securitisation of the Mobile Body", *Environment and Planning D: Society and Space*, No. 27, February 2009, pp. 274-295. Monahan, Torin, "Surveillance and Terrorism", in Kirstie Ball, Kevin Haggerty and David Lyon (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, New York, 2012, p. 286.

program) would flag more than twenty thousand false positives every day. This is quite a large number of innocent people who will be wrongly snagged by the system."[23] Hence, the social costs of those profiling systems can be significant. The use of huge databases and data mining software to perform behavioural analysis of the population without particular suspicion partly reverses the principle of the presumption of innocence.

Categorical suspicion and discrimination

Automated profiling refers to socio-technical mechanisms that are based on risk management and social sorting to discriminate between one group and another.[24] The classification and categorisation of population are not inherently bad to the extent that such processes can be implemented to better distribute resources in society according to individuals' needs. However, the implications of social sorting as a discriminatory mechanism can be both positive and negative. Numerous scholars show how surveillance as social sorting can reproduce and reinforce social inequalities.[25] Indeed, David Lyon uses the notion of "digital discrimination" to define surveillance practices in which "flows of personal data – abstracted information – are sifted and channeled in the process of risk assessment, to privilege some and disadvantage others, to accept some as legitimately present and to reject others".[26] With regard to social sorting that underlines the categorising enabled by new statistical and software practices, Oscar Gandy insists on statistical surveillance and he emphasises how statistical discrimination helps to reproduce and legitimise social inequalities, often along racial lines.[27] Statistical discrimination characterises "a decision to exclude or deny opportunity to an individual on the basis of the attributes of the group to which he or she is assumed to belong. For example, statistical discrimination occurs when an employer refuses to hire an African American male because he is assumed to be ignorant, dishonest, lazy, or criminally inclined on the basis of generally held, and perhaps statistically validated, estimates of the distribution of those traits among African Americans. As a result, what could be treated as illegal racial discrimination is routinely justified as a legitimate and inherently *rational act.*"[28] Consequently, people's life chances may partly depend on social sorting.

Such a "categorical suspicion" is also pervasive regarding surveillance practices that are related to counterterrorism.[29] In the aftermath of 11 September 2001, there has been some degree of error regarding decisions about individuals that have been made on the basis of their membership in groups. Indeed, the targeting of Arab and Muslim minorities has been disproportionate and unjustified in several countries.[30] As a result, while intrusion is a major problem of current surveillance systems regarding privacy, exclusion is also a key issue at stake regarding social division. Although the classic argument "if you've got nothing to hide

[23] Solove, Daniel, *Nothing to Hide. The False Tradeoff between Privacy and Security*, Yale University Press, Yale, 2011, p. 188.
[24] Surveillance Studies Network, *A report on the surveillance society*, Information Commissioner's Office, Wilmslow, 2006. Lyon, David (ed.), *Surveillance as social sorting: Privacy, risk and digital discrimination*, Routledge, London, 2003.
[25] For an overview, see Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2007.
[26] Lyon, David (ed.), *Surveillance as social sorting: Privacy, risk and digital discrimination*, Routledge, London, 2003, p. 74.
[27] Gandy, Oscar, *Coming to terms with chance: Engaging rational discrimination and cumulative disadvantage*, Ashgate, Farnham, 2009.
[28] Gandy, Oscar, "Statistical Surveillance: Remote Sensing in the Digital Age", in Kirstie Ball, Kevin Haggerty and David Lyon (eds.), Routledge Handbook of Surveillance Studies, Routledge, New York, 2012, pp. 126.
[29] Marx, Gary T., *Undercover: Police Surveillance in America*, University of California Press, Berkeley, 1988.
[30] Bigo, Didier, Laurent Bonelli and Thomas Deltombe (eds.), *Au nom du 11 septembre… Les démocraties à l'épreuve de l'antiterrorisme*, La Découverte, Paris, 2008.

you've got nothing to fear"[31] plays a significant role in the justification of surveillance programs, this argument is theoretically wrong regarding discrimination through categorical suspicion to the extent that there are disproportionate consequences on specific groups.[32] Categorical suspicion tends to increase negative effects on individuals who are targeted as members of groups at risk.[33]

Marginalising effects and social inequalities

Torin Monahan also suggests that social sorting can reinforce "marginalizing effects" by selectively targeting those of lower social status for the most invasive forms of monitoring.[34] He argues that there is unequal exposure to different surveillance systems based on social characteristics. Hence, invasive drug-testing and real-time location tracking are two examples of "marginalizing surveillance" to the extent that these monitoring practices are mainly reserved "for workers with the lower status and income levels".[35] Nelson Arteaga Botello also shows how the implementation of electronic surveillance in several Latin American countries is distributed unequally according to income level. Electronic surveillance is a privilege for powerful and wealthy groups to control the entrance of their neighborhoods to the extent that residential and commercial properties are securitized while poor urban spaces are much less surveilled. Moreover, electronic surveillance is used to contain "marginalized and excluded groups within and between neighborhood, business and consumer spaces, who are considered the source of criminal violence in Latin American societies. This has generated a group of "security archipelagos" that further fragment the mega-cities of the region. In these archipelagos, different forms of accessing and living in the city for groups and diverse individuals are established. The installation of large surveillance systems that feed enormous and costly data bases established new forms of organization and sorting which directly impact in the way in which the citizenry is structured and lives".[36]

Inhibition

Inhibition and the mainstreaming of behaviour represent another potential social cost of surveillance systems to the extent that "you act differently if you know that traces you leave will be processed".[37] "Pervasive monitoring of every first move or false start will, at the

[31] Solove, D., "'I've got nothing to hide' and other misunderstandings of privacy", *San Diego Law Review*, Vol. 44, No. 475, July 2007, pp. 745-772.
[32] Lyon, David, Surveillance Studies: An Overview, Polity Press, Cambridge, 2007.
[33] Bigo, Didier, Laurent Bonelli and Thomas Deltombe (eds.), *Au nom du 11 septembre… Les démocraties à l'épreuve de l'antiterrorisme*, La Découverte, Paris, 2008.
[34] Monahan, T., "Editorial: Surveillance and inequality", *Surveillance & Society*, Vol. 5, No. 3, September 2008, pp. 217-226.
[35] Ibid., p. 220. Staples, William, *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*, Rowman & Littlefield, Lanham, MD, 2000. Campbell, N., "Technology of Suspicion: Coercion and Compassion in Post-Disciplinary Surveillance Regimes", *Surveillance & Society*, Vol. 2, No. 1, January 2004, pp. 78-92. Fisher, Jill, "Indoor Positioning and Digital Management: Emerging Surveillance Regimes in Hospitals", in Torin Monahan (ed.), *Surveillance and Security: Technological Politics and Power of Everyday Life*, Routledge, New York, 2006, pp. 77-88.
[36] Arteaga Botello, Nelson, "Surveillance and Urban Violence in Latin America: Mega-Cities, Social Division, Security and Surveillance", in Kirstie Ball, Kevin Haggerty and David Lyon (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, New York, 2012, p. 265.
[37] De Hert, Paul, and Serge Gutwirth, "Regulating Profiling in a Democratic Constitutional State?", in Serge Gutwirth and Mireille Hildebrandt (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer science, Brussels, 2008, p. 291.

margin, incline choices toward the bland and the mainstream."[38] From video surveillance to telecommunication information processing, surveillance can inhibit freedom from engaging in various activities if individuals experience privacy disutility from being monitored although these activities can be socially desirable.[39] This inhibitory effect of surveillance "can make our behaviour less spontaneous and make us more self-conscious about where we go and what we do" and this effect can be particularly strong regarding engagement in political protest.[40] As a result, surveillance can undermine social and democratic activities.

Privacy, societal harm and erosion of trust

Finally, surveillance systems can also affect social dynamics and society more generally regarding power relationships between citizens, governmental agencies and business institutions. Indeed, the main privacy issues might be not where they are supposed to be. Critical studies are often characterised in looking for issues in terms of injuries to the individual while not questioning wider societal impact.[41] Most privacy-surveillance problems lack dead bodies and sensationalistic cases – such as blacklists – but it does not mean that privacy issues could not be harmful for individuals and for society as a whole. Daniel Solove studies two cases of information dissemination. "For example, after the September 11 attacks, several airlines gave their passenger records to federal agencies in direct violation of their privacy policies [counter-terrorism purposes] [...] A similar problem surfaces in another case, Smith v. Chase Manhattan Bank. A group of plaintiffs sued Chase Manhattan Bank for selling customer information to third parties in violation of its privacy policy, which stated that information would remain confidential [commercial purposes]".[42] Both groups of plaintiffs were ultimately dismissed, but Solove argues that court rulings reveal less the absence of privacy problems than the difficulty with the legal system in "recognizing harms that do not result in embarrassment, humiliation, or physical or psychological injury".[43] His two case studies refer to the problem of secondary use regarding information dissemination and information processing. "Secondary use involves data collected for one purpose being use for an unrelated purpose without people's consent."[44] Solove acknowledges that such a privacy problem frequently does not give rise to material (i.e., financial or physical) nor psychological injuries but, according to him, it is still harmful. The harmful dimension tends to be a structural one because it concerns not so much particular individuals as the population as a whole.

The harm is structural because it consists of a power imbalance between individuals and business institutions (banks, airlines and so on) and between citizens and their government. As Solove states for his example regarding airline passengers, the issue is not to question whether people know the privacy policies of these companies. The issue is to understand that in any case there is a "social value in ensuring that companies adhere to established limits on

[38] Cohen, Julie, "Examined Lives: Informational Privacy and the Subject as Object", *Stanford Law Review*, No. 52, May 2000, p. 1426.
[39] Song, A., "Technology, Terrorism, and the Fishbowl Effect: An Economic Analysis of Surveillance and Searches", *The Berkman Center for Internet & Society Research Publication*, No. 5, September 2003, pp. 1-26.
[40] Solove, Daniel, *Nothing to Hide: The False Tradeoff between Privacy and Security*, Yale University Press, Yale, 2011, p. 179.
[41] Den Boer, Monica, and Jelle Van Buuren, "Security clouds: towards an ethical governance of surveillance in Europe", *The Journal of Cultural Economy*, Vol. 5, No. 1, January 2012, pp. 85-103.
[42] Solove, D., "'I've got nothing to hide' and other misunderstandings of privacy", *San Diego Law Review*, Vol. 44, Issue 4, November 2007, p. 745.
[43] Ibid.
[44] Ibid.

the way they use personal information. Otherwise, any stated limits become meaningless, and companies have discretion to boundlessly use data."[45] Here, the social cost of surveillance is related to the possible erosion of trust between commercial establishments and consumers as well as between law enforcement agencies and the population. The issue is not strictly limited to know whether governmental and business institutions should be allowed to police individuals but whether they can do it without a proper mechanism of oversight and to what extent they can use data. "Social relationships depend on trust and permitting ourselves to undermine it… is like slow social suicide."[46]

5.3.2 Surveillance and conformity

Kirstie Ball, Open University

This section of the report considers whether and how conformity and its consequences can be considered a social cost of surveillance. The *Oxford English Dictionary* defines conformity as "compliance with rules or general custom". Since one of the primary aims of surveillance is to ensure governance, management or social control – in other words, to implement rules concerning accepted behaviours – conformity is certainly an expected outcome of surveillance practices. The section begins by outlining the different theoretical bases by which increased conformity and its consequences could be considered an outcome of a surveillance practice. Three perspectives are briefly reviewed: those which examine the relationship of surveillance practices with bureaucratic rationality; categorisation and panopticism. It then reviews the empirical evidence which examines conformity as an outcome of surveillance and observes any further consequences thereof.

Surveillance and conformity: theoretical perspectives

The problematic of surveillance and conformity stems from the historical development of the surveillance society, particularly its grounding in modern, bureaucratic organising practices. Today's "surveillance society"[47] emerged from a complex of military and corporate priorities, intimately linked with developments in the natural sciences, that were nourished through the active and "cold" wars that marked the 20th century. Their evolution and growth were dialectical rather than linear; each conglomeration of networks and actors was and is mutually constituted from, by and through the other. This synergy was made possible by the "complementarities" of government and corporate "needs". In 18th and 19th century Europe, for example, rural populations became urbanised and worked in factories or as outsourced home workers. Bureaucracies emerged so that national and local governments could manage the population, the information generated by their activities and their behaviour. For business organisations, information about customers, markets, production and employees was required. For governments, information about citizens, their tax, welfare, immigration, educational, health status and many other things was important. And as new urban forms became havens for theft, prostitution, gambling and drunkenness, public order and behavioural control increased in importance. When bureaucracies became computerised, new insights into the activities of customers, markets, employees and citizens were made possible, and modern surveillance was born. There is nothing conspiratorial about this process: today's surveillance society emerged in unpredictable, uncontrollable, non-linear ways – as Haggerty and

[45] Ibid.
[46] Surveillance Studies Network, *A report on the surveillance society*, Information Commissioner's Office, Wilmslow, 2006, p. 6.
[47] Lyon, David, *Surveillance Society: Monitoring Everyday Life*, Open University Press, Milton Keynes, 2001.

Ericson[48] remind us, there were a multiplicity of causes and effects. But it is not at all accidental that the vast majority of the technologies that shape our lives today, the "winners" of thousands of internecine battles for supremacy, are those that extend the social control of dominant institutions over designated others, making the other visible in ever more novel ways.[49]

Surveillance, conformity and bureaucratic rationality

The development of the modern bureaucracy is hence fundamental to the development of the surveillance society. Its cornerstone is the principle of rationality which requires a degree of conformity in order to operate. Decision-making within the bureaucratic ideal type depends, first, upon knowledge of files which contain information about the bureaucracy and its activities and, second, upon rational discipline which aims to eliminate subjective and irrational human qualities. The bureaucratic official's sphere of competence is clearly defined by legal rules; rigorous training, rational discipline by seniority and qualifications which indicate authority.[50] The individual is merely a cog in the administrative machine. Bureaucratic principles hence reach beyond systems and processes to the employees and others that surround the bureaucracy. Mayer argues "precision, speed, unambiguity, knowledge of the files, continuity, discretion, unity, strict subordination, reduction of friction and of material and personal costs- these are raised to the optimum point in the strictly bureaucratic administration and especially in its bureaucratic form" [51] and Dandeker states "as surveillance involves a deliberate attempt to monitor and/or supervise objects or persons it is to be found in its most developed form in formal organizations, which possess an explicitly stated goal, together with a formal administrative structure for achieving those goals, including arrangements for maintaining the boundaries and passages between the organization and outsiders"[52]

Conformity is an outcome of bureaucratic activities because, from a social point of view, bureaucracy, by its nature, is non-inclusive.[53] Unlike total organisations, such as prisons, to interact with governmental or business bureaucracies is to interact with a rationalised system of codes and categories which is divorced from the totality of one's lifeworld. Organisational conduct immediately becomes depersonalised and behaviour becomes standardised. Consumers, citizens and employees do not interact with these organisations in their full-blown cognitive, emotional and social complexities. The segmentation of life into separate spheres is a prerequisite for engaging with them. Separation and conformity become key because the idea of self-monitoring and the objectification of one's own activities as a consumer, citizen or employee would be impossible without them.

[48] Haggerty, Kevin, and Richard Ericson, *The New Politics of Surveillance and Visibility*, University of Toronto Press, 2006.
[49] Mosco, Vincent, *The Political Economy of Communication*, Sage, London, 1996. Mosco, Vincent, *The Digital Sublime: Myth, Power, and Cyberspace*, MIT Press, Cambridge, 2004. Williams, Raymond, *The Long Revolution*, Columbia University Press, New York, 1961. Williams, Raymond, *Culture and Materialism: Selected Essays*, Verso, London, 1980.
[50] Weber, Max, *The Protestant Ethic and the Spirit of Capitalism*, Allen and Unwin, 1956.
[51] Mayer Jacob P., *Max Weber and German Politics: A Study in Political Sociology*, Faber and Faber, London, 1944, p. 214.
[52] Dandeker, Christopher, *Surveillance, Power and Modernity*, Polity, Cambridge, 1990, p. 38.
[53] Kallinikos, Yiannis, "The social foundations of the bureaucratic order", *Organization*, Vol. 11, No. 1, 2004, pp. 13-36.

Surveillance, conformity and classification

Following the work of Bowker and Starr,[54] classification is a process which is also closely associated with surveillance practice. This is because surveillance practices are nearly always targeted at identifying and classifying behaviours, things or phenomena which fit into some previously defined phenomenological taxonomy. For example, customer relationship management practitioners use data analytics to determine how patterns of customer behaviour produce different consumer profiles which relate to different types of customers. They then seek to validate and test these profiles against further consumer behaviour data so that they can better target offerings to consumers. In their groundbreaking work, Bowker and Starr[55] discuss examples of disease, race and work based classification systems. They argue that these systems are infrastructural, in that they co-create over-arching structures to live by as well as being embedded within and reproduced by social practices. This renders the individual unable to distinguish the effects of the classification system in which they are implicated as they have no basis for comparing it to others. Bowker and Starr's[56] empirical work demonstrates that the boundaries of classificatory schemes reflect the political positions and insights of those charged with developing these schemes. They also imply that conformity is an undesirable consequence of classification by highlighting how individual trajectories run the risk of being twisted and torqued with classificatory trajectories. They warn: "it has become easier for the individual to act and perceive him or herself as a completely naturalised part of the 'classification society' … as we are socialised to become that which can be measured by our increasingly sophisticated measurement tools, the classifications increasingly naturalise across a wider scope".[57]

Surveillance, conformity and panopticism

This is perhaps the theoretical perspective which is most commonly associated with surveillance and conformity. In the 19th century, Jeremy Bentham devised a spatial strategy of surveillance, the Panopticon, an architectural, technological and discursive formation that allowed the few to scrutinise the many. The Panopticon was an idea, a concept and model of a new mode of control: it would reform lawbreakers by confining them in new institutions known as penitentiaries.[58] The genius of the design lay in the fact that those targeted were always visible to their controllers, but would never themselves know when and whether they were being observed. This, plus 24-hour isolation and religious training, would force the criminalised person to internalise discipline and self control. This clever system, it was thought, would supplement, ideally replace, external social controls with internal mechanisms. By instilling the bourgeois conscience in the offender, he (or she – lower class women and girls, particularly their sexuality, were primary targets of the new discipline) would learn new ways of behaving and punish themselves for transgressions, thereby lessening the need for legitimacy-threatening displays of coercion by the state. Institutions and regimes to discipline and train lawbreakers, the young and the mentally disordered became popular. Foucault's discussion of the panopticon associates it with forms of population governance which instil an internalisation of discipline – behavioural norms, in effect – through a microphysics of power. In this context, conformity is seen as a desirable

[54] Bowker, Geoffrey, and Susan Leigh Starr, *Sorting Things Out: Classification and its Consequences*, MIT Press, Cambridge, MA, 1999.
[55] Ibid.
[56] Ibid.
[57] Ibid., p. 326.
[58] Foucault, Michel, *Discipline and Punish*, Penguin, Harmondsworth, 1977.

objective for governance but one which is inherently and fundamentally contested and disrupted by power relations at every level.

Conformity as a cost?

The aforementioned theoretical perspectives highlight that conformity is a necessary feature of surveillance practices and even has some desirable characteristics. Applying surveillance practices to achieve conformity, whether that be through the generation of more accurate consumer profiles, better census data or reduced crime rates, certainly benefit the possessor of surveillance capacity. In relation to these examples, it may also be fair to say that certain classes of consumer may benefit from better targeted offerings; citizens from more accurate representation to government and from reduced victimisation and fear of crime. Indeed Bowker and Starr persuasively argue that classificatory schemes silently constitute the social world. Nevertheless, from either a Weberian or Foucauldian perspective, conformity can be problematised as it relates to non-inclusive organising practices. One may conform within a domain and then step outside to avoid its influence, hence making surveillance induced conformity inherently contestable. Furthermore, examples of conformity *as resistance* can also be found in discussions of surveillance and conformity in the GDR[59] and in a discussion of Švejkism as a resistant strategy in the workplace.[60] Švejkism refers to a character in Jaroslav Hašek's novel *The Good Soldier, Švejk* who resists through subtle forms of subversion which are invisible to those in charge – in other words, he only *appears* to conform. In spite of many theoretical perspectives, empirical work which examines the consequences of surveillance-induced conformity is scarce. This work is reviewed in the following pages. It appears in a number of social domains: the workplace, schools, medicine, social media, sports coaching and public housing.

Workplace

The workplace is perhaps the most obvious domain where surveillance-related conformity can be observed to incur not only social but economic costs. Employee surveillance practices, most notably the electronic monitoring of employee performance where conformity with performance standards is continually assessed, can be detrimental to employees for a number of reasons. First, because privacy can be compromised if employees do not authorise the disclosure of their information, and it is then broadcast to unknown third parties.[61] Second, because like all surveillance technologies, employee surveillance technologies can exhibit function creep. This is because monitoring technologies can sometimes yield more information than intended, and management need to avoid the temptation to extend monitoring practice without consulting employees first.[62] This is particularly stressful for employees if the information is being used in decisions about pay or promotion. Third, if employees realise their actions and communications are monitored, creative behaviour may be

[59] Pfaff, Steven, "The limits of coercive surveillance: Social and penal control in the German Democratic Republic", *Punishment and Society*, Vol. 3, No. 3, 2001, pp. 381-407.
[60] Fleming, Peter, and Graham Sewell, "Looking for the good soldier 'Švejk': Alternative modalities of resistance in the contemporary workplace", *Sociology*, Vol. 36, No. 4, 2002, pp. 857 - 873.
[61] Zweig, David, and Jane Webster, "Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems", *Journal of Organizational Behavior*, Vol. 23, No. 5, 2002, pp. 605 - 633.
[62] McCahill, Michael, and Clive Norris, "Watching the workers: Crime, CCTV and the workplace", in P. Davis, P. Francis and V. Jupp (eds.) *Invisible Crimes: Their Victims and their Regulation.* Macmillan, London, 1999.

reduced if they are worried about monitoring and judgement.[63] Fourth, exacting surveillance sends a strong message to employees about the kind of behaviours the employer expects or values, simply by the tasks it chooses to monitor. Research finds monitored tasks are deemed more valuable or critical than non-monitored ones, so workers will pay greater attention to those tasks and afford greater importance to the behaviours monitoring reinforces.[64] Additionally, the form monitoring takes also gives messages about the importance of quality over quantity and the importance of working as a team.[65] This can produce "anticipatory conformity" – where employees behave in a docile and accepting way, and automatically reduce the amount of commitment and motivation they display.[66] The interaction of surveillance practices with other forms of management, and its effects on conformity is highlighted by Hønneland[67] who examined fishermen working in the Barents Sea fisheries. They attributed their conformity with established fishing quotas not only to the exacting surveillance systems to which they were subject but to the legitimacy of the management bodies which governed the fishery, demonstrating the socio-technical nature of surveillance.

Finally, excessive monitoring can sometimes produce the behaviour it was designed to prevent. If workers perceive surveillance practices as an intensification and extension of control, it is likely that they will try to subvert and manipulate the boundaries of when, where and how they are measured.[68] Studies of call centres demonstrate that intense surveillance increases resistance, sabotage and non-compliance with management.[69] Here, workers are extensively monitored not only in terms of their quantitative outputs, but also their manner on the phone and their overall competence. They work their way around surveillance by manipulating measures by dialling through call lists, leaving lines open after the customer has hung up, pretending to talk on the phone, providing a minimal response to customer queries and misleading customers. Where call centre managers are also under surveillance, they sometimes collude with workers to produce the desirable results.

Schools

Schools have an important role as institutions of conformity through their numerous disciplinary mechanisms such as the school bell, the timetable, school uniform, classroom layouts, curricula and assessment.[70] In a review of literature on surveillance in schools, Taylor reports that the recent rise in the use of multiple surveillance technologies in schools

[63] Stanton, Jeffrey M., "Reactions to employee performance monitoring: Framework, review and research directions", *Human Performance*, Vol. 13, No. 1, 2000, pp. 85-113.
[64] Brewer, Neil, "The effects of monitoring individual and group performance on the distribution of effort across tasks", *Journal of Applied Social Psychology*, Vol. 25, No. 9, 1995, pp. 760 – 777. Carayon, Pascale, "Effects of electronic performance monitoring on job design and worker stress: results of two studies", *International Journal of Human Computer Interaction*, Vol. 6, No. 2, 1993, pp. 177 – 190. Larson, James R., and Christine Callahan, "Performance monitoring: How it affects work productivity", *Journal of Applied Psychology*, Vol. 75, No. 5, 1990, pp. 530 – 538.
[65] Brewer, Niel, and Tim Ridgeway, "Effects of supervisory monitoring on productivity and quality of performance", *Journal of Experimental Psychology: Applied*, Vol. 4, No. 3, 1998, pp. 211-227.
[66] Zuboff, Shoshana, *In the Age of the Smart Machine* New York: Basic Books, 1988.
[67] Hønneland, Gerd, "Compliance in the Barents Sea fisheries: How fishermen account for conformity with rules", *Marine Policy*, Vol. 24, 2000, pp. 11-19.
[68] McCahill, Michael and Clive Norris, "Watching the workers: Crime, CCTV and the workplace", in P. Davis, P. Francis and V. Jupp (eds.), *Invisible Crimes: Their Victims and their Regulation*, Macmillan, London, 1999.
[69] Callaghan, George and Paul Thompson, "We recruit attitude: The selection and shaping of routine call centre labour", *Journal of Management Studies*, Vol. 39, No. 2, 2002, pp. 233-254.
[70] Taylor, Emmeline, "Surveillance in Schools", in Kirstie Ball, Kevin Haggerty, David Lyon (eds.), *The Routledge Handbook of Surveillance Studies*, Routledge, London, 2012.

"undermines privacy, erodes trust, makes pupils feel criminalized and can have a 'chilling effect' on creativity and interaction".[71] Piro reports that the increased use of surveillance cameras in schools has caused some teaching trade unions in the United States to become concerned about its impact on the quality of teaching practice when it is used in the classroom.[72] He cites "teacher rapport with students, privacy, suppression of academic creativity and spontaneity"[73] as some of the key issues. As with the workplace, his concern is with the excessive disciplinarianism which is symbolised by the presence of cameras and other surveillance tools. These concerns are countered by head teachers' assertions that the presence of cameras in the public areas of schools improve student behaviour and makes schools safer places to learn. Media reports of school shootings in the US are nearly always referred to in these debates. Nevertheless, Taylor argues for a measured approach and reports that research has observed the negative impact of excessive surveillance on the social life within school as follows:

> Visual surveillance can have a detrimental impact on associational activity, curtailing creativity, innovation and experimental modes of expression. … Furthermore, surveillance has initiated a process of 'distanciation' whereby pupils are increasingly denied the opportunity for social interaction. Surveillance, whether it is facial recognition replacing registration, or fingerprinting to borrow library books, interrupts pupils' traditional patterns of 'sociation' or 'face-to-face' interaction with parents, teachers, and their peers.[74]

Social media

Although there have not been many studies of the surveillance and conformity within social media, users have produced fascinating insights.[75] In an interview study of younger Facebook users, they discovered that when users felt they had too many friends, they used conformity as a strategy to protect their privacy. In other words, they self-censored to maintain their privacy. They were concerned more about other social media users knowing too much about them, however, than Facebook itself, which is arguably the greater threat.

Medicine

Critical studies of medicine and medical practices have examined the way in which treatments impose particular norms on patients and have them conform in new ways. Bell[76], in a feminist study of therapies administered for Anorexia patients, argues that the treatment forces the patient to conform to a particular type of femininity that may not be helpful for the patient.

Sports coaching

---

[71] Ibid., p. 229.
[72] Piro, Joseph M., "Foucault and the architecture of surveillance: Creating regimes of power in schools, shrines and society", *Educational Studies: A Journal of the American Educational Studies Association*, Vol. 44, 2008, pp. 30-46.
[73] Ibid., p. 31.
[74] Taylor, Emmeline, "Surveillance in Schools", in Kirstie Ball, Kevin Haggerty, David Lyon (eds.), *The Routledge Handbook of Surveillance Studies*, Routledge, London, 2012, p. 230.
[75] Brandtzæg, Petter B., Marika Lüders and Jan H. Skjetnem, "Too many Facebook 'friends'?: Content sharing and sociability versus the need for privacy in social network sites", *International Journal of Human-Computer interaction*, Vol. 26, 2010, pp. 1006 - 1030.
[76] Bell, Mebbie, "Re/Forming the anorexic 'prisoner': Inpatient medical treatment as the return to panoptic feminity", *Cultural Studies ⇔ Critical Methodologies*, Vol. 6, No. 2, 2006, pp. 282-307.

In an in-depth study of junior swimming teams and their coaches, Lang further explores the social cost of surveillance- induced conformity.[77] There is a history of research within sports studies which examines sports discipline and the production of the compliant body[78] . Lang concludes that the depth and extent of visibility, monitoring and surveillance involved damages the social and 'fun' side of the sport, as well as the relationships between coaches and swimmers.[79] She observes the "scientific" nature of training regimes which were designed to produce compliant athletes that monitor, guard and discipline themselves. Alongside training regimes and the monitoring of performance, diet and weight, swimmers are subject to the physical gaze of the coach in the pool and even analysis of underwater camera footage. A hierarchy of surveillance results as coaches are also monitored by an external body as well as by their peers, and are constantly on their guard against allegations of child abuse. The constant climate of surveillance and scrutiny, dominated by conformity with either training programmes or coaching standards, precluded coaches and swimmers from engaging in a relationship which emphasised pastoral care as well as performance.

Public housing

The final example is from a study of public housing by Monahan.[80] He compared the use of technological surveillance practices in two different types of housing development: a public housing estate and an affluent gated community. Both sites were in Arizona. Increased conformity was only observed in the affluent gated community, as residents felt that they had to regulate their appearance and behaviour because of surveillance technologies. They were more wary of where they walked on the complex, or what they had in their front yards, for example. One respondent commented, "If you have cameras everywhere, you will create robots."[81]

By contrast, the experience of residents in the public housing complex was that surveillance provided little protection from outside threats and occasionally the security guards used it to police their behaviour. Therefore, within the affluent gated community, surveillance wove into the social fabric to re-enforce already existing norms to a more intense degree, with residents complying accordingly. As compliance was enforced in the public housing complex, surveillance was less welcome and created more problems than it solved, similar to reports in the workplace surveillance literature.

---

[77] Lang, Melanie, "Surveillance and conformity in competitive youth swimming *Sport*", *Education and Society* Vol. 15 No. 1, 2010, pp. 19 - 37.

[78] Aycock, Alan, "The confession of the flesh: disciplinary gaze in casual bodybuilding", *Play and Culture*, Vol. 5, No. 4, 1992, pp. 338-357. Carlisle Duncan, Margaret, "The politics of women's body images and practices; Foucault, the Panopticon and 'Shape' magazine", *Journal of Sport and Social Issues*, Vol. 18, 1994, pp. 48- 65. Markula, Pirkko H, "Firm but shapely, fit but sexy, strong but thin: the postmodern aerobicising female bodies", *Sociology of Sport Journal*, Vol. 12, No. 4, 1995, pp. 424-453. Chapman, Gwen E., "Making weight: Lightweight rowing, technologies of power and technologies of the self", *Sociology of Sport Journal*, Vol. 14, No. 3, 1997, pp. 205-223.

[79] Lang, Melanie, "Surveillance and conformity in competitive youth swimming", *Sport, Education and Society* Vol. 15, No. 1, 2010, pp. 19-37.

[80] Monahan, Torin, "Electronic fortification in Phoenix: Surveillance technologies and social regulation in residential communities", *Urban Affairs Review*, Vol. 42, No. 2, 2008, pp. 169-192.

[81] Ibid., p. 185.

Conclusion

In 2006, Surveillance Studies Network questioned whether a society which relied on surveillance to get things done would be committing a slow social suicide. The theoretical work covered indicated that increased conformity was a likely feature of surveillance practice and empirical material presented highlights its social cost. Surveillance-related conformity seems to damage the quality of social relations within specific social domains. The following phenomena, as reported in the literature, can be considered the social costs of surveillance related conformity:

- threats to worker privacy, a reduction in creative employee behaviour, anticipatory conformity and disengagement, increase in worker stress, a focus on completing only monitored tasks and increased resistance and sabotage in the workplace;
- a decline in the quality of interactions between teachers and pupils in schools, in terms of rapport with students, trust, spontaneity and creativity in the class room;
- a decline in the quality of social interactions between pupils and each other, in terms of new forms of self expression and creativity at school;
- self-censorship in social media by young people;
- a pressure to conform with gender norms in the treatment of anorexia, which may not be appropriate or helpful for the patient;
- a decline in the importance of pastoral care in the coaching of junior sports people;
- increased awareness of public appearance and behaviour in gated housing projects.

In making these assertions, we note that surveillance practices are woven into the social fabric and may enhance or intensify norms which are already operant in any one particular domain. Furthermore, it is also important to note that each of the empirical examples cited featured a very direct and overt relationship between the individual and the surveillance practices to which they were subject. It is easy to identify the impact of surveillance in enclosed spaces such as schools, workplaces, sports complexes, medical facilities and housing schemes. It is unclear as to whether such results would apply if the individual was not aware that they were under surveillance, as is the case in consumer or communications surveillance, where the relationship between watcher and watched is more intermediated and distanciated.

5.4 ECONOMIC COSTS OF SURVEILLANCE TECHNOLOGIES

Dara Hallinan, Michael Friedewald, Frauenhofer ISI

Introduction

The evaluation of the financial impact of surveillance technologies is notoriously difficult. Whilst it is possible to identify and evaluate certain limited first-level costs, for example, the costs of the technical installations themselves, any broad cost analysis is difficult, if not impossible, for at least two main reasons.

First, the reasoning and arguments for and against the installation of a certain technical solution take place in a context in which the provision of security and even the prevention of terrorism have to be weighed against the value and integrity of civil liberties. These themes do not lend themselves either toward definition, quantification or to expression in economic terms. Indeed, it is apparent that, in any case in which civil liberties may be impacted, any

financial impact assessment should come only following strict evaluation of its necessity and proportionality in a democratic society.

Second, the uncertainties involved, for example, the assumptions that must be made regarding terrorist motivation and activity, are huge. Accordingly, there is very little hard evidence from which to evaluate economic impact – indeed, as will be mentioned in the cases below, attempts to populate such concepts with figures often lead to rather unpleasant equations, for example, the necessity of putting a specific price on a human life.

Despite the above difficulties, considering the financial impact and cost of surveillance technologies is a valuable perspective. First, money is also a social resource; once a decision has been made to engage surveillance to a specific end, it is valuable to see that money is spent cost efficiently and proportionally toward that end. Further, as a social resource, its allocation, both in planning and implementation, not only reflects values implicit in the decision-making and social balancing process (money spent on surveillance and security is money not spent elsewhere), but will also play a role in the final shape and impact of the funded object. Finally, surveillance, security and technology are not only political concepts and instruments, but are also the focus of significant industrial interests. The consideration of the financial impact of surveillance technologies offers a unique prism through which to observe the engagement and consequences of the engagement of industry and politics.

With this in mind, we approach the issue of the financial impact of surveillance technologies using prominent cases where the public interest was high enough to initiate a public assessment of costs. For the majority of less prominent security solutions, especially when installed by private companies, there is only little information available publicly. In the first case, we focus on a specific security and surveillance technology – the body scanner used in one specific location – the airport, generally in response to one form of threat – terrorism. In the second case, we broaden our focus to consider the EUROSUR proposal, a proposal which would involve the set up of a wide-scale international surveillance system, functioning internationally, employing a number of technologies and communication networks and aimed at the simultaneous achievement of a range of goals.

Case study 1: body scanners

Body scanners are machines which produce information about potential threats concealed on that individual's physical person. The machines take advantage of the fact that certain wave forms are capable of passing through clothes, but not through skin, metal, narcotics and other substances. There are various types of body scanners, using different technologies to achieve essentially the same result. Following the events of 9/11 and the shift in focus to the prevention of terror attacks, aviation security has come under particular scrutiny. Amongst areas in which advanced technologies were seen to offer solutions to perceived risks was the detection of hidden objects.[82]

Whilst aviation security is predominantly the competence of Member States, the cross-border and trans-national nature of air travel means that the EU and other international fora play a large role in coordinating initiatives and policy on common arrangements. Despite a number

[82] Mordini, Emilio, "Whole Body Imaging at airport checkpoints: the ethical and policy context", in René von Schomberg (ed.), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, Publications Office of the European Union, Luxembourg, 2011, pp. 165-209.

of tests, body scanners have enjoyed limited uptake in Europe in the face of civil liberties, health and effectiveness concerns.

In the paragraphs that follow, we evaluate what little evidence we have found from the European context, drawing on the financial impact assessment conducted by the EU and certain Member States. We then consider the broader, cost-benefit studies conducted in the US context.

Financial impact of body scanners in Europe

The difficulty in conducting a full economic impact analysis was immediately evident from European reports which state, "because of the scarcity of available detailed information especially as regards the cost elements related to the use of security scanners, a full cost-benefit analysis was not possible".[83] Certain countries, for example, France, had conducted no cost assessment on account of the use of the scanners as demonstrations only. Others had only conducted specific targeted cost assessments. The Netherlands, for example, had assessed cost effectiveness only in terms of better employing security staff. In fact, "among all countries deploying security scanners only the UK have conducted an assessment of the economic impact of deploying security scanners at their airports compared to the current situation, which is publicly available".[84] Even the UK assessment does not provide a full cost-benefit analysis, but only analyses costs in relation to a final code of practice aimed at securing the health and privacy of passengers.[85]

However, based on information available, certain direct costs could be identified. First, considering information from manufacturers, each body scanner machine costs between €100,000 and €200,000.[86] This price does not reflect the upgrades which may be required to take further public or legal concerns into account (for example, in relation to data protection or privacy). Nor does it factor in upgrades which may be required or components which would facilitate automatic use. The cost of such extra components is estimated at approximately €20,000.[87] Not including the possibility that the cost of each unit will drop with a rise in production, this cost is considerably higher than that of the currently used metal detectors, which cost between 6,000 and 17,000 per unit.[88]

In terms of staff, the exact cost is dependent on the set up of the body scanner, the set up of the other aspects of the security lane and the supporting operation policies (for example in the case of a general opt-out policy being implemented, more staff may be required for the purposes of hand-screening). Despite these uncertainties, the number of staff required to operate a security lane complete with scanner is estimated at between six and 10.[89] A lane without a scanner requires between six and nine members of staff. Judging from data collected from 12 countries, and considering the net cost of deploying staff for the airport,

[83] European Commission, "Impact Assessment on the possible use of security scanners at EU airports (Draft)", Commission Staff Working Paper, Brussels, 2011, p. 5.
[84] Ibid.
[85] UK Department for Transport, "Impact Assessment on the use of security scanners at UK airports", London, 2010.
[86] European Commission, Impact Assessment on the possible use of security scanners at EU airports (Draft), Commission Staff Working Paper, Brussels, 2011, p. 42.
http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2011/sec_2011_1327_en.pdf
[87] Ibid.
[88] Ibid.
[89] Ibid., p. 41.

costs for employing one member of staff as a screener range between €61,320 and €331,653 per year.[90] The cost for training and retraining of staff to operate the scanners does not seem to have been taken into account in the final cost evaluation.

Considering the cost of a scanner (depreciated over seven years) and including yearly maintenance etc., each airport will face costs of between €25,285 and €39,571 per year per scanner.[91] In the case of the use of a scanner requiring a remote viewer, and on the assumption that this will require the employment of one extra member of staff, each airport will thus face costs of between €86,605 and €371,225 per year (some scanners do not require a remote viewer).[92] To this must be added potential policy enforcement costs, which, according to a UK assessment, could cost £53,000 per year for two to four scanners.[93] It may be possible, however, to mitigate cost by reorganising checkpoints to more cost-effectively deploy security scanners as well as, over time, to achieve cost reduction through the better deployment of personnel.[94] The potential costs of reshaping airport space were mentioned in one report as a cost to be borne in mind, but were ignored in the final cost assessment. Extra costs will most likely be borne by passengers – through a rise in ticket prices, for example – and other commercial airport users such as cargo shippers, with minimal costs borne by governments or the airports themselves.[95]

Finally, analysis points out certain opportunity costs that might be saved by body scanner deployment. First, considering the higher detection capability of body scanners compared to metal detectors, airports deploying body scanners may avoid the obligation to employ extra screening mechanisms, and therefore extra security costs, which arise following a new security event. For example, in Europe, after the Detroit incident – in which a young man boarded a plane from Amsterdam to Detroit with explosives hidden in his underwear – overall staff costs increased between €10,000 and €50,000 per week. Second, over time, the efficiency of scanners (and scanner-to-staff ratios) may increase, potentially improving cost-effectiveness and total throughput of passengers. Third, in light of the general trend toward increased passenger screening, the ability of body scanners to reduce security costs may increase over time. Finally, public perception of increased security and the efficiency of the body scanning procedure in comparison to current methods may lead to more positive evaluations of the airport and more time for passengers to use airport facilities, potentially leading to higher non-aviation related income. The gains here could be considerable as up to 43 per cent of income is derived from non-aviation related activities.[96] However, it must also

[90] Ibid., p. 42.
[91] Ibid.
[92] Ibid.
[93] UK Department for Transport, 2010, p. 3f.
[94] European Commission, Impact Assessment on the possible use of security scanners at EU airports (Draft), Commission Staff Working Paper, Brussels, 2011, p. 42.
http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2011/sec_2011_1327_en.pdf
[95] European Commission, Commission Staff Working Document Accompanying the Proposal for a Directive of the European Parliament and the Council on aviation security charges: Impact Assessment, SEC 2009 (615), Brussels, 11 May 2009; European Commission, Impact Assessment on the possible use of security scanners at EU airports (Draft), Brussels, 2011, p. 10.
http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2011/sec_2011_1327_en.pdf
[96] European Commission, Impact Assessment on the possible use of security scanners at EU airports (Draft), 2011, p. 44.
http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2011/sec_2011_1327_en.pdf.This is perhaps a contradictory set of possibilities considering the sensitivity setting of a body scanner is correlated to the probability it will pick up a threat, but is also correlated to how many false positives it will register, and therefore

be mentioned that the speed of processing is arguably not held up by current metal detectors, but rather by the passenger luggage check that occurs in the same lanes. In this respect, body scanners thus offer no solution.

Cost-benefit analysis of body scanners in the US

As can be seen, the European evaluation predominantly considers only direct and easily identifiable costs of deployment. Research into the American context has gone somewhat deeper and offers a perspective based on a cost-benefit analysis. The US context and the cost-benefit approach there offer a different perspective; first, in terms of the analysis of a wide-scale and permanent deployment of body scanners across the country (as opposed to European estimates based on limited trials) and, second, in terms of a much broader consideration of costs (including indirect costs) against potential benefits – for example, the potential cost of the terrorist attack scanner installation is aimed at preventing (as opposed to European estimates which focussed narrowly on cost difference between scanners and current systems). Whilst we are aware of the potential inapplicability of transferring findings from the US context onto the European context, we feel that certain of the approaches provide insight into potential costs on a broader scale, and a template from which useful guidance can be acquired.

Even in the US context, official cost analysis on security measures has been limited. Despite repeated calls for the Department of Homeland Security (DHS) to improve its economic analysis capabilities generally, significant criticisms exist related to the validity and reliability of current approaches and the fact that the DHS has not been "following the critical scientific practises of documentation, validation, peer review by technical experts external to DHS, and publishing. Given the lack of that disciplined approach…it is difficult to know how analyses are being done and whether their results are reliable."[97] In the case of body scanners, the Transport Security Administration (TSA, the body responsible for deployment) has not conducted a cost analysis at all, despite specific observation from the Government Accountability Office (GAO) that "conducting a cost benefit analysis of the TSA's body scanner programme is important".[98]

The US has been pursuing a policy of body scanner deployment since 2009 and plans are in place to procure and deploy 1,800 body scanners by 2014 achieving 60 per cent coverage across the top three (of five) classes of airports in the US.[99] Cost estimates for machines seems to vary slightly – TSA estimates put the cost for each machine at $170,000 (€131,500), whilst the 2011 DHS budget states $430,000 (€332,000) for each machine (plus installation).[100] The 2011 DHS budget requested 500 new machines at a total initial purchase and installation cost of $214.9 million (€165.9 million), plus $218.9 million (€169 million) for 5,355 additional Transport Security Officers, plus $95.7 million to fund the administrative costs associated with the creation of these new positions. An additional annual cost relating to

---

could prejudice the efficiency of processing passengers and indeed have the opposite effect of passenger perception.

[97] National Research Council, *Review of the Department of Homeland Security's Approach to Risk Analysis*, National Academies Press, Washington, DC , 2010.

[98] Lord, Steve, "Aviation Security: TSA Is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to This Effort and Other Areas of Aviation Security Remain", Testimony before the Subcommittee on Transportation Security and Infrastructure Protection, Committee on Homeland Security, House of Representatives GAO-10-484T, US Government Accountability Office, Washington, DC, 2010.

[99] Ibid.

[100] Ibid.; US Department of Homeland Security, "FY 2011 Budget in Brief", Washington, DC, 2011.

upkeep and machine support must also be factored in. The TSA stated that the first 1,000 machines will run at a total operating cost of $650 million (€501.8 million) per year.[101] Taking these numbers as a base, Stewart and Mueller thus estimate the enormous total cost for the total 1,800 units at $1.8 billion (€1.4 billion) per year.[102]

Stewart and Mueller broaden this first-level, cost perspective to consider the indirect costs that body scanner deployment may incur. They also point out the economic implications of the perception and feeling toward body scanners. They suggest that the privacy intrusiveness arising from the deployment of body scanners may deter some people from air travel.[103] If those people don't travel by air, but instead travel by road, Stewart and Mueller use an estimate of 500 extra road accidents per year as a result of existing airport security measures, which, using a (DHS-calculated) value of $6.5 million (€5 million) per life, results in a loss of $3.2 billion (€2.5 billion) per year.[104] On the other hand, they also consider that the "security theatre" aspect of body scanners may make people feel safer and accordingly encourage them to travel by air. They concede, however, that such broad calculations are complex, difficult to quantify and are in need of further research.[105]

Stewart and Mueller follow this analysis with a consideration of the potential economic impact of a terrorist attack, resulting from a failure to install body scanners, could have on the economy. The losses sustained would be considerable. First, the losses sustained as a result of the loss of one plane with 300 passengers has been estimated at $1 billion (€0.7 billion).[106] These losses are compounded by the probable shutdown of airspace for a number of days, and the following prolonged recovery period – one study estimates a loss of $3 billion (€2.3 billion) during the shutdown and a further loss of $15 billion (€11.6 billion) assuming a 15 per cent drop in air travel over six months, another estimates a total economic loss of $214 – 420 billion (€165 – 324 billion) based on a two-year recovery period.[107] The cost of terrorism is, however, difficult to measure and obvious large sectoral losses may be offset by gains across other sectors, as economic activity is substituted away from vulnerable areas – for example, after 9/11, Hawaii experienced a boom in domestic visitors as more Americans vacationed closer to home.[108] It is suggested that, in purely economic terms, the losses for a large economy are generally modest and of a short-term nature. Estimates as to the financial impact of the 9/11 attacks, for example, sit at between 0.3 and 1 per cent of total GDP.[109]

---

[101] Rossides, Gale, "Advanced Imaging Technology – Yes It's Worth It". http://blog.dhs.gov/.
[102] Stewart, Mark G., and John Mueller, "Risk and Cost-Benefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening", Research Report 280.11.2101, The University of Newcastle, Australia, 2011, p. 5.
[103] Ibid.
[104] Robinson, Lisa A., "Valuing Mortality Risk Reductions in Homeland Security Regulatory Analyses", Final Report for US Customs and Border Protection, Department of Homeland Security, 2008.
[105] Stewart and Mueller, 2011, p. 5.
[106] Chow, James, James Chiesa, Paul Dreyer et al, "Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat", Occasion Paper, Rand Corporation, Santa Barbara, CA, 2005, p. 7. The study assumes a value of life at only $2 – 2.5 million (€1.5 – 1.9 million).
[107] Ibid., pp. 7-9; Gordon, Paul, James E. Moore, JiYoung Park and Harry W. Richardson, "The Economic Impacts of a Terrorist Attack on the US Commercial Aviation System", *Risk Analysis*, Vol. 27, No. 3, 2007, pp. 505-512.
[108] Bonham, Carl, Christopher Edmonds and James Mak, "The Impact of 9/11 and Other Terrible Global Events on Tourism in the US and Hawaii", *Journal of Travel Research*, Vol. 45, No. 1, 2006, pp. 99-110.
[109] Blomberg, Stephen Brock, and Adam Z. Rose, "Editor's Introduction to the Economic Impact of the September 11, 2001, Terrorist Attacks", *Peace Economics, Peace Science, and Public Policy*, Vol. 15, No. 2, 2009, pp. 1-14.

Stewart and Mueller then consider the reduction in risk due to the application of body scanners as a security measure. They consider factors including the effectiveness of body scanners as opposed to conventional detection technologies, the likelihood of a bomb going off and destroying the plane should a terrorist succeed in bypassing security, the risk reduction introduced by body scanners considering their place in a layered security system, amongst others.[110]

Taking the above costs, potential losses and risks into account and applying uncertainty and sensitivity analysis to their findings, they conclude, based on mean results, that body scanners would need to disrupt at least one attack – originating from inside the US and that would have succeeded despite the other layers of security – every two years, to justify their cost.[111]

Summary

Body scanners cost enormous amounts of money. Both the European and US evaluation demonstrate this. However, these evaluations are problematic and suffer from a lack of data and analysis. Both approaches considered here are instructive in some ways, but are severely deficient in others. The European financial impact evaluation gives an indication of the direct costs and the relative difference in costs between the deployment of body scanners and current conventional methods. However, its focus is very narrow, both as it only considers single security gates and as its evaluation is predominantly restricted to direct costs and a comparison with current technology. The cost-benefit analysis focussing on the US context, on the other hand, considers a broad systemic deployment of scanners and a wide ranging economic impact assessment including both direct and indirect costs. However, it appears greatly deficient in its evaluations of cost and risk, suffers from the complexity of what it attempts to undertake and, eventually, seems decidedly callous in its application of figures and economics to life and society. Both evaluations almost fully ignore the more important, but yet more abstract, social costs and benefits.

Case Study 2: EUROSUR

The European External Border Surveillance System (EUROSUR) is a border control and surveillance proposal which, according to the European Commission, "can be described as a set of measures enhancing the co-operation and information exchange of border control authorities at national and European level as well as when cooperating with neighbouring third countries".[112] Through this co-operation, EUROSUR attempts to considerably increase the border surveillance and reaction capabilities of member states and FRONTEX at, and indeed beyond, EU borders.

Practically, the proposal obligates the Schengen states to conduct extensive continuous surveillance of high risk land and sea borders, and would mandate FRONTEX to surveil the maritime space beyond EU territory – including the ports of North Africa. The proposal aims at three parallel goals: first, to reduce the number of irregular immigrants entering the EU undetected; second, to increase internal security by preventing cross border crimes (such as

[110] Stewart and Mueller, 2011, pp. 8-17.
[111] Ibid., p. 18.
[112] European Commission, Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR), SEC (2011) 1538 final, Brussels, 12 Dec 2011, p. 3.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2011:1537:FIN:EN:PDF

trafficking in human beings and the smuggling of drugs); third, to reduce the number of lives lost at sea.[113]

Whilst EUROSUR is not a surveillance technology itself, it represents the construction of a wide-scale surveillance system based around a network of special national surveillance systems, connected both multilaterally and through FRONTEX, as well as the employment of a range of state-of-the-art surveillance technologies – including satellite monitoring systems, ship-based monitoring systems and even the deployment of unmanned aerial vehicles (UAVs).[114]

The proposal raises various concerns. First, the EUROSUR proposal stokes a general debate revolving around the legitimacy of EU immigration policy and the level and form of border surveillance generally. Second, the proposal has potentially significant, but unaddressed, fundamental and human rights concerns – particularly regarding the rights to asylum, privacy and data protection. Finally, there are questions as to which interests, particularly those of the defence industry, really stand to benefit from its implementation.[115]

In the paragraphs that follow, we consider the European Commission's financial impact analysis relating to the set up and maintenance of the EUROSUR system. We then consider the extra costs which will be incurred through the requisite supporting research and development programmes, and how, through these programmes, industry meets, and influences, the surveillance agenda. Finally, we present a set of challenges to the accuracy, accountability and transparency of the Commission's estimated costs.

European Commission's financial impact analysis

Even before work had begun on EUROSUR, initial problem definition and feasibility reports were produced at considerable cost, with one contractor paid €1.8 million to produce a preliminary report on the management and operational requirements for the "Common Pre-Frontier Intelligence Picture".[116]

Following work conducted between 2008 and 2011, the European Commission summarised its latest execution plan and cost estimation in documents released on 12 December 2011. These documents came complete with a series of clarified steps toward the realisation of EUROSUR.[117] Seven steps were then grouped and assessed on a range of bases, including cost.[118]

---

[113] European Commission, "Proposal for a Regulation of the European Parliament and of the Council Establishing the European Border Surveillance System (EUROSUR)", COM (2011) 873 final, Brussels, 12 Dec 2011, p. 1. http://ec.europa.eu/home-affairs/doc_centre/borders/docs/eurosur%20final.pdf.

[114] Keller, Ska, and Barbara Unmüßig, "Preface", in Ben Hayes and Mathias Vermeulen (eds.), *Borderline: The EU's New Border Surveillance Initiatives: Assessing the Costs and Fundamental Rights Implications of EUROSUR and the "Smart Borders" Proposals*, Heinrich Böll Stiftung, Berlin, 2012, p. 4. http://www.statewatch.org/news/2012/jun/borderline.pdf

[115] Hayes, Ben, and Mathias Vermeulen, *Borderline: The EU's New Border Surveillance Initiatives: Assessing the Costs and Fundamental Rights Implications of EUROSUR and the "Smart Borders" Proposals*, Heinrich Böll Stiftung, Berlin and Brussels, 2012.

[116] Ibid., p. 50.

[117] European Commission, Proposal for a Regulation of the European Parliament and of the Council Establishing the European Border Surveillance System (EUROSUR), COM (2011) 873 final, Brussels, 12 Dec 2011. http://ec.europa.eu/home-affairs/doc_centre/borders/docs/eurosur%20final.pdf.

1. The set-up of National Coordination Centres;[119]
2. The setting up of the EUROSUR network (step 6, the set-up and impact of the Common Pre-Frontier Intelligence Picture, –and step 7,the impact of the Common Information Sharing Environment for the combating of serious crime –were also assessed under this head);
3. The set-up of cooperation with neighbouring third countries;
4. Research and development (which relied on FP7 funding and was considered as separate from set up and maintenance costs and was thus not considered in the cost impact assessment. This will be specifically considered in the next section);
5. The set-up of the common application of surveillance tools;
6. The set-up and impact of the Common Pre-Frontier Intelligence Picture;
7. The set-up and impact Common Information Sharing Environment.

Three policy options were presented for the estimation of cost between 2011 and 2020. Policy option 1 followed a decentralised approach and would cost €318.1 million if fully followed; policy option 2 followed a partly centralised approach and would cost €544.9 million if fully followed; and policy option 3 followed a fully centralised approach and would cost €913 million if fully followed. In a selection of options from across the various policies, the preferred option for EUROSUR was estimated to cost €338.7 million in total.[120]

- With regard to step 1, namely, the set-up of the National Co-ordination Centres, the decentralised approached was deemed to be the most suitable. It was seen to require no restructuring of national administration and thus could be easily implemented. The cost for the set-up of the National Co-ordination Centres was estimated at €99.7 million. On top of this would come €95.5 million for the establishment of a FRONTEX situation centre.[121]
- With regard to step 2, namely, the set up of the EUROSUR network, the partly centralised option was chosen. This choice was based on the perceived difficulties and delays which could arise out of the need to share information in a decentralised network and partly on the relatively small difference in cost between the construction of decentralised and centralised networks. This was estimated to cost €46.7 million.

European Commission, Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR), SEC(2011) 1538, Brussels, 12.12.2011,
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2011:1538:FIN:EN:PDF; European Commission, Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council. Steps are laid out in European Commission, Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR), SEC(2011) 1538, Brussels, 12.12.2011, p. 3,
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2011:1538:FIN:EN:PDF.

[118] The documents in fact work from an eight-step program. However, the eighth step, "Creation of a *common information sharing environment* for the EU maritime domain… is developed in the framework of the EU Integrated Maritime Policy and was not included in the cost assessment. See European Commission, Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR), SEC(2011)1536 final, 12 Dec 2011, p. 21.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2011:1536:FIN:EN:PDF

[119] The set-up of National Co-ordination Centres step includes the setting up of a FRONTEX situation centre.

[120] European Commission, Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR), SEC(2011) 1536 final, 12 Dec 2011, p. 39.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2011:1536:FIN:EN:PDF

[121] Ibid., pp. 29-31.

On top of this would come the estimated €29.3 million estimated for the set up of a partly centralised approach to the Common Pre-Frontier Intelligence Picture.[122]

- With regard to step 3, namely the promotion of co-operation with neighbouring third countries, the partly centralised policy option was chosen. This choice was made in light of the perception that there is an urgent need for enhancing the situational awareness and reaction capability for border control in the Mediterranean region. This was estimated to cost €5.4 million.[123]
- With regard to step 5, namely the common application of surveillance tools, the partly centralised option was seen to offer best value and was estimated to cost €62.1 million.[124]

Research and development

Step 4 – research and development – is aimed at the development and testing of the technical capabilities envisaged in the other steps.[125]

Research and Development for EUROSUR receives funding from the EU's Framework Research Programme (FP7), which runs from 2007-2013. The FP7 programme incorporates the European Security Research Programme (ESRP), which was launched in 2004 and has, as one of its five core mission areas, border security. Hayes and Vermeulen identify 15 projects to date in the area of border security to which the EU has contributed more than €170 million, half of which contributes directly or indirectly to EUROSUR.[126] The results of two more calls on border surveillance will be announced before 2013, when FP7 comes to an end. If its successor programme, Horizon 2020, is also used to fund EUROSUR at the same rate, Hayes and Vermeulen estimate funding between now and 2020 could reach up to between €300 and €400 million.[127]

ESRP funding will be supplemented by funding from the Global Monitoring for Environment and Security programme (GMES) – also part of FP7. Whilst it initially focussed solely on environmental information, it has also been increasingly used to support EUROSUR. To date, seven GMES projects have contributed to EUROSUR at a cost of €36 million.[128]

Finally, the Commission has also funded EUROSUR development projects external to FP7, including the MARSUNO and BLUEMASSMED projects, at a cost of more than €5 million.[129]

The funding of EUROSUR research offers an insight into the network of connections that develop around the economics of surveillance politics, and their potential bias to certain actors, and consequently their goals, at the expense of other actors. Hayes and Vermeulen note the presence of defence industry interests in the inception and shaping of the ESRP. They also note the increasing presence of FRONTEX in the development and guidance of the ESRP and the significant overlap in the interests of FRONTEX with those of defence contractors.

[122] Ibid., pp. 31-33.
[123] Ibid., pp. 33-35.
[124] Ibid., pp. 35-37.
[125] Ibid., p. 21.
[126] Hayes and Vermeulen, 2012, p. 59.
[127] Ibid.
[128] Ibid., p. 64.
[129] Ibid.

This overlap is evident in the ubiquity of the same defence contractors who have been noted to have had an impact of the development of the research programme, in EUROSUR project consortia.[130] The bias of interests is also visible in the division of funding between the three parallel goals of EUROSUR. It is conspicuous that there is a total lack of funding for projects concerned with rescue at sea (in pursuit of saving the lives of immigrants) as opposed to projects aimed toward the other two EUROSUR goals (and those more closely connected with the defence industries) – prevention of illegal migration and combating cross-border crime.[131]

This is a significant cause for concern as "the ESRP appears to have had the effect of consolidating relations between the security and defence industries and those responsible for developing and implementing border policies at the EU level, while at the same time marginalising those perspectives that are not convinced of the need for smart surveillance."[132] The same phenomenon has been noted by other commentators, and notably in a 2010 report commissioned by the European Parliament's Citizens' Rights and Constitutional Affairs' policy department.[133]

Questioning cost estimations

Despite the number of studies, and the relatively detailed set of cost estimates produced by the Commission, EUROSUR provides an excellent example of the questionable reliability of financial impact estimates for large-scale technology-based surveillance systems for several reasons.

First, there are questions as to the accountability of the funding, necessity and results of many aspects of the EUROSUR proposal. This is evident in the classification of certain of the original studies, making true transparency into costs and funding difficult.[134] Second, it is evident in the consideration of funding allocated to research and development projects supporting EUROSUR. On the one hand, considering the dispersal of funds across projects with direct and indirect input into EUROSUR, it is difficult to evaluate the exact funding EUROSUR R&D is receiving. As Hayes and Vermeulen point out, "a separate budget line for EUROSUR R&D with clear goals and objectives would provide for greater democratic control and legitimacy".[135] On the other hand, independent review of the results of these projects and their implications for EUROSUR has been conspicuously lacking, making it difficult to evaluate their initial or continuing qualification for funding.

Second, there are considerable methodological problems with current cost estimates. 2011 estimates rely on information taken from estimates in prior feasibility studies, current projects

[130] Ibid., pp. 55-57.
[131] Ibid., p. 59.
[132] Ibid., p. 56.
[133] Jeandesboz, Julien, and Francesco Ragazzi, "Review of security measures in the Research Framework Programme", Study PE 432.740, European Parliament, Directorate-General for Internal Policies, Policy Department C "Citizen's Rights and Constitutional Affairs", Strasbourg, 2010; Gutwirth, Serge, Rocco Bellanova, Michael Friedewald, Dara Hallinan, David Wright, et al., *Smart Surveillance – State of the Art Report*, Deliverable 1, SAPIENT Project, 2012, pp. 185-214. www.sapientproject.eu.
[134] European Commission, Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR), SEC(2011) 1538, Brussels, 12.12.2011, p. 10, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2011:1538:FIN:EN:PDF..
[135] Hayes and Vermeulen, 2012, p. 59.

supported by the European Border Fund and Member State responses to a questionnaire. Estimates from current projects and from previous EUROSUR studies provide only a broad, and potentially outdated, template for cost evaluation. Also, Member State response to the questionnaire was limited "in response to our data collection exercise for national co-ordination centres, four Member States (Norway, Iceland, Sweden and Denmark) did not provide a response. A further two Member States (Germany and Portugal) provided some descriptive information for their NCCs, but no cost data", whilst "the completeness and comparability of that data varied to a large extent".[136] In light of this difficulty in comparison, the decision was made to evaluate cost based only on information from two states for each policy option – the two states selected were different for each policy option. This significantly limits the reliability of cost estimates.

Third, there are question marks over the construction of the proposal and its alignment with cost estimations. Specific articles have been pointed out as problematic – for example, Article 12 has an open formulation in regard to which technologies may be employed and accordingly what they may eventually cost. Also, no specific limit has been placed on funding.[137] Without this, and a clarification of funding sources, there is no control mechanism (the European Parliament, for example, would be powerless in this respect) to prevent costs spiralling out of control.

Indeed, when Hayes and Vermeulen analysed costs, the Commission's cost estimates fail to stand up to scrutiny, even contain contradictions. Whilst their cost analysis is formulated slightly differently, they make certain direct comparisons. In terms of the set-up of the National Co-ordination Centres, the Commission estimates €99.6 million from 2013 to 2020. Hayes and Vermeulen consider the EUROSUR Regulation's estimated budget allocation from the Internal Security Fund (ISF) between 2014 and 2020 (€112 million) plus Member State estimates from 2011 to 2013 (€105 million), to put the total rather closer to €227 million.

The Commission estimates €5.4 millionfrom 2013 to 2020 for establishing networks with third countries. Hayes and Vermeulen consider funds allocated from the Development Co-operation Instrument thematic programme for co-operation with third countries in the areas of migration to third countries who co-operate in the framework of EUROSUR, plus funding from the ISF for enhanced cooperation with third countries, to come to a total of €98 million.[138]

As opposed to the Commission's total estimate of €338.7 million, the total resulting from Hayes and Vermeulen's recalculations (not including the projects funded under FP7) stands at €553.3 million.[139]

---

[136] European Commission, Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR), SEC(2011) 1538, Brussels, 2011, p. 36, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2011:1538:FIN:EN:PDF.

[137] European Commission, Proposal for a Regulation of the European Parliament and of the Council Establishing the European Border Surveillance System (EUROSUR), COM(2011) 873 final, Brussels, 12.12.2011, Article 12, pp. 18-19, http://ec.europa.eu/home-affairs/doc_centre/borders/docs/eurosur%20final.pdf. European Parliament, Committee on Civil Liberties, Justice and Home Affairs, LIBE Committee Meeting, 11 October 2012. http://www.europarl.europa.eu/ep-live/en/committees/video?event=20121011-1500-COMMITTEE-LIBE&category=COMMITTEE&format=wmv.

[138] Hayes and Vermeulen, 2012, pp. 67-69.

[139] This total estimate does not take into account Hayes and Vermeulen's estimate regarding the common application of surveillance tools and instead relies on the Commission's figure of €29.9 million. Taking Hayes and Vermeulen's estimate of €350 million into account, the final total would be €873.7 million. Ibid., pp. 70. See

Summary

EUROSUR will cost a huge amount of money. However, and despite a relatively comprehensive approach toward evaluating the cost of the system, the European financial impact evaluation only gives an indication of the direct costs involved in setting up and maintaining the network. Accordingly, its focus is very narrow, and does not consider the broader economic, social or human costs, or benefits, of the proposal. Equally, the approach fails to make a comparison with other policy alternatives.

Despite the above issues with the approach, EUROSUR is a fascinating case study into the financial impact of surveillance. The planning and final distribution of financial resources not only reflect the social evaluations and balances implicit in the creation and deployment of surveillance policy and technology, but also play a role in the definition of the final shape, function and consequence of those policies. In the consideration of the costs of EUROSUR, we can directly observe certain of the networks and connections between industry and policy and trace the structured interest transfers which take place and define initial planning, final funding and eventually will define the final function or the system.

Finally, through analysis of the cost evaluation of EUROSUR, we observe the difficulty in evaluating the financial impact of surveillance systems and appreciate that such estimates, either by reason of design or uncertainty, may be decidedly unreliable.

Table of cost estimations 2011 - 2020

Step no.	Step	EC's cost estimate (in million euro)*	Alternative estimates where direct comparison made, Hayes and Vermeulen (in million euro)	Difference (in million euro)
1	*National Co-ordination Centres*	99.6	227	127.4
1	*FRONTEX Situation Centre*	95.6	N.A.	N.A.
2	*EUROSUR Network*	46.7	46.7	0,00
7	*Common Information Sharing Environment*			
6	*Common Pre-Frontier Intelligence Picture*	29.3	N.A.	N.A.
3	*Co-operation with third countries*	5.4	98	92.6
4	*Research and development*	N.A.	350	N.A
5	*Common application of surveillance tools*	62.1	N.A.	N.A.
Total cost estimate		338.7	873.7**	535**

*See pp. 240-243 and footnote 151. Hayes and Vermeulen's table of cost estimates is slightly differently constructed. Direct comparisons have been made only where possible.

---

also European Commission, Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR), SEC(2011) 1538, Brussels, 2011, pp. 28-39, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2011:1538:FIN:EN:PDF.

**Hayes and Vermeulen's original figures have been used in this table. See above and footnote 152, for qualification.

Conclusion

We have analysed only relatively large scale, public deployments of surveillance technologies. Even with regard to these, information was limited and relatively difficult to find. Whilst more information may be available, we imagine that the majority of organisations conducting such studies would find no benefit in public release. The vast majority of smaller, private and "banal" surveillance deployments may never be costed.

The information we have found, and the methodologies they employ for estimating cost, have shown themselves to be somewhat limited. Even comparable evaluations can arrive at significantly different results. We see in the body scanner case the difficulty, and eventual absurdity, of attempting a broad scale cost-benefit analysis of a surveillance and security technology. Whilst financial impact assessments fare somewhat better, costing, as they do, that which can be costed in financial terms, we can see in the EUROSUR case that even here there are problems.

The lack of information and the flaws in methodology leave many systemic and indirect costs unaddressed – for example, the costs of resistance or potential reductions in innovation due to increased conformity. Without significant further research the identification and consideration of such costs can be attempted in only the most abstract terms. The difficulty in precise evaluation, and the inability to define precisely how, or how well, specific funding achieves specific goals, also leads to the inability to apply traditional accountability, proportionality and necessity tests to surveillance funding, and explains why surveillance projects tend toward significant overspending.[140] Without considering the inapplicability of using cost analysis to define social debates, these methodological issues and the variation in results alone should serve as a warning regarding the use of cost analysis as a tool for political decision-making.

Despite reservations as to the availability of information and the methodologies used, our analysis offers certain important insights. First, it is apparent that surveillance, and surveillance technologies, represent huge economies. EUROSUR plans run into the millions and the systemic deployment of body scanners into the billions (in the US). Second, through the study of these economies, we can see the connection between the vendor (industry) and the purchaser (policy-makers) and observe how this financial relationship has become systemic, shaping the deployment of surveillance technologies toward political ends. Finally, considering money as another form of social resource – the distribution of which is a reflection of social preference – the analysis of the financial impact of surveillance technologies offers, at both planning and execution phases, an often ignored perspective on the place and development of surveillance in European society.

[140] This tendency towards overspending is not limited to surveillance projects, of course, but is a phenomenon that has been identified in management literature and is associated with large projects generally. See Jørgensen, Magne, and Kjetil Moløkken-Østvold, "How large are software cost overruns? A review of the 1994 CHAOS report", *Information and Software Technology*, Vol. 48, No. 2, pp. 297-301.
We would however argue that the unique difficulty of precisely defining and then attaching financial values to the necessity and goals implicit in surveillance projects adds a new, and potentially significant dimension to this phenomenon, one which would be a fascinating topic for further research.

5.5 THE RELEVANCE OF SOCIAL AND ECONOMIC COSTS OF SURVEILLANCE

Ivan Szekely, Beatrix Vissy, EKINT

In the foregoing, a whole range of social and economic costs of surveillance have been identified and the most important social and economic costs analysed and evaluated. Such important social costs are the social damage caused by "false positives" of suspects of criminal and terrorist activities, the categorical suspicion and discrimination of members of certain social or ethnic groups, the marginalising effects and the social inequalities caused by invasive monitoring of those of lower social status, the inhibitory effects of surveillance which can undermine social and democratic activities, or the erosion of trust in society; evident economic costs are the costs of developing, implementing and operating surveillance technologies, the increase of costs in sectors and activities where such technologies are built into the normal operation (transport, traveling, financial transactions), and there are several indirect economic costs of surveillance, from the reduced level of innovation due to increased conformity, through the impact of changes in behaviour on welfare, to the costs of decreasing individual responsibility for security due to reliance on surveillance systems.

In an ideal decision-making process, all these costs, together with the envisioned positive effects – such as increasing security, the feeling of safety, prevention of crime and terrorism, increased efficiency in workplaces – have to be taken into consideration when deciding over the use of surveillance methods and the deployment of surveillance technologies. In order to approach such an ideal process – or more realistically, to ameliorate existing decision-making processes – first we need to explore why and how social and economic costs of surveillance should be identified, assessed and taken into consideration. In the course of this analysis, we hypothesise a well-working democratic rule-of-law environment.

For the legitimisation, or more precisely, for guaranteeing the legitimate nature, of a decision to introduce, to extend or even to discontinue the use of surveillance methods and tools, both social and economic costs have to be considered and evaluated. Economic costs are easier to evaluate, since in modern capitalist societies all goods and services can be easily converted to financial or economic values; this logic, together with the necessarily globalised methods, are well-known not only in public administration and public management, or in the business sector, but also among the IT professionals – in other words, those who conceptualise, develop, realise and maintain the surveillance systems in today's society. Social costs are more difficult to evaluate, partly because of the difficulties in comparing and weighting competing social values, interests and rights, and partly because of the difficulties in weighting such values, interests and rights against direct financial or economic costs.

Analysing of social costs is indispensable for setting the space of action of the power in general, and for marking the boundaries of surveillance in concrete cases. If a decision (or the lack of it) implies social costs, it has to be justifiable that the costs are worth the end result, consequently the decision is permissible. If such a justification is missing, the decision is arbitrary. Mapping and analysing social costs are necessary not only for making an adequate decision about the permissibility of surveillance, but also for ensuring the possibility to justify the decision retrospectively.

When analysing social costs, the general level, abstract normative decisions and the individual decisions relating to concrete cases have to be taken into consideration. It is important to observe that the individual or normative characteristic of a decision has relevance in itself

when reviewing the social costs of a decision. While the social costs of the general level decisions of normative nature appear in a systemic manner at the macro level (see the social costs of the EU Data Retention Directive), the social costs of individual decisions (such as an order to keep certain individuals under surveillance by secret services) are manifested at micro levels. However, it would be a completely unjustifiable effort to reduce social costs in a way that "only" individual members of society were affected by such decisions, since the infringement of rights of individual members of the political community also results in social costs for the whole of the community.

Decision-making mechanisms of democratic societies are in general suitable for conducting a wide-scale review and analysis of the social and economic costs of the acts of power. However, if such a procedure is left out from the decision-making process, this fact in itself can undermine the legitimacy of the decision, irrespective of the fact whether or not the resulting social and economic costs are justifiable in a substantive sense.

The mere fact that surveillance may have negative social or economic impacts does not mean that such surveillance is not permissible: its costs should always be compared to the legitimate aim of the surveillance. A minimum requirement of the decisions on surveillance is that a publicly accessible and reasonable argument should counterbalance the social and economic costs resulting from surveillance. Where such reasonable connection between the benefits of surveillance as a legitimate aim and the resulting social costs cannot be identified, the decision is necessarily arbitrary. In certain cases, the requirement of defining reasonable arguments is not sufficient, because there exist certain social costs (the restriction of fundamental rights), which require a justification stronger than necessary in a general case. In such cases, the principle of proportionality, as a general principle of EU law accepted by the European Court of Justice, should be applied.[141] The application of this principle in legal practice consists of three tests: the necessity, suitability and proportionality tests. The necessity test assesses whether the chosen surveillance measure is necessary to achieve the proposed goal, meaning that the measure chosen should be the least restrictive on the given norm, causing the smallest social costs. The suitability test assesses whether the chosen surveillance measure is suitable or appropriate in order to achieve the given aim. The proportionality test determines that a surveillance measure, although suitable and necessary, is disproportionate if it imposes an excessive burden on the affected parties. To define the exact content of this last test is the most difficult of the three tests. It has been criticised by some legal scholars, as this test can undermine the rationality of the principle of proportionality itself, namely, to provide objective guidelines according to which the decision-makers' – especially the courts' – reasoning should be conducted in hard cases.[142]

Although it goes beyond the extent of the present analysis, it should be noted that not all legal systems include the principle of proportionality in judicial practice. In the practice of the US Supreme Court, this optimisation process is missing; the decisions are made on the basis of the "strong rights" concept. This practice reflects the liberal concept of law where there is no room for balancing mechanisms like the one laid down in the principle of proportionality.[143] Nevertheless, the mere obligation to conduct these tests and provide adequate reasoning can result in better substantiated decisions in any legal and administrative system.

[141] Harbo, Tor-Inge, "The Function of the Proportionality Principle in EU Law", *European Law Journal*, Vol. 16, No. 2, March 2010, pp. 158–185.
[142] Ibid., p. 165.
[143] Dworkin, Ronald, *Taking Rights Seriously*, Harvard University Press, 1978.

One possible methodological framework, which is theoretically suitable for serving the purposes of an ideal decision-making process involving the social and economic costs of surveillance, is the recently conceptualised and worked out surveillance impact analysis (SIA).

The first suggestion to work out such a methodology originates from *A Report on the Surveillance Society*, prepared by the Surveillance Studies Network for the UK Information Commissioner's Office[144] in 2006, to mean the assessment of surveillance on individual rights (including privacy) as well as on a range of social and other processes and values. The first practical initiative emerged in an FP7 project, Surveillance, Privacy and Ethics (SAPIENT),[145] the research consortium of which proposed the development of a surveillance impact assessment methodology. The phases of the development can be followed in recent publications;[146] the methodology will be field tested on three different surveillance projects, the first time such tests will be conducted at European level. The paper summarising the elements of such a methodology[147] identifies the main areas of impact as individual privacy issues and impacts, social issues and impacts, economic and financial issues and impacts, political issues and impacts, legal issues and impacts, and ethical issues and impacts. It also identifies a long list of potential stakeholders: central governments, local authorities, the police, telecom companies and Internet service providers, industry (manufacturers, integrators, suppliers), banks, credit card companies, credit reporting companies, insurance companies, social networks and other Web-based companies, employers, health care providers, schools, universities, the media, foreign governments and industry, as well as our family and friends, members of social media, even criminals (who are not only potential targets of surveillance but may use surveillance methods and technologies for their purposes). Naturally, of these wide range of areas and stakeholders only those should be taken into consideration in the course of the decision-making process which has relevance in the given case, and this "will depend on contextual factors, such as the scale of the system to be deployed, the technologies to be used, the purpose of the surveillance, where and when it will be deployed, and so on".[148]

However, in practice, neither micro nor macro level decisions on the introduction, implementation and diffusion of surveillance methods, technologies and equipment, are made in a centralised way, nor are there forums where the necessary expertise in the relevant areas and the various societal interests and fundamental rights are adequately represented: such decisions are often made as a reaction to actual problems or events, initiated by lobby groups, which are attempting to influence decision-makers independently of each other.

The lobby groups and organizations representing these conflicting values and interests regard each other as adversaries. In the efficiency-driven public administration and business sector the "privacy lobby" is seen as an obstacle of efficiency, development and profit-making, while among advocates of human and informational rights similarly pejorative expressions

[144] Surveillance Studies Network (SSN), *A Report on the Surveillance Society*, prepared for the Information Commissioner, September 2006.
[145] SAPIENT project, Surveillance, Privacy & Ethics, 2011-2014, http://www.sapientproject.eu/.
[146] Raab, Charles, and David Wright, "Surveillance: Extending the limits of privacy impact assessment", in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012, pp. 363-383.
[147] Wright, David, and Charles Raab, "Constructing a surveillance impact assessment", Paper presented at the Living in Surveillance Societies (LiSS) workshop, Budapest, 1-3 October 2012. The paper was subsequently published as follows: Wright, David, and Charles Raab, "Constructing a surveillance impact assessment", *Computer Law & Security Review*, Vol.28, No. 6, December 2012, pp. 613-626.
[148] Ibid., p. 617.

are used for the “risk industry” or the interpenetration of political power and surveillance. The virtual coalition of pro-surveillance forces typically consists of the law enforcement sector, the efficiency minded public administration and the “risk industry”; the anti-surveillance coalition is typically composed of the civil sector, liberal intellectuals and a segment of the media.

However, if we accept Lawrence Lessig's famous view whereby “the code is the law” in modern information societies, it will follow directly that the coders – the IT professionals – are the de facto law-makers in today’s society, among them those who develop and maintain surveillance systems. Therefore, it is important to learn the opinion of these professionals, together with the opinion of their bosses, in order to involve them in the pool of stakeholders during the decision-making process in surveillance-related matters.

One of the few comprehensive studies in this white area was conducted in the framework of the international research project "Broadening the Range Of Awareness in Data protection" (BROAD). [149] One of the three main action areas of the project was to study the views of IT professionals in the Netherlands and in Hungary on issues of privacy and surveillance. The results of the qualitative and quantitative studies revealed that one of the initial hypotheses, namely that IT professionals tend to identify with the value system of their bosses or clients proved to be unfounded: the respondents seemed to have more sophisticated views on the social impacts of the systems they design, build or operate (although their attitudes only marginally influence their actual behavior).[150]

Paradoxically, empirical studies may also hinder the adequate observance of social costs of surveillance. Pro-surveillance parties often refer to survey results reflecting the supporting opinion of the respondents. This practice raises two fundamental questions: first, to what extent are these surveys unbiased, and are they suitable at all for exploring the opinion of the people, and second, what weight should be given to public opinion when making a decision affecting fundamental rights and freedoms. These are general questions in decision-making but have special relevance in surveillance related decisions. The first question has been raised in the course of the research conducted in the framework of the first international multidisciplinary academic program to consider issues relating to everyday life in surveillance societies, called "Living in Surveillance Societies" (LiSS).[151] The researchers involved in this program observed that over the past 40 years, there have been a large number of public opinion surveys of attitudes towards, or knowledge about, surveillance and privacy, the findings and conclusions of which are often biased, yet they are interpreted and used selectively by participants in the process of policy-making to support their different causes. The research team started to take stock of existing surveys at the intersection of surveillance and privacy, to analyse them from a methodological standpoint of good practice, and to evaluate their reliability and comparability. The aim of the research team was to compare those characteristics of existing surveys which are relevant to their scientific value, the reliability of their findings and the applicability of their conclusions in policy-making, to identify critical points in the process of creating surveys, and to draw lessons from this

[149] BROAD Project, Broadening the Range Of Awareness and Data protection, 2009-2010. http://www.broad-project.eu.

[150] Szekely, Ivan, “What Do IT Professionals Think About Surveillance?”, in Christian Fuchs, Kees Boersma, Anders Albrechtslund and Marisol Sandoval (eds.), *Internet and Surveillance. The Challenge of Web 2.0 and Social Media*, Routledge, New York, 2011, pp. 198-219.

[151] LiSS is a COST (European Cooperation in Science and Technology) Action, supported by the European Commission. www.liss-cost.eu.

exercise so that surveys in the future can be conducted and reported on a better footing. This research has also been continued and extended in the framework of the EU research project PRISMS.

Social (and economic) costs do not have the same effect in all societies; these costs may have different importance in societies with different priorities, different political and historical traditions and different levels of resilience towards surveillance.[152] In Europe, the different democratic contexts as well as the different historical periods of political repression or dictatorship and their impact of present-day public perception of surveillance may result in different weighting of these costs. This may, however, lead to an unsatisfactory situation, where decision-makers under-estimate the relevance of certain social costs because of the lower sensitivity of society. This is especially undesirable because a significant part of social costs are not directly perceptible for the members of society.

In the new democracies of Europe – those countries which experienced a profound change in their formerly antidemocratic political system at the end of the eighties or later – specific models of perception of surveillance can be observed, and this has a significant impact on how social costs of surveillance are perceived in these countries. Theorists point out that in new democracies the pervasive fear of the former repressive regime was quickly replaced by a fear of crime;[153] in these societies the threshold of abstraction (above which people do not realize the intrusion in their privacy) in the area of surveillance is lower than in more experienced democracies;[154] the 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; or the members of these societies are less experienced and more gullible vis á vis business and marketing offers, including industry-driven surveillance.[155]

Finally, certain social and economic costs may have long-lasting effects which exert an impact on society beyond the actual costs of a concrete case of surveillance. Such effects may direct the development of society in an undesirable direction – for example, losing trust in institutions, thereby lowering the general level of social capital – or simply result in conserving undesirable attitudes and patterns in society from the aspect of a democratic rule-of-law system.

Besides purely social impacts, one specific technical characteristic of present-day information systems, namely that the information collected through surveillance activities will be extremely difficult to erase, if possible at all, results in a constant temptation to use this information for purposes exceeding the original purpose, thereby causing further social and

[152] See, for example, Samatas, Minas, Chiara Fonio, Catarina Frois and Gemma Galdon Clavell, "Authoritarian Surveillance and its Legacy in South-European Societies: Greece, Italy, Spain, Portugal", in William C Webster, 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.

[153] Los, Maria, "Post-communist fear of crime and the commercialization of security", *Theoretical Criminology*, Vol. 6, No. 2, 2002.

[154] 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, 2010.

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

economic costs. These effects should also be taken into consideration when evaluating the social and economic costs of surveillance.

In conclusion, the following recommendations can be made for decision-makers for due taking into account of the social and economic costs of surveillance:

- In the decision-making process, due consideration and evaluation of social and economic costs of surveillance, unbiased representation of interests and values, and the involvement of adequate expertise should be guaranteed.
- In this process, especially when restriction of fundamental rights is at stake, the principle of proportionality and the tests of necessity, suitability and proportionality should be applied.
- It should be taken into consideration that a decision implying social costs has to be justifiable on grounds of whether the costs are worth the end result, and if such a deliberation is missing, it makes the decision unjustifiable and illegitimate in itself.
- Empirical data regarding social costs should be used with precaution.
- A wide range of stakeholders should be involved in the process, according to the scale and characteristics of the subject of the decision; the opinion of IT professionals is particularly relevant.
- It is advisable to use a formalised methodology, such as surveillance impact assessment; however, these methodologies should not be used in a mere formal, bureaucratic way.
- All these requirements impose additional burdens on decision-makers; however, such a process may result in better substantiated decisions and ensures the possibility to justify the decision from the legal and ethical points of view, even retrospectively.

5.6 CONCLUSION

Johann Čas, OeAW-ITA

The increasing relevance of surveillance in security policies is a consequence of many, partly interwoven developments: technical progress as an enabling factor, increased focus of politics and media on security as a result of past terrorist attacks, industrial interests to create new markets for security technologies, political interests to focus public attention on problems for which “hard solutions” appear to be available, or societal tendencies to support policies promising any kind of security gain in times of increasing social and economic instabilities, to name but a few.

It is, however, also the consequence of a more general shift of paradigm in (security) policies. The new paradigm is based on prevention and pre-emption as core elements and objectives of security policies; early detection of unusual behaviour and possibly related risks are further key objectives. Surveillance does not stop at detection; also changes of behaviour are intended, it is not limited to predicting the future, it also aims at shaping it. Paradoxically, economic policies fostering market liberalism and reducing social security are accompanied by tendencies of increasing control and restrictions concerning more and more aspects of individual behaviour.

The chapters on the social and economic costs clearly demonstrate that surveillance is an expensive activity. The violation of the presumption of innocence, inherent to any large-scale,

undirected surveillance measures, is not only a legal and constitutional issue and a serious harm to the fundamentals of liberal and democratic societies, it is also costly in social and economic terms. Any untargeted surveillance activity aimed at detecting potential terrorists needs to be extremely sensitive to be able to fulfil its objective. Increasing sensitivity implies necessarily to increase the number of false positives; false positives are not only costly for the concerned persons and society on the whole, but they are also binding follow up capacities within the security sector in a very inefficient way. Attempts to reduce the rate of false positives by profiling are in conflict with the principles of non-discrimination.

Examples of surveillance measures applied to increase conformity is frequently incurring other social and economic costs and accompanied by pretended compliance or non-compliance in less controlled activities. It also remains open to what extent increased conformity is consistent with democratic and liberal societies or to what extent it is decreasing social and economic innovations, which are key factors and long-term competitiveness.

The examples of body scanners and EUROSUR as large-scale implementations of surveillance measures show that the required direct expenditures of such a magnitude of the public debate on the efficiency and effectiveness of the intended implementations and on available alternatives appears to be inevitable. They demonstrate also a lack of transparency on the involved costs that cannot be justified and undermines the control of the efficient use of public resources.

The relevance, magnitude and importance of social and economic costs of surveillance on the one hand and the difficulties in identifying and quantifying them, on the other hand, suggest at least two recommendations to reduce this mismatch. First, more research in methodological improvements on the analyses of social and economic aspects of surveillance is needed to improve the reliability and comparability of such assessments. In addition, the complexity of the involved issues and the danger of domination by individual interests demands the representation of different interests and perspectives in any decision-making on surveillance.

6 IMPACTS OF SURVEILLANCE ON CIVIL LIBERTIES AND FUNDAMENTAL RIGHTS

Charles Raab, University of Edinburgh

6.1 INTRODUCTION

Charles Raab, University of Edinburgh

6.1.1 Task description

This chapter examines surveillance systems, especially since 9/11, in terms of their protection or infringement of civil liberties and fundamental rights and ethical aspects. We review the literature dealing with the impact of surveillance on privacy, autonomy, dignity, freedom of speech, freedom of association, freedom of movement, non-discrimination, social integration, due process and the presumption of innocence. We consider the effects on particular rights or values of particular people. We will also examine the impacts of fundamental rights and values on surveillance systems, i.e., how they affect the design, deployment and oversight of surveillance systems. Finally, we identify instances of "best practice" where surveillance systems have the least negative impact on fundamental rights while still being (seen as) relatively effective.

6.1.2 Overview

We first examine the propensity of surveillance systems to infringe fundamental rights and values. Distinguishing between different forms of surveillance, we draw on the literature dealing with the impact of surveillance on a variety of specific but inter-related rights, freedoms and values that are considered to be at risk through the use of surveillance technologies and systems. We start by commenting on the effects of surveillance on privacy, dignity, autonomy and various rights and freedoms as well as values.

Going beyond privacy, the effects of surveillance on different categories of people are examined. This is a neglected focus in many sources on privacy, which deal with "data subjects" as legal abstractions who have rights, but which rarely investigate the differentiated, and often systematically biased, effects of surveillance on various social categories. Scholars in the emerging field of surveillance studies as well as others, however, regard the social patterning of surveillance and the unevenly distributed ability of individuals and groups to have their privacy protected as an essential focus of analysis and policy.

Turning the question around, we consider the impacts of fundamental rights and values on surveillance systems in terms of how they might affect the design, deployment and oversight of surveillance systems, in the light of the current emphasis being given by those who are involved in regulation and governance to ways of mitigating surveillance through technological and systemic measures. We identify some instances of good practice, where surveillance systems have the least negative impact on fundamental rights while still being (seen as) relatively effective.

6.1.3 Surveillance – a variety of practices

In order to assess the effect of surveillance on human values and rights, and to assess the effect of these rights and values on the design of surveillance systems, it is important to consider the meaning of key terms: in this Introduction, "surveillance" and "privacy" are considered. For analytical precision, the term "surveillance" must be disaggregated into a variety of types that are used singly or in combination in many different situations and locations: in transport facilities, public space, private premises, in the "virtual" worlds of databases, communications facilities and online transactions. Although there are many overlaps as well as deliberate combinations of techniques, several types of surveillance are mentioned: they include watching, listening, locating, detecting, and personal data monitoring ('dataveillance'). Some types are targeted on particular individuals, groups or social categories of persons, while others operate generically.

Any consideration of the effects of surveillance must specify what types are under examination, operating in what situations, targeting what persons or groups, and for what purposes. For example, visual surveillance is practised in public spaces and in private premises such as shops and office buildings to detect or prevent crime and anti-social behaviour. Surveillance by eavesdropping or wiretapping (and wireless-tapping) – with or without judicial authorisation – usually targets individuals rather than groups for many purposes including counter-terrorism and combating organised crime. Location tracking is built into many products and services, including social networking tools and mobile telephony, to keep track of and control convicted criminals, wayward school pupils, suspicious persons, and others. It is used in vehicle safety systems, often anonymously but sometimes with discriminatory effects, in road-charging schemes, and in many communications devices and infrastructures. Some forms of surveillance involve detection by means of technologies of ubiquitous computing or ambient intelligence, e.g., networking sensors and actuators, sometimes referred to as "smart dust", and radio-frequency identification (RFID) devices. Other technologies – still experimental – propose to detect "abnormal" patterns of behaviour of suspicious characters in certain places and contexts.

Dataveillance – the intensive and extensive use and analysis of database information – is a main means of surveillance in the Internet era. It is a defining characteristic of the modern bureaucratic state, building upon the historic use of records gathered and stored by older technologies, and it is essential to the functioning and profitability of the modern economy as well as to the conduct of social and interpersonal relationships. Various dataveillance applications, including data monitoring, sharing, aggregation and mining, are used in the provision of public services and in marketing. Online monitoring of what people download or of what websites they visit is also a form of dataveillance. So, too, is the retention and analysis of electronic records of telephone calls and Internet usage for law-enforcement and counter-terrorism purposes. Online social networking would hardly be possible without the data sources that enable connections to be made.

All forms and practices of surveillance give rise to debate over the social, economic and individual benefits that result, and about the detriment to individual privacy and freedoms or to the texture of social life and relationships. There are several inter-related issues here. The first is the extent of its visibility: surveillance can be visible or invisible, leaving individuals uncertain about when, where or how they are being monitored. The second is legality: it is not always certain whether a particular surveillance practice is legal or not, and the grounds for legality vary across jurisdictions. Some practices may lead to questioning about their

proportionality, necessity or compatibility with the target's "reasonable expectation of privacy". The third issue is surveillance's power implications concerning the complex and nuanced relationship between the surveillants and the surveilled, where the latter is at a disadvantage to the former, perhaps resulting in other adversities flowing from the surveillance itself. However, it is not assumed that surveillance practices are necessarily ominous in either the intent of their operators and designers, or the chain of untended consequences that result. It is important to take as unbiased a position as possible if the analysis of these phenomena is to command widespread respect.

6.1.4 Privacy – a range of values and rights

"Privacy" is another key term, but whether this is a descriptive or a normative term has been debated. We do not aim to enter this debate, or to embark on a fruitless chase after a singular, clear definition. But it can be noted that the many sources that have attempted – and failed – to achieve this have nevertheless cast light on a host of relevant issues despite the continuing controversy over definitions. A reasonable position for present purposes is to recognise that the various definitions of privacy share a "family resemblance", as Daniel Solove has posited.[1] The unitary concept can be divided into many categories for analytical convenience but also in the interests of seeing how different technologies or practices affect different dimensions of privacy. Information privacy is only one of these dimensions, most frequently addressed in terms of data protection, but it is important to note that surveillance may have an effect upon a wider range of personal attributes and that the mitigation of these effects may require measures beyond those of data protection as such.

As with surveillance, privacy must be disaggregated along, and within, several dimensions for more precise use in analysis and policy-making. Here it is useful to distinguish between seven types of privacy: privacy of the person, privacy of behaviour and action, privacy of personal communication, privacy of data and image, privacy of thoughts and feelings, privacy of location and space, and privacy of association (including group privacy).[2] Modern surveillance technologies affect these types in different ways, so that it makes analytical (and regulatory) sense to disaggregate the concept privacy as far as possible. This is so, even though there are many overlaps among the various types, and only a rough correlation between types of surveillance and types of privacy.

Other categorisations of privacy are available, perhaps putting the types into different language that is compatible with several of these. Six general and overlapping types of privacy are sometimes identified: the right to be let alone, limited access to the self, secrecy, control over personal information, personhood, and intimacy. However, these are often too broad or too narrow for use in empirical analysis, and they suffer from the attempt to define the essence of privacy in terms of common elements that are shared by these types. Another well-known classification concerns "states of privacy": solitude, reserve, intimacy and anonymity.[3] These categorical schemes are touched on in the light of the main aim.

In addition to the question of categorisation, a variety of values are said to be associated with, or even incorporated within the meaning of, privacy. These include autonomy, dignity, liberty, personality and self-determination. Each of these, and all of them taken together,

[1] Solove, Daniel, *Understanding Privacy*, Harvard University Press, Cambridge, MA, 2008, p. 40.
[2] Finn, Rachel, David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes, Paul De Hert et al., *European data protection: coming of age?*, Springer, Dordrecht, 2013.
[3] Westin, Alan, *Privacy and Freedom*, Atheneum, New York, 1967, p. 31.

express something of the essence of being human that needs to be protected or nurtured above all else, although in specific and circumscribed instances, it may be necessary to set privacy aside in favour of the preservation or achievement of other equally, or more, important human values. The interests of national security, the public interest and the common good are typical trump-cards used against the privacy right or interest, although the playing of these cards is controversial and subject to judicial challenge in many countries. As is indicated, the emphasis on autonomy and dignity point up the deontological nature of rights-based constructions of privacy, as contrasted with consequentialist or interest-based utilitarian arguments that involve weighing the desirable outcomes of information processing, or other practices impinging on privacy, against the value of privacy protection for individuals. The "four-states-of-privacy" concept closely connected to utilitarian perspectives on privacy, rather than to those based on rights or ethics.

It is less frequently recognised that privacy is of value for society and political systems, in addition to its importance as an individual right. In this sense, it is relevant to consider – as is done here – the important values of social integration, political democracy, the rule of law and equality of treatment across individuals and groups; these values may be threatened when privacy is invaded, as some writers have argued. This trans-individual dimension of privacy is examined, including the question of how the effects of surveillance upon the values involved can be mitigated.

6.1.5 The importance of context

A final introductory remark is that this chapter endorses a growing trend in contemporary discussions of privacy and surveillance: emphasising the importance of *context* in any proper understanding of the way privacy works in myriad situations in which norms operate to shape relationships, interactions and outlooks. Grasping the idea that one should understand privacy by reference to the violation of informational norms that are relevant to the particular social context in which relationships and activities occur is one way of side-stepping endless definitional controversies because it accommodates contrasting conceptions. There is a strong tradition in sociology – but which has resonance in other academic fields – that looks in a microscopic fashion at social interaction in various settings, and between different kinds of people, in which privacy and personal identity are at stake. Situational norms shape, and are shaped, by such encounters in social contexts that may range from the highly structured to those that may be fleeting but nonetheless take place within normative parameters, including expectations of privacy.

An appreciation of context also serves to avoid deterministic and non-empirical suppositions about the implications of technology for society, individuals, rights and values. Studies of surveillance sometimes fall prey to technophobic or technophilic assumptions about these matters, creating either alarm or complacency. We are aware of this danger, and aim to avoid it.

In this chapter, we can only note, but not fully explore, the importance of context in the relationship between surveillance, privacy and other values, and in the mitigating strategies and techniques for placing those relationships on a footing of legality and propriety.

6.2 EFFECTS OF SURVEILLANCE ON PRIVACY, AUTONOMY AND DIGNITY

Charles Raab, University of Edinburgh

6.2.1 Privacy

The many forms of surveillance that have been identified affect privacy, but in different ways and to varying degrees.[4] They also affect the privacy of different kinds of individual or group, but the analysis of those effects is not well developed in the privacy literature although it is at the forefront of the surveillance literature on "social sorting".[5]

If that surveillance impacts upon privacy, it is important to recognise that privacy has been defined in different ways, but that a widely agreed definition remains elusive.[6] It is a difficult term to define because it means different things to different people in different contexts at different times. Many privacy scholars have commented on this difficulty. Whitman, for example, observes that "privacy, fundamentally important though it may be, is an unusually slippery concept. In particular, the sense of what must be kept 'private,' of what must be hidden before the eyes of others, seems to differ strangely from society to society." The "slipperiness" of privacy is compounded by virtue of the fact that the "ideas of privacy have shifted and mutated over time".[7]

Similarly, Solove describes privacy as "a concept in disarray.… Currently, privacy is a sweeping concept, encompassing (among other things), freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations."[8] Solove therefore avoids a search for a single definition, essence or common denominator and adopts a Wittgensteinian approach in which "family resemblances" are seen in the plurality of contexts in which privacy problems are said to arise, so that privacy becomes an "umbrella term".[9] This may not be an entirely satisfactory solution, but it avoids endless and fruitless argument over a "true meaning". In this perspective, context and situational norms shaping relationships become an important key to understanding and protecting privacy, as Nissenbaum's analysis shows.[10] These approaches acknowledge that the way privacy is viewed is closely bound up with an understanding the public/private

---

[4] This section draws upon Raab, Charles, and David Wright, "Surveillance: Extending the Limits of Privacy Impact Assessment", in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012, pp. 363-383; Raab, Charles, "Privacy, Social Values and the Public Interest", in Andreas Busch and Jeanette Hofmann (eds.) 'Politik und die Regulierung von Information' ['Politics and the Regulation of Information'], *Politische Vierteljahresschrift* Sonderheft 46, 2012, Nomos Verlagsgesellschaft, Baden-Baden, 2012, pp. 129-151; and on Raab, Charles, and Benjamin Goold, *Protecting Information Privacy*, Research Report RR69, Equality and Human Rights Commission, London, 2011.

[5] For example, Lyon, David (ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge, London, 2003.

[6] Gutwirth, Serge, *Privacy and the Information Age*, Rowman and Littlefield, Lanham, MD, 2002, p. 31. Many canonical articles on the concept of privacy can be found in Schoeman, Ferdinand (ed.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, New York, 1984.

[7] Whitman, James Q., "The Two Western Cultures of Privacy: Dignity Versus Liberty", *The Yale Law Journal*, Vol. 113, 2004, pp. 1151-1221 [pp. 1153-1154].

[8] Solove, Daniel J., *Understanding Privacy*, Harvard University Press, Cambridge MA, 2008, p. 1.

[9] Solove, Daniel J., *Understanding Privacy*, Harvard University Press, Cambridge MA, 2008, ch.3.

[10] Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Stanford, CA, 2010. See also her earlier paper, "Privacy as Contextual Integrity", *Washington Law Review*, Vol. 79, No. 1, 2004, pp. 101-139; other remarks on wider varieties of context are found in Gutwirth, Serge, *Privacy and the Information Age*, Rowman and Littlefield, Lanham, MD, 2002, p. 29.

divide, and that this boundary is constantly shifting as a result of the ever-changing relationship between the individual and the state, or the "surveillance state". Finally, this broad approach to privacy helps to ensure that privacy is not simply regarded as a function of person or of place, but rather as a product of the two, and that one does not fall into the trap of thinking that privacy is just about confidentiality or good data management or data protection practices. Moreover, it avoids the fallacy of thinking that particular surveillance technologies or systems inevitably impact privacy in known and determinate ways.

Just as there is no agreed single definition of privacy, there are also many different but overlapping ways in which privacy can be understood and justified, and its erosion criticised. As Lindsay points out in distinguishing between deontological and consequentialist constructions of the concept,[11] privacy can be seen as a good in itself, as essential to our development as individuals and bound up with ideas of dignity, liberty, and personhood; and privacy can also be justified for the individual on more instrumental grounds. Without a degree of privacy, individuals cannot easily maintain an individually and socially important distinction between their personal and public lives, or exercise other important social and political rights, such as rights to freedom of religion, freedom of association and freedom of expression. In this section and later parts of this chapter, these further facets of privacy and freedoms are explored in terms of their relationship to surveillance. However, the intrinsic/functional distinction should not be too sharply drawn, because most privacy discourse embraces both emphases; indeed, Rössler claims that "most of the definitions and explanations of privacy to be found in the literature are 'functional' or can at last be interpreted as such".[12]

Westin's four "states" of privacy: intimacy, anonymity, solitude, and reserve,[13] are convenient rubrics under which many or most of the dimensions and values of privacy, as well as the consequences of surveillance, can be understood. However, there are many overlapping meanings of the concept of privacy even when simplified into such a fourfold conception. The 'right to be let alone', is perhaps the classic one, enunciated by Warren and Brandeis.[14] It denotes the ability of individuals to keep society and the state at bay, and to obtain a remedy where there has been an unwanted intrusion. Broader than this, privacy as limited access to the self is based on the idea that individuals should be able to control access to both their person and to information about them, and is often linked to arguments about "informational self-determination". Privacy has also been seen, both favourably and critically, in terms of secrecy;[15] as protective of the individual's personality, sense of self, and moral title to her autonomous existence;[16] and as an aspect of personhood which is associated with dignity, autonomy and the ability to form meaningful relationships with others.[17] Autonomy and

[11] Lindsay, David, "An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law", *Melbourne University Law Review*, Vol. 29, 2005, p. 179 (online pagination: 1-45), Sections III-B and V-A. http://www.austlii.edu.au/au/journals/MULR/2005/4.html

[12] Rössler, Beate, *The Value of Privacy*, Polity Press, Cambridge, 2005, p. 69.

[13] Westin, Alan F., *Privacy and Freedom*, Atheneum, New York, 1967, pp. 31-32.

[14] Warren, Samuel D., and Louis D. Brandeis (1890) "The right to privacy", *Harvard Law Review*, Vol. 4, 1890, pp. 193-220.

[15] Posner, Richard, "Privacy, secrecy and reputation", *Buffalo Law Review*, Vol. 28, 1979, pp. 1-55.

[16] Reiman, Jeffrey H., "Privacy, intimacy and personhood", *Philosophy & Public Affairs*, Vol. 6, No. 1, Fall 1976, pp. 26-44; Benn, Stanley I., "Privacy, freedom and respect for persons", in J. Roland Pennock and John W. Chapman (eds.), *Nomos XIII: Privacy*, Atherton Press, New York, 1971, pp. 1-26.

[17] Variously, 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; Rachels, James, "Why privacy is important", *Philosophy & Public Affairs*, Vol. 4, No. 4, Summer 1975, pp. 323-333; Fried, Charles, "Privacy", *Yale Law Journal*, Vol. 77, 1968, pp. 475-493; and Rössler, Beate, *The Value of Privacy*, Polity Press, Cambridge, 2005.

dignity are discussed below.

These perspectives on the intrinsic value of privacy often merge, in a functionalist or consequentialist frame, with privacy's importance for the individual in the formation and maintenance of these interpersonal and social relationships.[18] For many writers, privacy is important because it is a value inherent in a liberal society, and is to be defended for that reason; invasions of privacy potentially threaten the persistence of a form of society in which individuals can live their lives within the limited and necessary constraints of state or social control. It is one step from there to a more persistent emphasis on the social and political values of privacy, in which privacy is seen by a variety of authors as indispensable for a liberal, democratic, pluralist society with a multiplicity of social relationships and groups at different levels of scale, from the intimate up to the maximal society. It is also seen as a foundation stone of political democracy and of a panoply of human or civil rights.[19]

Finn *et al.*'s delineation of seven types of privacy, which are not completely discrete, can be partially mapped onto the facets discussed above, and it also introduces dimensions that combine with them in different ways.[20] Nonetheless, using this scheme makes it possible to be more precise about how particular surveillance technologies affect different types of privacy. Their seven types of privacy are:

- the person[21]
- behaviour and location
- communication
- data and image
- thoughts and feelings
- location and space
- association (including group privacy).

The technologies these authors discuss are:

- whole-body image scanning
- RFID-enabled travel documents
- unmanned aircraft systems
- second-generation DNA sequencing technologies
- human enhancement
- second-generation biometrics.

Finn *et al.*'s analysis of each privacy type in terms of the effects of each surveillance technology is interesting, drawing attention to overlapping facets and multiple effects. This analysis is too elaborate to reproduce here, but let us consider some of the examples adduced.

---

[18] Gavison, Ruth, "Privacy and the limits of law", *Yale Law Journal*, Vol. 89, 1980, pp. 421-471.

[19] Sources include, variously, Solove, Daniel J., *Understanding Privacy*, Harvard University Press, Cambridge MA, 2008; Regan, Priscilla, *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, Chapel Hill, NC, 1995; Westin, Alan F., *Privacy and Freedom*, Atheneum, New York, 1967; Schoeman, Ferdinand, *Privacy and Social Freedom*, Cambridge University Press, Cambridge, 1992; Raab, Charles, "Privacy, Social Values and the Public Interest", in Andreas Busch and Jeanette Hofmann (eds.) 'Politik und die Regulierung von Information' ['Politics and the Regulation of Information'], *Politische Vierteljahresschrift* Sonderheft 46, Nomos Verlagsgesellschaft, Baden-Baden, 2012, pp. 129-151; Goold, Benjamin, "Surveillance and the political value of privacy", *Amsterdam Law Forum*, Vol. 1, No. 4, 2009, http://amsterdamlawforum.org

[20] Finn, Rachel, David Wright and Michael Friedewald, "Seven Types of Privacy", in Serge Gutwirth, Ronald Leenes, Paul De Hert et al., *European data protection: coming of age?*, Springer, Dordrecht, 2013.

[21] Their understanding of this is in terms of the physical body, rather than of the self or personality.

Body scanners affect the privacy of data and image, and derivatively, of behaviour. RFID-enabled travel documents also affect privacy of behaviour and action, of data, and of location and space. All of these privacy types, plus association, are affected by unmanned aircraft systems, or drones, while the privacy of the person is additionally implicated by DNA sequencing technologies. Human enhancement through, for example, neuro-enhancing pharmaceuticals and electroencephalography, potentially impact upon all of these plus the privacy of thoughts and feelings. The privacy of communication, in addition to the other types, comes into question through the use of biometrics such as voice and speech recognition technologies.[22]

These are interesting and fruitful lines of enquiry. As mentioned, one should not, however, suppose that these effects on privacy are inevitable or highly likely, nor that the effects on privacy are all of the same seriousness or are unrestrained by regulatory measures of governance. In other words, the risk of harm to privacy cannot be read off from knowledge of what a technology can do, and must be empirically investigated bearing in mind the context and the culture, among many other variables. Nor can it be claimed that all uses of surveillance technologies are inherently detrimental to privacy and the other human values or rights associated with it. However, the message conveyed by Finn *et al.* is that "scholars, legal theorists, policy makers and other actors must maintain an awareness that there are different types of privacy in order to ensure adequate protection of individuals (and society) in relation to existing and emerging technologies, applications and practices".[23] The focus now shifts to an examination of the effects of surveillance on two of the principal value dimensions of privacy described in more classical literature.

6.2.2 Autonomy

There is a strong emphasis on the value of the autonomous individual in the literature on privacy, whether as a distinct element or intertwined with other values such as dignity and liberty. Even the emphasis on withdrawing, temporarily or permanently, from the gaze of others behind a wall of secrecy or solitude is inspired by the importance of conducting one's life autonomously, free of external control or influence and manifesting one's preferences and personality in the choices one makes, even in the choice – not really paradoxical – of which social relationships to engage. Benn claims that we become autonomous by practising independent judgement. Although privacy protects the possibility of this, it is not, he maintains, a consequentialist or utilitarian argument for privacy: autonomy is premised, instead, on respect for persons, in which any role that privacy may play in increasing the chances of independent decision is not the central point. He argues that a person, and not her privacy as such, deserves respect, and is entitled to pursue her decisions and purposes unobserved. This is especially so if the observation or spying is covert, unknown by the person concerned who is thereby deceived and prevented from making rational decisions because the conditions of her action have been altered by the surveillance. This is why the operation of dataveillance and databases without the knowledge or consent of the individual violates respect for persons, even if there are laws safeguarding against abuse. But there may

[22] Finn, Rachel, David Wright and Michael Friedewald, "Seven Types of Privacy", in Serge Gutwirth, Ronald Leenes, Paul De Hert et al., *European data protection: coming of age?*, Springer, Dordrecht, 2013, pp. 3-32 [pp. 6-18].
[23] Ibid., p. 19.

be justifiable, public-interest grounds for overriding privacy through the work of a free press.[24]

Respect for the person also plays an important part in Fried's utilitarian analysis.[25] Privacy is the necessary context for respect, love, friendship and trust; it is a principle of morality that persons as persons have the right to be respected as ends by each other. Fried instances electronic monitoring, involving data on location, conversations, and other kinds including blood pressure, pulse rate and even brain-wave patterns, as an intolerable violation of privacy. Not only does it remove from the individual the power to control her information, it also interferes with intimacy, and thus friendship, love and the ability to enter into trusting relationships. It alters the context for these relations by eliminating the person's control over her environment that privacy would provide as the condition for autonomous action. This kind of electronic tagging pertains not only to the probationers whom Fried had primarily in mind more than a generation ago, for it can now be implemented remotely from any person's body. It may therefore affect privacy seen in terms of autonomy, but not exclusively seen in that light, because it intersects with other types of privacy as well, including thought and behaviour, and location. Nissenbaum, for example, remarks that freedom from tracking contributes to autonomy and freedom of thought and action.[26]

Privacy seen in terms of moral autonomy is central to the way Rössler connects privacy with freedom: "[t]he concept of freedom that I wish to elucidate defines the core of modern freedom as individual autonomy. A person is autonomous if she can ask herself the question what sort of person she wants to be, how she wants to live, and if she can then live in this way. Such personal autonomy…is determined on the one hand by subjective abilities, while on the other hand external conditions are necessary for its success."[27] Some of the implications of surveillance for autonomy are highlighted in her analysis. Resembling Benn's argument, Rössler's discussion of informational privacy – decisional and local privacy are the other types she considers – instantiates voyeurism, video surveillance in public places and the surreptitious access to one's personal and sensitive data by someone to whom the individual has not given consent, as technologies and practices that infringe autonomy.[28] More generally, the technologies that are adversely consequential for information privacy and thus autonomy include "[t]he taping of telephones, CCTV and video surveillance of shops and public spaces, 'tracing' on the internet, data transmission between firms or insurance companies, and the audiovisual supervision of houses and flats".[29]

There thus appears to be a consensus, with some variations, among prominent contributors to theorising the relationship between privacy for autonomy, that there are threats to autonomy from surveillance technologies and practices that have an impact on privacy, when the latter is seen in terms of other values that privacy either helps to realise or with which it is closely associated. These perspectives deal mainly, if not exclusively, with the privacy of the individual, seen as a right and/or as a value. The other side of the coin is the importance of privacy for social and political relationships, not as superseding its importance to the freedom,

[24] Benn, Stanley I., "Privacy, freedom, and respect for persons", in J. Roland Pennock and John W. Chapman (eds.), *Nomos XIII: Privacy*, Atherton Press, New York, 1971, pp. 1-26.
[25] Fried, Charles, "Privacy", *Yale Law Journal*, Vol. 77, 1968, pp. 475-493.
[26] Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Stanford, CA, 2010, p. 82.
[27] Rössler, Beate, *The Value of Privacy*, Polity Press, Cambridge, 2005, p. 17.
[28] Ibid., pp. 114-115.
[29] Ibid., p. 119.

autonomy or dignity of the individual, but as correlative in a rounded view of privacy.[30] Some of the freedoms associated with this, the effects of surveillance upon them, and the wider social consequences of surveillance are discussed below.

6.2.3 Dignity

As has been seen, dignity is a privacy value, and some have argued that it is one of the main ones associated with privacy. Post clarifies the importance of privacy-as-dignity by locating dignity within social structures and norms:

> To equate privacy with dignity is to ground privacy in social forms of respect that we owe each other as members of a common community. So understood, privacy presupposes persons who are socially embedded, whose identity and self-worth depend upon the performance of social norms, … If privacy is conceived as a form of dignity, it presupposes a particular kind of social structure in which persons are joined by common norms that govern the forms of their social interactions. These norms constitute the decencies of civilization.… Privacy as dignity locates privacy in precisely the aspects of social life that are shared and mutual. Invading privacy causes injury because we are socialized to experience common norms as essential prerequisites of our own identity and self-respect.[31]

Whitman claims that "[c]ontinental privacy protections are, at their core, a form of protection of a right to *respect* and *personal dignity*.… On the Continent, the protection of personal dignity has been a consuming concern for many generations."[32] Relatively, but not absolutely,[33] he contrasts this concern for one's image, name and reputation with the American conception of privacy in terms of liberty against the state, and distinguishes between the need for dignity and those market operations that commodify consumer data.

Some of the reasons for protecting privacy are principally concerned with what it is to be an individual person endowed with morally significant attributes, whereas others lean more in the direction of the social utilitarianism of individual privacy. It has been argued that these categories are not distinct; but in any case human dignity is closer to the first than the second. Warren and Brandeis' "right to be let alone"[34] seeks to protect the individual's private domain, personality, self-esteem and the opinion others hold about this individual, in the face of the dissemination of facts about her private life. Prosser reduces this privacy interest to several other non-privacy ones, to be protected legally by torts relating to several types of intrusion.[35] Others, perhaps most prominently Bloustein, rebut this by arguing that this ignores the moral distinctiveness of privacy in terms of the value of dignity and individuality.[36]

---

[30] See Schoeman, Ferdinand (ed.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, New York NY, 1984, pp. 8, 22-26 and the literature cited therein.

[31] Post, Robert, "Three concepts of privacy", *Georgetown Law Review*, Vol. 89, 2000-01, pp. 2087-2098 [pp. 2092-2094].

[32] Whitmore, James Q., "The Two Western Cultures of Privacy: Dignity versus Liberty", *Yale Law Journal*, Vol. 113, 2004, pp. 1151-1221 [p. 1161]; emphasis in original.

[33] Ibid., p. 1163: "One's sense of personhood can be grounded just as much in an attachment to liberty as in an attachment to dignity."

[34] Warren, Samuel D., and Louis D. Brandeis, "The right to privacy", *Harvard Law Review*, Vol. 4, 1890, pp. 193-220.

[35] Prosser, William, "Privacy", *California Law Review*, Vol. 48, 1960, pp. 338-343.

[36] 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 [p. 1003]: "The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been

Although it is difficult to separate dignity from other values that comprise individual personality, it is clear that surveillance in its different forms may have an adverse effect on dignity and its penumbra of connotations. As in the general case of privacy discussed earlier, certain technologies may constitute a striking affront to a person's dignity by increasing the likelihood of personal embarrassment. For example, airport security routines, especially as they involve body scanning,[37] pat-downs, and divestment of clothing and shoes, make it difficult for people to maintain their dignity in circumstances that appear to place them under suspicion until the technology and employees' activities declare them to be "clean"; the importance of the presumption of innocence is discussed below. If the images of the body that are captured through scanning technology reveal evidence of prosthetic devices or physical alterations connected with the treatment of certain diseases, the individual may feel that her dignity has been infringed, even if the images are only available to a small number of security staff. Some of the social norms constituting the decencies of civilisation are suspended, albeit temporarily, but they may, over time, exert an influence over behaviour in other settings, to the extent that *in*dignity becomes the new norm, and the reasonable expectation of privacy changes empirically, if not normatively. The offence to dignity can be said to have been committed even if there are convincing public security interests that override this dimension of privacy.

Another illustration is the way in which DNA technologies[38] may reveal embarrassing information about a person's physical being that she would regard as discrediting, making it difficult to maintain or re-establish her dignity. This information may be sensitive, indicating something about sex, ethnicity, mental and physical health, and other features that the individual would otherwise seek to manage or conceal, partly for reasons of self-image and self-respect, but also because there may be further functional and social consequences of such revelation. Nonetheless, dignity values are implicated, although the management of DNA sequencing systems and their implementation in practical applications could be performed in ways that minimise the effects on dignity and on other dimensions or types of privacy. Much the same could be said of sophisticated applications of biometrics that identify and classify people according to physical or behavioural traits that the individual may wish to conceal as essential to her dignity.[39] Goffman discusses the way physically or morally stigmatised, "discredited" persons, or persons who may be "discreditable", attempt to control the impressions they make and the information they might convey to others about their (ab)normality and identity.[40] This is relevant to an understanding of the creation and re-creation of social norms in interactions, including interaction norms of tacit agreement not to undermine the image the individual wishes to project. The tension inherent in these social situations may be exacerbated to the extent that technologies are available that, through the revelation of certain information beyond the control of the individual, might contribute to the

---

deprived of his individuality and human dignity. Such an individual merges 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. Such a being, although sentient, is fungible; he is not an individual." See the discussion in Schoeman, Ferdinand, "Privacy: philosophical dimensions of the literature", in Ferdinand Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, New York, NY, 1984, pp. 1-33.

[37] Finn, Wright and l Friedewald, op. cit., pp. 7-8.

[38] Ibid., pp. 11-13.

[39] Ibid., pp. 15-18.

[40] Goffman, Erving, *Stigma: Notes on the Management of Spoiled Identity*, Penguin Books, Harmondsworth, 1968.

damage to dignity that could result through discrediting and unmasking. There may, of course, be practical concerns and ulterior motives involved with the desire to maintain one's dignity in such encounters; dignity is not the only value at stake.

In sum, autonomy and dignity are important dimensions, whether as part of privacy or alongside it, but they do not fully comprise the totality of values or rights that surveillance might affect adversely. There are several freedoms that are also crucial for the functioning of democratic societies and for the enjoyment of human or civil rights, and these are discussed next.

6.3 EFFECTS OF SURVEILLANCE ON FREEDOM OF ASSEMBLY AND ASSOCIATION, AND ON FREEDOM OF EXPRESSION

Dara Hallinan, Fraunhofer ISI

Freedom of assembly and association are enshrined as fundamental rights in Article 12 of the EU Charter of Fundamental Rights and as human rights in (amongst others) Article 11 of the ECHR.[41] Freedom of expression is enshrined as a fundamental right in Article 11 of the EU Charter of Fundamental Rights and as a human right in (amongst others) Article 10 of the ECHR.[42] Freedom of expression essentially protects the right to express oneself and the means one chooses to do it, while freedom of association and assembly protects the right to share one's beliefs or ideas, and to act in a public capacity, in community with others. The centrality of these rights to the European concept of democratic society has been repeatedly clarified by the European Court of Human Rights (ECtHR) in its affirmation of the direct links between them and democracy and pluralism.[43]

In essence, the rights are designed to protect the public sphere[44] from the interference of the government (apart from under certain restrictive "necessity" conditions laid down in the second paragraphs of the articles).[45] They negatively demarcate an area in which the individual and individuals must be left alone by authorities and through this negative demarcation to refrain from all interference, these rights also define the boundaries of state

[41] Article 12, EU Charter of Fundamental Rights, OJ, C 364/10, 18.12.2000; Article 11 European Convention of Human Rights, Council of Europe, 1950. www.echr.coe.int.

[42] Ibid. Article 11 and Article 10. Named 'Freedom of Expression and Information' in the European Charter of Fundamental Rights.

[43] See, for example, the Court's statement in *Stankov*. "The essence of democracy is its capacity to resolve problems through open debate. Sweeping measures of a preventive nature to suppress freedom of assembly and expression other than in cases of incitement to violence or rejection of democratic principles – however shocking and unacceptable certain views or words used may appear to the authorities, and however illegitimate the demands made may be – do a disservice to democracy and often even endanger it. In a democratic society based on the rule of law political ideas which challenge the existing order and whose realisation is advocated by peaceful means must be afforded a proper opportunity of expression through the exercise of the right of assembly as well as by other lawful means." ECtHR (1st sect.), *Stankov a.o. v. Bulgaria* (Appl. No. 29221/95), judgment of 2 October 2001, para. 97.

[44] In this sense, we refer to the public sphere of ideas and the requisite means to express those ideas. Security of the public sphere can clearly have other connotations, for example, the obligation of the state to secure the public sphere from terrorism.

[45] Only convincing and compelling reasons can justify interference. Accordingly, the term "necessity" is not interchangeable with terms such as useful or desirable. See on the meaning of this in the context of the freedom of association: ECtHR (GC), *Maestri v. Italy* (Appl. No. 39748/98), judgment of 17 February 2004, *Rep*. 1998, para. 30 *et seq*.

power and function.[46] The rights thus function on an individual level, providing the individual the freedom to form connections, develop ideas and publicly express themselves alone or in combination with others, without interference from the state. They also function as part of the democratic infrastructure, defining the role of the state in relation to ideas, individuals and groups, and accordingly to the public sphere more generally.

The concept of state interference with these rights is broadly conceived to include any form of interference or exertion of power that could undermine the function of the rights or the enjoyment of the rights, whilst the negative formulation of the role of the state also indicates the obligation to remain neutral to ideas and groupings within the public sphere.[47] ECtHR case law has also confirmed that the state, as a guarantor of human rights, has a positive obligation to secure the conditions permitting the exercise of the rights and the reality of pluralism in society by providing the institutional context in which they can exist *de jure* and *de facto*.[48] Both rights are integrally connected to a number of other rights, particularly those aimed at defining and protecting the public sphere or the development of personality or ideas – for example, freedom of thought, conscience and religion (Article 10 ECHR) and privacy (Article 8 ECHR).[49]

6.3.1 The theoretical impact of surveillance on the public sphere

Surveillance as a tool of the state is an extension of the state apparatus.[50] Accordingly, much state surveillance constitutes interference, although according to necessity, this interference may, in certain situations, be justified and acceptable: for example, when national security or public safety is held to be at stake, justifying limitation of the rights outlined above. Different forms and moments of surveillance will impact the right in different ways. However, there are general features of surveillance that alter the reality of negative non-interference and the theoretical role of state in the model elaborated above, the result of which is a stagnation of the public sphere and a chilling effect on public engagement.[51] Among these features are the following:

First, the right forms part of a model which attempts to provide a separation between the state and the public sphere and give individuals the freedom to engage unhindered and unobserved in public activities, and in public debate in association with others. The act of surveillance

[46] See EU Network of Experts on Fundamental Rights, "Commentary of the Charter of Fundamental Rights of the European Union", June 2006, pp. 124-131.
http://158.109.131.198/catedra/images/experts/COMMENTARY%20OF%20THE%20CHARTER.pdf

[47] See van Dijk, Pieter, Fried van Hoof, Arjen van Rijn and Leo Zwaak (eds.), *Theory and Practice of the European Convention on Human Rights*, Intersentia, Antwerpen/Oxford, 2006, pp. 773-841.

[48] In *Plattform "Ärzte für das Leben!"*, the Court states that: "Genuine, effective freedom of peaceful assembly cannot, therefore, be reduced to a mere duty on the part of the State not to interfere: a purely negative conception would not be compatible with the object and purpose of Article 11 [ECHR]. Like Article 8 [ECHR], Article 11 sometimes requires positive measures to be taken, even in the sphere of relations between individuals, if need be." ECtHR, *Plattform "Ärzte für das Leben! v. Austria* (Appl. No. 10126/82), judgment of 21 June 1988, para. 32.

[49] For a discussion of the close link between the freedom of association and, for instance, the freedom of religion, see: ECtHR(GC), *Hasan & Chaush v. Bulgaria* (Appl. No. 30985/96), judgment of 26 October 2000, para. 62. Links have also been found in relation to the right to a fair trial (Article 6 ECHR) in relation to the granting of legal entity status to an association of individuals and even, in extreme cases, to the right to life (Article 2 ECHR), for example, in a recent case concerning the death of a trade union official last seen with state agents. ECtHR (2nd sect.), *Süheyla Aydin v. Turkey* (Appl. No. 25660/94), judgment of 24 May 2005, para. 203.

[50] Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2007, pp. 94-137.

[51] Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, MIT Press, Cambridge MA, 2006, pp. 33-47.

alters the balance of this separation. It brings the gaze of the government into the realm of the public sphere and accordingly shifts the boundary of this separation – eventually potentially changing the role of the state from that of "negative" independence. The balance between state and public sphere thus alters toward the former, at the expense of the latter.[52]

Further, surveillance, and particularly the development of a culture of surveillance and surveillance employed in a precautionary capacity, undermine the quality and solidity of the separation. The quality of the separation is built firstly around the concept of the state's negative exclusion from the public sphere. Interference is only justified when certain necessity and proportionality criteria, defined narrowly and with a heavy burden of proof of actual wrongdoing, are fulfilled. Surveillance by default, or as a precautionary measure, undermines the solidity of this separation, neither adhering to the ideology of negative exclusion, or to a fulfilment of obligations of necessity, proportionality or burden of proof of wrongdoing, before interference.[53] Surveillance thus tends to reverse the presumption of innocence, as will be discussed later. This has the further structural consequence of undermining the perceived value of these rights and the public sphere against the other goals for which surveillance has been deployed – for example, security.

Finally, Solove argues that surveillance is never value-neutral. Surveillance is an observation, and information collection, mechanism, which can be seen as an extension of an apparatus of directed control from which it cannot be separated. The state's role ceases to be neutral adjudicator and infrastructure provider, but becomes increasingly judgemental – imposing its own normative values through a feedback of surveillance and action.[54] Thus, with the surveillance of the public sphere comes an alteration in the quality of state neutrality toward the content of ideas and activity of citizens and groups within that sphere. Accordingly, not only does the sphere shrink quantitatively, but qualitatively as well.

6.3.2 The practical consequences of surveillance

These theoretical alterations manifest in a variety of forms, with final acts of intervention forming only the end point on a continuum of activity. In fact, it may often not be possible to connect specific surveillance measures to consequences. The public sphere and the activity and thoughts of groups and individuals within that sphere do not exist independently of, and in fact are shaped by, the institutional context supporting them.[55] Surveillance shapes an institutional context of control, rather than of freedom. Indeed the perception or fear of surveillance and of being considered a suspect, and the perception of the consequences it may bring, can be just as detrimental to this sphere as the acts of surveillance themselves.[56]

Surveillance may weaken the human and organisational bonds composing the public sphere through the collection and retention of information on the connections between groups and individuals and the actions in which they engage. Within groups, the threat or knowledge of

---

[52] White, Robin C.A., and Clare Ovey (eds.), *The European Convention on Human Rights*, Oxford University Press, Oxford, 2010, pp. 425-475.
[53] See, for example, ECtHR, *Ezelin v. France* (Appl. No. 11800/85), judgment of 26 April 1991, *Ser.* A, vol. 202-A, para. 53, for a description of the high standard of actual proof of wrongdoing necessary, before interference becomes legitimate.
[54] Solove, Daniel, *The Digital Person*, New York University Press, New York, 2004, pp. 165-188.
[55] Goold, Benjamin, "How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy", in D.W. Schartum (ed.), *Overvåkning i en rettsstat - Surveillance in a Constitutional Government*, Fagbokforlaget, Bergen, 2010, pp. 38-48.
[56] Ibid.

surveillance may make it difficult for the members of that group to communicate (or feel free to communicate) with each other. Equally, should other groups be aware, or believe, that a group or an idea[57] is a target for surveillance, it may make them hesitant to interact with that surveilled group or idea for fear of falling under surveillance themselves. Citizens may also decide to avoid interacting with a group or being thought to be associated with an idea. This may occur as they associate surveillance with guilt or a declaration of social undesirability, or as they wish to avoid becoming the target of surveillance. Indeed the perception of a group or idea being under surveillance may make it very difficult for that group to effectively communicate its message or personality to the public through the stigma of surveillance. This in turn may change the behaviour, composition and focus of the ideas and groups within the public sphere as they try to avoid what may be perceived to draw surveillance attention.[58] In these ways, surveillance may introduce an atmosphere of fear, distrust, and avoidance of engagement in public or collaborative activities: this is the "chilling effect" that has frequently been adduced in contemporary discourse on surveillance.

Accordingly, through the disruption of the bonds and connections, the qualitative dimension of the public sphere changes. In order to ensure survival, the ideas may thus be tailored toward the alteration, with ideas at the fringe of the perceived norm suffering the most.[59] The consequence of this is a reduction of the wealth and breadth of ideas, and a narrowing of the range of public moments of expression; for example, the number of public protests may dwindle. In turn, the possibilities for exchange and development of ideas are restricted, both through the increasing limitation in number and range of ideas represented in the public sphere, and in the breaking or weakening of the bonds which had facilitated cross-fertilisation. A vicious circle can be imagined in which weaker bonds and a shrinking market of ideas feed an institutional context out of which only ever more "sanitised" ideas, and ever fewer ideas, emerge.

The individual's relationship with the public sphere and their perception of public participation thus also changes. As ideas, and groups' voices, are muted or ostracised, individuals will experience a lack of choice and ideas in the public sphere.[60] As a consequence of this stagnation and as a consequence of the awareness of the prevalence of state surveillance, citizens may then be dissuaded from engaging with their peers in political debate, or becoming publicly or politically active.[61] Considering that rights also revolve around the existence of the reality of choice, such developments may render the rights de facto illusory.[62] This will have a knock-on effect on citizens' perceptions of the function of the reality of their possibility to participate, their relationship with social institutions and the

---

[57] As the state becomes a normative presence in the public conversation, it also begins to define the legitimacy of ideas and directions of thought. Accordingly, whilst ideas themselves cannot be surveilled, the area of thought, and the groups, activities and expressions of that thought can form a substance and area to be surveilled.

[58] Starr, Amory, Luis A. Fernandez, Randall Amster, Lesley J. Wood and Manuel J. Caro, "The Impact of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis", *Qualitative Sociology*, Vol. 31, No. 3, 2008, pp 251-270.

[59] Ibid.

[60] Raab, Charles, and Benjamin Goold, "Protecting Information Privacy", Equality and Human Rights Commission, Research report 69, 2011, p. 28.
http://www.equalityhumanrights.com/uploaded_files/research/rr69.pdf

[61] Goold, Benjamin, "CCTV and Human Rights", in European Forum for Urban Security, Roxana Calfa, Sebastian Sperber and Nathalie Bourgeois (eds.), STIBA, Montreuil, 2010, pp. 27-35 [pp. 31-35]. http://cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Publication/CCTV_publication_EN.pdf

[62] Simões, Maria João, "Surveillance: A (Potential) Threat to Political Participation?", The Fifth International Conference on Digital Society, 2011, pp 94-99 [p.95].
http://www.thinkmind.org/index.php?view=article&articleid=icds_2011_3_40_10096

operation of democracy generally.[63] Surveillance may thus impose an individual isolation that is far different from the choice of a "solitude" state of privacy, in Westin's terms.

6.3.3 Surveillance online

The danger of surveillance's ability to impact the freedoms of association and expression is particularly pronounced in the online environment, especially considering the importance of the Internet for communication and the development and dissemination of ideas. First, the nature of online groups and the relationship, definitions and specifics of online environments in relation to the definitions and frameworks created by these rights are uncertain and still forming. For example, when does an online group become a group in the sense of the conception of the right? What constitutes "expression" online and, indeed, in what ways does the online world constitute a "public sphere", and does "the public" retain the same definition online as offline? According to some scholars, it may be that these uncertainties in conception of the digital sphere – and thus in how conventional standards apply – leave legal gaps for the exploitation of power which are not present in the physical world.[64]

Second, the ability to design surveillance invisibly into the infrastructure of the online environment, including the ability to co-opt other actors (for example, Internet providers) into this surveillance may have significant consequences. On the one hand, it alters the level of transparency of surveillance, undermining certain rule-of-law principles on which the rights rely.[65] On the other hand, it creates enormous surveillance potential (in that the informational substance of the online environment lends itself unprecedentedly to collection and processing) combined with unique surveillance possibilities, for example, the possibility to collect and extrapolate novel forms of data from social networks.[66]

Freedom of movement is another important dimension of the public sphere in liberal democratic society. This is discussed next.

6.4 SURVEILLANCE AND FREEDOM OF MOVEMENT

Anthony Amicelle, PRIO

This discussion begins with a relevant quotation:

---

[63] Starr, Amory, Luis A. Fernandez, Randall Amster, Lesley J. Wood and Manuel J. Caro, "The Impact of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis", *Qualitative Sociology*, Vol. 31, No. 3, 2008, pp. 251-270. See also Raab, Charles D., "Privacy, Social Values and the Public Interest", in Andreas Busch and Jeanette Hofmann (eds.) 'Politik und die Regulierung von Information' ['Politics and the Regulation of Information'], *Politische Vierteljahresschrift* Sonderheft 46, Nomos Verlagsgesellschaft, Baden-Baden, 2012, pp. 129-151.

[64] Strandburg, Katherine J., "Surveillance of Emergent Associations: Freedom of Association in a Network Society", in Alessandro Acquisti, Sabrina De Capitani di Vimercati, Stefanos Gritzalis and Costas Lambrinoudakis (eds.), *Digital Privacy: Theory, Technologies, and Practices*, Auerbach Publications, Boca Raton, 2007, pp. 435-459.

[65] Ibid. Also see Akdeniz, Yaman, "Freedom of Expression on the Internet: A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the internet in OSCE participating states", Report, OSCE, Office of the Representative on Freedom of the Media, 2010. http://www.osce.org/fom/80723

[66] Strandburg, Katherine J., "Surveillance of Emergent Associations: Freedom of Association in a Network Society", in Alessandro Acquisti, Sabrina De Capitani di Vimercati, Stefanos Gritzalis and Costas Lambrinoudakis (eds.), *Digital Privacy: Theory, Technologies, and Practices*, Auerbach Publications, Boca Raton, 2007, pp. 435-459.

> It is striking to note how the security problem does not arise in terms of the fence as in the previous age (for which the two symbols were the prison, for internal security, and the border for external security), but of control of flows and movements. The major sites of security are no longer borders that delimit States, but, within the same territory, airports or train stations, that is to say all nodes of communication and exchange. The major issue becomes that of 'traceability': being able to identify each time who moves, where he comes from, where he goes, what he does where he is, and whether he effectively has access to the network in which he moves or whether this network is prohibited for him.[67]

Issues of internal security and terrorism have lent further impetus to the intensification of surveillance operations on many fronts, especially since the tragic events in the USA of 11 September 2001, the Madrid bombings of March 2004 and the London bombings of July 2005. Nevertheless, this trend in surveillance has not led to a general return to state border control and old logics of enclosure. These events have rather served as a catalyst to extend and reconfigure existing processes. The latter are based on a conception of security that moves away from the structuring role of state borders and that focuses on risk management and surveillance at a distance of transnational flows of capitals, goods, persons and services. Although the valorisation of the principle of freedom of movement has remained a fundamental dimension (especially in the European Union), security professionals have increasingly emphasised the risks to this principle.[68] Mobility is interpreted in terms of economic opportunity and security risk alike. It is framed by the conflicting relationship between the "requirements" of prevention and the "imperatives" of circulation. This tension joins the fight against transnational crime and terrorism with the idea that free movement would only be possible inside a secured space in which there is a wide distribution of checkpoints and radars.[69] The acceptance of the relative risk that would be linked to mobility consequently leads to a securitisation of this mobility. Therefore, countermeasures are drawn from a surveillance model that is based on *traceability*.

While it has seemed inconceivable to obstruct the principle of freedom of movement in the so-called age of globalisation, modalities of control and surveillance have been shaped to respect it, and even to serve as a basis for it.[70] The notion of traceability encapsulates the wide set of techniques that would tackle the "dynamic tension between freedom of mobility and the provision of security".[71] First and foremost, traceability techniques are used methodically to collect and store information in order to be able to follow flows (persons, capital, information, products). The implementation of these techniques has led to the re-articulation of the model

---

[67] Gros, Frédéric, Monique Castillo and Antoine Garapon, "De la sécurité nationale à la sécurité humaine", *Raisons politiques*, Vol. 4, No. 32, 2008, p.7. Original quotation: "Il est frappant de constater à quel point le problème de la sécurité ne se pose plus dans les termes de la clôture comme dans l'âge précédent (pour lequel les deux symboles étaient la prison, pour la sécurité intérieure, et la frontière pour la sécurité extérieure), mais dans ceux du contrôle des circulations et des passages. Les grands lieux de la sécurité ne sont plus les frontières qui délimitent les États, mais, à l'intérieur même du territoire, les aéroports ou les gares, c'est-à-dire tous les nœuds de communication et d'échange. Le problème majeur devient celui de la « traçabilité » : pouvoir repérer à chaque moment qui se déplace, d'où il vient, où il va, ce qu'il fait à l'endroit où il est, et s'il a effectivement accès au réseau dans lequel il se meut ou si ce réseau lui est interdit."

[68] Huysmans, Jef, *The politics of insecurity: fear, migration and asylum in the EU*, Routledge, London, 2006.

[69] Stirling-Belin, Florence, "Traçabilité, liberté de circulation et Union européenne", *Revue de la recherche juridique, droit prospectif*, Vol. 30, No. 1, 2005, pp. 409-432.

[70] Biersteker, Thomas, "Targeting terrorist finances: the new challenges of financial market globalization", in Ken Booth and Tim Dunne (eds.), *Worlds in Collision: Terror and the Future of Global Order*, Palgrave/St. Martins, London, 2002, pp.74-84.

[71] Amoore, Louise, Stephen Marmura and Mark Salter, "Editorial: smart borders and mobilities: spaces, zones, enclosures", *Surveillance & Society*, Vol. 5, No. 2, 2008, p. 100.

of the geographical and/or territorial fence and its topology of the "container".[72] Mobility controls have not erased the "logic of enclosure", but they have integrated it towards another configuration and another rationality of flow management. Contrary to previous propositions of territorialised management, techniques of traceability do not block circulation as a whole, but rather monitor and categorise it. The set of traceability techniques intends to differentiate and/or relocate illegitimate flows depending on requests, thresholds and watch lists while enabling the general dynamic of flows.[73] Furthermore, contemporary practices of surveillance at a distance do not oppose but rely on global circulation as a systemic framework. These practices operate through electronic "traces left by everything which moves",[74] that are recorded in databases to identify or recover the "undesirables". Contemporary surveillance is associated with the willingness to take advantage of information technologies in order to identify, monitor and manage the flows.[75]

Hence, a vast literature exists on the management of transnational flows of persons and the transformation of bordering processes.[76] Numerous authors illustrate how data collection and data gathering represent a significant fact of the technological management of European borders.[77] Several European databases are used to monitor movements across borders, inside the European Union as well as at the EU external borders and even outside the EU.[78] Thus, practices of border controls are not only deployed at the border itself or within the EU but also abroad, at consular posts.[79] For instance, the very logic of the Schengen visa consists in

[72] Bigo, Didier, "Du panoptisme au ban-optisme. Les micro-logiques du contrôle dans la mondialisation", in Pierre-Antoine Chardel and Gabriel Rockhill (eds.), *Technologies de contrôle dans la mondialisation. Enjeux politiques, éthiques et esthétiques*, Editions Kimé, Paris, 2009, pp. 59-80.

[73] Torny, Didier, "La traçabilité comme technique de gouvernement des hommes et des choses", *Politix*, No. 44, 1998, pp. 51-75.

[74] Bigo, Didier, "Security: a Field left fallow", in Michael Dillon and Andrew Neal (eds.), *Foucault on Security, Politics and War*, Palgrave Macmillan, Basingstoke, 2008, p. 109.

[75] Levi, Michael, and David Wall, "Technologies, Security, and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society*, Vol. 31, No. 2, 2004, pp. 194-220.

[76] Amoore, Louise, Stephen Marmura and Mark Salter, "Editorial: smart borders and mobilities: spaces, zones, enclosures", *Surveillance & Society*, Vol. 5, No. 2, 2008, pp. 96-101; Andreas, Peter, and Timothy Snyder (eds.), *The Wall around the West: State Borders and Immigration Control in North America and Europe*, Rowman & Littlefield, Lanham, 2000; Bigo, Didier, and Elspeth Guild (eds.), *Controlling Frontiers: Free Movement into and within Europe*, Ashgate, London, 2005; Bonditti, Philippe, "Biométrie et maîtrise des flux: vers une 'geo-technopolis du vivant-en-mobilité'?", *Cultures & Conflits*, No. 58, 2005, pp. 131-154; Groenendijk, Kees, Elspeth Guild and Paul Minderhoud (eds.), *In Search of Europe's Borders*, Kluwer Law International, The Hague, 2003; Jeandesboz, Julien, "Logiques et pratiques de contrôle et de surveillance des frontières de l'Union européenne", in Amandine Scherrer, Emmanuel-Pierre Guittet and Didier Bigo (eds.), *Mobilité(s) sous surveillance: Perspectives croisées UE-Canada*, Athéna, Montréal, 2010.

[77] Broeders, Dennis, "The new digital borders of Europe: EU databases and the surveillance of irregular migrants", *International Sociology*, Vol. 22, No. 1, 2007, pp. 71-92; Brouwer, Evelien, *Digital Borders and real rights: Effective remedies for Third-country national in the Schengen information system*, Martinus Nijhoff Publishers, Leiden 2008.

[78] Geyer, Florian, "Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice", *CHALLENGE Research Paper*, No. 9, 2008.

[79] Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi, *Security technologies and society: A state of the art on security, technology, borders and mobility*, INEX Deliverable D.1.1PRIO, Oslo, 2008; Darley, Mathilde, "Le contrôle migratoire aux frontières Schengen: pratiques et représentations des polices sur la ligne tchéco-autrichienne", *Cultures & Conflits*, No. 71, 2008, pp. 13-30; Faure Atger, Anaïs, "The Abolition of Internal Border Checks in an Enlarged Schengen Area: Freedom of movement or a web of scattered security checks?", *CHALLENGE Research Papers*, No. 8, 2008; Gatev, Ivaylo, "Border Security and the Eastern Neighbourhood: Where Bio-politics and Geopolitics Meet", *European Foreign Affairs Review*, No. 13, 2008, pp. 97-116; Makaremi, Christopher, "Pénalisation de la circulation et reconfigurations de la frontière: le maintien des étrangers en 'zone d'attente'", *Cultures & Conflits*, No. 71, 2008, pp. 55-74.

identifying individuals at their point of departure, before entering the Schengen space.[80] This act of control (i.e., identification) preconditions the surveillance at a distance of flows: "[t]he control should activate extensive monitoring mechanisms that are based on the traceability of the considered subject".[81]

With regard to the freedom of movement of capital, banking institutions have become "traffic wardens" required to assist in regulating the flow of financial traffic with reference to an outsourced surveillance.[82] The surveillance of capital flows establishes banking institutions as protective filters of the international financial architecture. These filters have to freeze the assets of blacklisted persons and entities. They also perform differential risk assessment and management intended to result in the exclusion of illegitimate flows without obstructing the systemic fluidity of movements of money.[83] Banking actors participate in state mechanisms of security to the extent that they have to filter (financial) circulation rather like "the twin and apparently contradictory aims of the airport" in relation to the mobility of people and goods.[84]

As a result, techniques of tracing the flows partly delocalise surveillance sites from geographical borders to various "soft checkpoints"[85] within and outside national territories as well as within electronic circulation channels. Security places are as related to the territorial lines – i.e., "the formal geographical partition of political communities"[86] – as they are to the different communication and exchange nodes.[87] The key issue at stake is the reinforcement of information gathering to increase the routine registering and mining of data to detect illegitimate flows.[88] Consequently, contemporary surveillance mainly aims at organising the three interdependent elements of traceability that refer to (1) the existence of traces (data), (2) the mechanisms to collect the traces (databases), and (3) the structures to analyse the traces (law enforcement, intelligence services, etc.) within an organised system of vigilance.[89] The issue of flow management is neither one of enclosure nor one of full liberation of circulation, but one that refers to the implementation of techniques of surveillance at a distance.

According to the official narrative, traceability will contribute to both ensure systemic fluidity of movements and to know what happens in order to detect the movements of the "undesirables". The multiple soft checkpoints have to carry out sorting processes to identify

---

[80] Bigo, Didier, and Elspeth Guild (eds.), "La logique du visa Schengen: la mise à l'écart des étrangers", *Cultures & Conflits* (special issue), No. 49, 2003.

[81] Bonditti, Philippe, *L'antiterrorisme aux Etats-Unis (1946-2007)*, PhD dissertation, Sciences Po Paris, 2008, p. 501.

[82] Amicelle, Anthony, "Trace my money if you can: European Security Management of Financial Flows", in Ulrika Morth and Karin Svedberg Helgesson (eds.), *Transforming the Public Domain: Privatization, Securitization and Accountability in the Field of AML*, Routledge, London, 2012, pp. 110-131.

[83] See Power, Michael, *Organized Uncertainty: Designing a World of Risk Management*, Oxford University Press, Oxford, 2007; Amoore, Louise, and Marieke De Goede (eds.), *Risk and the War on Terror*, Routledge, London, 2008.

[84] Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2008, p. 123; see also Salter, Mark (ed.), *Politics at the Airport*, University of Minnesota Press, Minneapolis, MN, 2008.

[85] Razac, Olivier, *Histoire politique du barbelé*, Editions Flammarion, Paris, 2009.

[86] Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi, *Security technologies and society: A state of the art on security, technology, borders and mobility*, INEX Deliverable D.1.1, PRIO, Oslo, 2008, p. 16.

[87] Gros, Frédéric, Monique Castillo and Antoine Garapon, "De la sécurité nationale à la sécurité humaine", *Raisons politiques*, Vol. 4, No. 32, 2008, pp. 5-7.

[88] Amoore, Louise, and Marieke De Goede, "Introduction. Data and the war by other means", *Journal of Cultural Economy*, Vol. 5, No. 1, 2012, pp. 3-8.

[89] Hermitte, Marie-Angèle, "La traçabilité des personnes et des choses. Précaution, pouvoirs et maîtrise", in Philippe Pedro (ed.), *Traçabilité et responsabilité*, Economica, Paris, 2003, pp. 1-44.

these "undesirables" in order either to exclude them from the continuous flows or to reinforce their monitoring. Thus, communication nodes such as banks and airports act as data filters[90] that monitor customers to detect and block the blacklisted people. Screening operations have to be carried out related to the development of various watch lists, especially the official lists of individuals and organisations suspected of having ties to terrorist activities.[91] In the wake of 9/11, the prioritisation of the fight against terrorism has led to a new impetus to blacklists. Some states and supranational bodies, most notably the United Nations and the European Union, thus publish their own nominal lists while lists that had been created prior to 2001 experienced considerably heavier use.[92]

Although the principle of data filtering against watch lists is simple in theory, its implementation is much more complicated to the extent that the main purpose consists in sifting databases of customers and thousands or millions of operations on a daily basis. One issue at stake is related to two opposed features that have to be avoided: the false negative and the false positive.[93] On the one hand, the notion of false negative refers to blacklisted persons and entities who have avoided restrictive measures because the competent authorities have failed to detect them and consequently to block them. On the other hand, the notion of false positive is related to organisations and individuals who are not blacklisted but who can be affected by unfair restrictions because they are construed as official suspects. False-positives are mainly related to homonymy cases. This form of error can strongly affect the principle of freedom of movement of people and capital. A false positive person can have his assets frozen (i.e., end of capital mobility), but his own mobility can also be deeply affected to the extent that UN and EU sanctions include a travel ban. Further issues concern the processes by which no-fly lists and blacklists are generated, the transparency and accountability of these processes, and the means of redress available to those who have been thus affected.

Although no official statistics exist on false positives, the existence of "collateral damages" related to blacklists and no-fly lists is acknowledged at the EU and UN level. While the quantity and quality of identifiers are presented as a basic requirement to identify blacklisted people, the lack of identifiers remains a serious problem.[94] The use of filtering tools to process this random quality data is de facto imperfect and it is prone to failures and errors. Moreover, the lack of information is not the only problem to the extent that some official lists include erroneous information. According to a report from the American Justice Department, 24,000 individuals wrongly figured on the FBI's consolidated anti-terrorist list, which included around 400,000 individuals, corresponding to more than one million names and

[90] Lyon, David, "Airport as data-filters: Converging surveillance systems after September 11th", *The Journal of Information, Communication and Ethics in Society*, Vol. 1, No. 1, 2002, pp. 13-20.
[91] Guild, Elspeth, "The Uses and Abuses of Counter-Terrorism Policies in Europe: The Case of the 'Terrorist Lists'", *Journal of Common Market Studies*, Vol. 46, No. 1, 2008, pp. 173-193; Hayes, Ben, and Gavin Sullivan, *Blacklisted: Targeted sanctions, preemptive security and fundamental rights*, ECCHR: 10 years after 9/11 Publication Series, 2010.
[92] Amicelle, Anthony, and Gilles Favarel-Garrigues, "Financial Surveillance: Who cares?", *The Journal of Cultural Economy*, Vol. 5, No. 1, 2012.
[93] Brouwer, Evelien, *Digital Borders and Real Rights: Effective Remedies for Third-country nationals in the Schengen Information System*, Martinus Nijhoff Publishers, Leiden 2008; Ericson, Richard, "Ten Uncertainties of Risk-Management: Approaches to Security", *Canadian Journal of Criminology and Criminal Justice*, Vol. 48, No. 3, 2006, pp. 345-357.
[94] United Nations. Security Council, *Letter dated 13 May 2008 from the Chairman of the Security Council Committee established pursuant to resolution 1267 (1999) concerning Al-Qaida and the Taliban and associated individuals and entities addressed to the President of the Security Council*, S/2008/324, New York, 14 May 2008.

aliases.[95] Various subsets of this list are used by government screeners from airport "no-fly list" processes and visa procedures to local law enforcement checks.[96] These various flaws can have a negative impact on freedom of movement. Indeed, such mistakes and the issue of false positives are associated with significant problems, from bureaucratic inconvenience to serious infringements of mobility.

Furthermore, while traceability is presented as the only way to regulate the contingent order, the desire to trace everything also tends to make suspect any system based on trust and acquaintanceship rather than on conventional paper trails.[97] Hence, traceability is also used to make illegal non-controllable circulations. To be clear, traceability does not stigmatise as such but its usages and official discourses participate in abnormalising the non-traceable. With regards to movements of money, informal fund transfer systems such as *hawala* have been identified as suspicious per se to the extent that they do not provide the paper trails in the ways in which have been prescribed for the formal banking systems.[98] This stigmatisation has had negative consequences on migrant remittances and the movements of money for migrant workers. [99]Therefore, traceability techniques do not avoid tensions with the principle of freedom of movement, collective security and individual liberties.

6.5 SURVEILLANCE AND DISCRIMINATION

Anthiny Amicelle, PRIO

A quotation from David Lyon, perhaps the leading scholar on the subject of surveillance and social sorting, initiates this discussion: "Today's surveillance is a peculiarly ambiguous process in which digital technologies and personal data are fundamentally implicated and meet in software coding that classifies yet more groups in different ways."[100] Contemporary surveillance depends increasingly on the recording, storage, processing and retrieving of electronic personal information to manage and to influence populations' activities through social categorisation.[101] This classifying drive of surveillance represents a "specific form of population targeting via data"[102] that usually relies on automated profiling practices. Automated profiling comprises an amalgam of techniques (software) such as data mining, a "process that has as its goal the transformation of raw data into information that can be

[95] U.S. Department of Justice, Office of the Inspector General Audit Division, *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Process*, 2009.
[96] Amicelle, Anthony, "Towards a 'new' political anatomy of financial surveillance", *Security Dialogue*, Vol. 42, No. 2, 2011, pp. 161-178.
[97] De Goede, Marieke, "Hawala Discourses and the War on Terrorist Finance", *Environment and Planning D: Society and Space*, Vol. 21, No. 5, 2003, pp. 513-532.
[98] Haggerty, Kevin, and Maryam Razavy, "Hawala under Scrutiny: Documentation, Surveillance and Trust", *International Political Sociology*, Vol. 3, No. 2, 2009, pp. 139-155.
[99] Passas, Nikos, "Fighting Terror with Error: The counter-productive regulation of Informal Value Transfers", *Crime, Law & Social Change*, 2006; Maimbo, Samuel Munzele, and Nikos Passas, "The design, development, and implementation of regulatory and supervisory frameworks for informal funds transfer systems", in Thomas Bierstecker and Sue Eckert (eds.), *Countering the Financing of Terrorism*, Routledge, New York, 2008, pp. 179-182.
[100] Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2008, p. 5.
[101] Surveillance Studies Network, *A report on the surveillance society*, Office of the Information Commissioner, Wilmslow, 2006.
[102] Amoore, Louise, and Marieke De Goede, "Introduction. Data and the war by other means", *Journal of Cultural Economy*, Vol. 5, No. 1, 2012, p. 4. See also Hildebrandt, Mireille, "Defining Profiling: A New Type of Knowledge?", in Serge Gutwirth and Mireille Hildebrandt (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Science, Brussels, 2008, pp. 17-45.

utilized as strategic intelligence within the context of an organization's identifiable goals. At its core, data-mining efforts are directed towards the identification of behaviour and status markers that serve as reliable indicators of a probable future."[103] Dataveillance,[104] based on data-mining applications, represents a key feature of contemporary surveillance with the convergent trend of anticipatory orientation and the unending quest for personal data.[105] Furthermore, the systematic use of personal data systems perfectly illustrates the tendency for surveillance devices to function as social sorting processes,[106] i.e., as mechanisms for societal differentiation.[107] The operation of social sorting refers to the classification of people into categories according to varying indicators in order to implement a differential treatment of each category. Consequently, although no individual and social group can expect to be left outside scrutiny anymore,[108] the drive for social categorization indicates that levels and purposes of scrutiny strongly differ depending on the categories into which people are sorted.

Consequently, according to numerous authors, "surveillance as social sorting" is related to "discriminatory" (in the sense of distinguishing between, e.g., A and B) technologies to the extent that social sorting relies on decision support systems that are precisely designed to differentiate and discriminate.[109] Surveillance as social sorting aims at discovering or manufacturing differences in order to act upon these differences. Indeed, the main purpose consists in segmenting and targeting individuals as members of different constructed categories. These decision support systems act "as an aid to discrimination – a choice between entities".[110] They perform so-called "rational discrimination" because they are based on statistics and probability to identify, classify and assess individuals or groups of individuals in order to make decisions. To be clear, this kind of discrimination is not in itself necessarily harmful and social categorisation can exist for various vital purposes. However, "while human life would be unthinkable without social and personal categorization",[111] many studies highlight that the automated sorting by categories of personal data can (re)produce marginalising effects and negative discrimination.[112] Social justice is one of the issues at stake

[103] Gandy, Oscar, "Data mining, surveillance and discrimination in the post 9/11 environment", in Haggerty, Kevin, and Richard Ericson (eds.), *The new politics of surveillance and visibility*, University of Toronto Press, 2006, p. 364.
[104] Clarke, Roger, *Introduction to Dataveillance and information privacy, and definition of terms*, 2006, http://www.rogerclarke.com/DV/Intro.html; Garfinkel, Simson, *Database Nation: The Death of Privacy in the 21st Century*, O'Reilly, Sebastopol, CA, 2000.
[105] Bigo, Didier, "Security: a field left fallow", in Michael Dillon and Andrew Neal (eds.), *Foucault on Security, Politics and War*, Palgrave Macmillan, Basingstoke, 2008, pp. 93-114.
[106] Lyon, David (eds.), *Surveillance as social sorting: Privacy, risk and digital discrimination*, Routledge, London, 2001.
[107] Monahan, Torin, "Editorial: Surveillance and inequality", *Surveillance & Society*, Vol. 5, No. 3, 2008, pp. 217-226.
[108] Haggerty, Kevin, and Richard Ericson (eds.), *The new politics of surveillance and visibility*, University of Toronto Press, 2006; Mathiesen, Thomas, "The viewer society: Michel Foucault's panopticon revisited", *Theoretical criminology*, Vol. 1, No. 2, 1997, pp. 215-234.
[109] Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2008; Gandy, Oscar, *The Panoptic sort: a political economy of personal information*, Westview, Boulder, 1993; Guzik, Keith, "Discrimination by Design: predictive data mining as security practice in the United States' 'war on terrorism'", *Surveillance & Society*, Vol. 7, No. 1, 2009, pp. 1-17.
[110] Gandy, Oscar, *Consumer protection in cyber space*, Communication Policy and Technology Section IAMCR, Istanbul, 2011, p. 2.
[111] Lyon, David (eds.), *Surveillance as social sorting: Privacy, risk and digital discrimination*, Routledge, London, 2001, p. 14.
[112] Monahan, Torin, "Surveillance as governance: social inequality and the pursuit of democratic surveillance", in Kevin Haggerty and Minas Samatas (eds.), *Surveillance and Democracy*, Routledge, New York, 2010, pp. 91-110.

that becomes all the more critical given that the use of sophisticated discriminatory technologies is still growing in the areas of both business and security.

Historically, the strategic use of automated profiling was initially introduced in commercial settings.[113] For instance, customer relationship management (CRM) mainly consists in an information technology tool that has been developed in commercial sectors such as banking and insurance to analyse clients' behaviours in order to identify their potential needs. With regard to consumption as a sphere of surveillance, CRM thus involves "capturing and managing data generated by consumers as they select, purchase, and use products. This, in turn, enables organizations to select, attract, and retain high-value customers. Databases of customer characteristics and buying behavior are used to produce statistical consumer profiles."[114] CRM refers to an opportunity calculus that aims at discerning and constructing differences among customers in order to treat them differently depending on their personal characteristics. Hence, consumer dataveillance aims at facilitating market segmentation to improve marketing in commercial companies and to identify consumer niches. Data-mining techniques hence constitute a significant resource in this business context to discover patterns and distinguish between "risk and value based categories".[115] Personal data represents the critical element of this process to the extent that this information is used and analysed to produce profiles that make possible the differentiation of individuals as consumers who fit into various market segments. While this differentiation is based on virtual profiles, it has concrete implications on individuals' daily lives regarding their choices and chances.

Indeed, this marketing technique determines the range of services offered to clients. Straightforwardly, automated social categorisation aims at targeting and keeping the most profitable customer relationships and dismissing those that are unprofitable or of little value. Although this social sorting process is not necessarily unethical in essence, the systematic use of this method by many firms tends to reinforce disparities and socio-economic inequalities according to numerous authors. With reference to the United States, Oscar Gandy coins the concept of cumulative disadvantage to argue that computer techniques for rational discrimination contribute to maintaining historical disparities that negatively affect the quality of life that "African American and other poor people of color" can hope to enjoy.[116] David Lyon emphasises that the "reinforcing of social and economic inequalities by such means [social sorting] is hardly the 'fault' of some individual firm, but it is a tangible reality for those whose lives are systematically disadvantaged, as it is for those who are privileged".[117]

Moreover, practices of profiling and social categorisation can also result in "rational discrimination" that hides stereotypes and categories that would be declared illegal in other settings, but that attract less attention when these assumptions are embedded in algorithms.[118]

---

[113] Backhouse, James, and Ana Canhoto, "General Description of the Process of Behavioural Profiling", in Serge Gutwirth and Mireille Hildebrandt (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Science, Brussels, 2008, pp. 47-63.

[114] Ball, Kirstie, Elizabeth Daniel, Sally Dibb and Maureen Meadows, "Democracy, surveillance and 'knowing what's good for you': the private sector origins of profiling and the birth of 'citizen relationship management'", in Kevin Haggerty and Minas Samatas (eds.), *Surveillance and Democracy*, Routledge, New York, 2010, pp. 111-126.

[115] Gandy, Oscar, *Coming to terms with chance. Engaging rational discrimination and cumulative disadvantage*, Ashgate, Farnham, 2009, p. 13.

[116] Ibid., p. 12.

[117] Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2008, p. 102.

[118] Solove, Daniel, "Data mining and the security-liberty debate", *University of Chicago Law Review*, Vol. 74, 2008, pp. 343-362. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=990030

For instance, one famous US legal case revealed that a white woman was refused a credit card only because her residential postcode was associated with a predominantly black neighbourhood that was considered to be too risky according to the credit-checking system.[119] This particular example illustrates a form of geo-demographic determinism as well as the broad issue of "categorical vulnerability" in which individuals can suffer from negative discrimination by virtue of being associated with a specific profile. Furthermore, categorical vulnerability is not only a significant issue regarding business strategies. This issue is also pervasive from a security perspective in connection with surveillance practices that have been justified in the name of the fight against terrorism and that often draw upon CRM techniques. Indeed, in recent years, there has been an increasing convergence between commercial and state systems of surveillance that draws attention to digital discrimination.[120] The fight against terrorist financing is a striking example of this tendency. The sorting of financial activities to counter the financing of terrorism becomes a routine task for banking actors that have had to devise and implement procedures for keeping watch over their clientele on behalf of the tasks that governments ask them to perform.[121]

As a result, banking actors use technological tools to categorise clients and transactions in order to detect suspicious activities.[122] These tools offer profiling functions, i.e., techniques of behavioural analysis designed to detect unusual account activity by constructing types of individuals or situations on the basis of scattered data. The correlation of this data and the construction of groups of peers allow one to predict the behaviour of a client and to distinguish deviations from his or her profile. These tools are designed to enable end-users to differentiate between what is "normal" and what is suspicious for each of its business relationships, with real-time payment screening, transaction monitoring and client screening. Profiling software aims at analysing the specific characteristics of every single customer; supporting contextual and historical analysis; recognising risk factors (country risk, product risk, etc.) and known patterns of money laundering and terrorist financing; detecting predetermined risk scenarios. These can be fine-tuned by end-users; and centralising all red flags in a single decision-making unit regardless of where a particular financial transaction occurred. Through the adoption of such an approach, all operations can be examined in real time by a combination of matching techniques such as behavioural profiling, list analysis and comparison with peer groups.[123]

Profiling tools reflect the transformation of tools of seduction (intended to attract and keep clients such as CRM) into tools of suspicion.[124] Before becoming financial security tools, these tools were initially used in banks to analyse the behaviour of clients and identify their potential needs. The ways in which such computer software functions resembles the earlier

[119] Ball, Kirstie, Elizabeth Daniel, Sally Dibb and Maureen Meadows, "Democracy, surveillance and 'knowing what's good for you': the private sector origins of profiling and the birth of 'citizen relationship management'", in Kevin Haggerty and Minas Samatas (eds.), *Surveillance and Democracy*, Routledge, New York, 2010, pp. 111-126.
[120] Lyon, David, *Surveillance after September 11*, Polity Press, Cambridge 2003.
[121] Heng, Yee-Kuang, and Kenneth McDonagh, *Risk, Global Governance and Security: The Other War on Terror*, Routledge, New York, 2009.
[122] Amoore, Louise and Marieke De Goede (eds.), *Risk and the War on Terror*, Routledge, London, 2008; Levi, Michael and David Wall, "Technologies, Security, and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society*, Vol. 31, No. 2, 2004, pp. 194-220.
[123] Amicelle, Anthony, "Towards a 'new' political anatomy of financial surveillance", *Security Dialogue*, Vol. 42, No. 2, 2011, pp. 161-178.
[124] Gandy, Oscar, *The Panoptic sort: a political economy of personal information*, Westview, Boulder, 1993; Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2008; Marx, Gary T., *Undercover: Police Surveillance in America*, University of California Press, Berkeley, CA, 1988.

data-mining exercises that were developed by financial institutions for credit scoring and other types of customer-related assessment.[125] The redeployment of commercial risk equipment in the surveillance technologies used in the fight against "dirty money" has been massive. Many companies now sell "advanced data analysis solutions" and are attempting to capitalise on the growing market opportunities of what Larner calls the institutionalisation of "terrorist risk as a global business practice".[126]

One of the big issues in this respect involves the process of specifying the parameters of these tools and managing the risk categories that influence the eventual decisions. The tasks of defining the criteria used in sorting processes and interpreting the outcomes of those processes mainly fall on financial institutions. Various studies have pointed out that profiling is not just a technical process but also a social one, in which the subjectivities of the analysts play an important role.[127] Profiling operations depend on parameters that correspond to precise regulatory rules (for example, the definition of a transaction threshold beyond which banking vigilance must be reinforced) or are defined according to the priorities of the establishment by compliance officers. The chief compliance officers distinguish not only between at-risk sectors of activity but also the geographical zones that they believe are particularly exposed to money-laundering practices.[128] Profiling techniques thus give an important place to the at-risk countries that appear in transactions. Stereotypes about foreign countries – for example, those located on the African continent or in the post-communist zone – can be held by the chief compliance officers.[129] Their choices are usually made free of any oversight, and they can also help to identify unwanted clients that the bank should shed.[130]

This socio-technical process can have a real impact upon the individuals being profiled. The issue of subjectivity is especially problematic in relation to methods of terrorist fund-raising that are difficult to detect owing to factors such as the relatively low value of the transactions involved, or the use of ordinary financial operations to provide support for terrorist groups.[131] Given the enormous difficulties involved in detection, it would probably be more accurate to argue that regulated actors have to manage situations of uncertainty[132] rather than risks. The

[125] Backhouse, James, and Ana Canhoto, "Profiling under conditions of ambiguity: an application in the financial services industry", *Journal of Retailing and Consumer Services*, Vol. 14, No. 6, 2007, pp. 408-419.
[126] Larner, Wendy, "Spatial imaginaries: economic globalization and the war on terror", in Amoore, Louise, and Marieke De Goede (eds.), *Risk and the War on Terror*, Routledge, London, 2008, p. 51.
[127] Backhouse, James, and Ana Canhoto, "General Description of the Process of Behavioural Profiling", in Serge Gutwirth and Mireille Hildebrandt (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer Science, Brussels, 2008, pp. 47-63; Favarel-Garrigues, Gilles, Thierry Godefroy and Pierre Lascoumes, *Les sentinelles de l'argent sale : les banques aux prises avec l'antiblanchiment*, La Découverte, Paris, 2009.
[128] Amicelle, Anthony, and Gilles Favarel-Garrigues, "Financial Surveillance: Who cares?", *The Journal of Cultural Economy*, Vol. 5, No. 1, 2012.
[129] Amicelle, Anthony, and Gilles Favarel-Garrigues, "Financial Surveillance: Who cares?", *The Journal of Cultural Economy*, Vol. 5, No. 1, 2012; De Goede, Marieke, "Hawala Discourses and the War on Terrorist Finance", *Environment and Planning D: Society and Space*, 2003, Vol. 21, pp. 513-532.
[130] Amicelle, Anthony, and Gilles Favarel-Garrigues, "Financial Surveillance: Who cares?", *The Journal of Cultural Economy*, Vol. 5, No. 1, 2012; Vlcek, William, "Surveillance to combat terrorist financing in Europe: whose liberty, whose security?", *European Security*, Vol. 16, No. 1, 2007, pp. 99-119; Vlcek, William, "A Leviathan Rejuvenated: Surveillance, Money Laundering, and the War on Terror", *International Journal of Politics, Culture and Society*, Vol. 20, Nos. 1-4, 2008, pp. 21-40.
[131] Mitsilegas, Valsamis, "Countering the Chameleon Threat of Dirty Money: 'Hard' and 'Soft' Law in the Emergence of a Global Regime against Money Laundering and Terrorist Finance", in Adam Edwards and Peter Gill (eds.), *Transnational Organised Crime: Perspectives on Global Security*, Routledge, London, 2003, pp. 195-211.
[132] Barthe, Yannick, Michel Callon and Pierre Lascoumes, *Agir dans un monde incertain : essai sur la démocratie technique*, Editions du Seuil, Paris, 2001.

uneasiness of regulated institutions and the managerial focus on technological extrapolations from data may lead to principles of action that negatively discriminate against particular groups or individuals. As the Financial Action Task Force (FATF) guidance document declares, "an over-zealous effort to counter the risks could be damaging and counter-productive, placing unreasonable burdens on industry, and act against the interests of the public by limiting access to financial service for some segments of the population".[133] In other words, the classic argument "if you've got nothing to hide, you've got nothing to fear"[134] is theoretically wrong to the extent that matching with a specific group is sufficient to attract categorical suspicion and possible prejudice.

6.6 THE EFFECTS OF SURVEILLANCE ON SOCIAL INTEGRATION

Gemma Galdon Clavell, UB

Social sorting can connote theories about how societies are constructed, and about the exclusionary effects of the discriminatory processes that have just been seen. The question of discrimination that has just been examined relates closely to the understanding of social integration and the factors, including surveillance, that interfere with its realisation. According to one of its early theorists, Emile Durkheim, social integration involves society's ability to accommodate the structural forces that lead to differentiation and specialisation. In his work, social integration is linked to solidarity, collective consciousness and identity.[135] In more recent accounts, the United Nations defines social integration as "an inclusive society" that "emanates from the well-being of each individual, mutual trust, sense of belonging and inter-connectedness".[136]

When referring to social integration, therefore, we are looking at social relations and the structural and informal elements underpinning them. Surveillance, in its multiple forms, constitutes one of those elements with a potential to impact on the way social relations are practised and organised. In dealing with such a broad concept, however, a degree of categorisation is useful. First, we need to differentiate between formal (rights) and informal (practices) prerogatives and processes of social integration. Second, we need to approach different technologies differently – we suggest a different approach to "dataveillance" (retrieval of digital data from computers or networks) from "physical surveillance" (when the information collected is not digital or only digitalised at the time of collection). In this latter case, because of its impact on one of the main spheres of democratic society-building and interaction – public space[137] – we will concentrate the analysis mainly on CCTV.

Informally, however, processes of social integration and actual enjoyment of rights have a lot to do with attitudes, practices and social constructs. Formal rights and avenues for social integration granted by a formal legal structure (and enabled by surveillance mechanisms)

---

[133] Financial Action Task Force (FATF). *Guidance on the risk-based approach to combating money laundering and terrorist financing: High level principles and procedures*, Paris, 2007, p. 16. http://www.fatf-gafi.org/dataoecd/43/46/38960576.pdf. The FATF is the intergovernmental organisation seeking to develop and promote national and international policies in order to fight against money-laundering and the financing of terrorism. See www.fatf-gafi.org

[134] Solove, Daniel, "'I've got nothing to hide' and other misunderstandings of privacy", *San Diego Law Review*, Vol. 44, November 2007, pp. 745-772.

[135] Durkheim, Emile, *The Division of Labour in Society*, The Free Press, New York, NY, 1997/1933.

[136] Social Policy and Development Division of the UN. http://social.un.org/index/SocialIntegration.aspx

[137] Sennett, Richard, *The Fall of Public Man*, Norton, New York, NY, 1974.

might become irrelevant when they are ignored by social practices or policy developments. This has been observed abundantly in the case of CCTV proliferation and its impact on communities, personal identity, equality of treatment, trust and inclusion. For instance, the freedom to practise one's religion, the right to non-discrimination and the presumption of innocence are curtailed when surveillance is installed in Muslim neighbourhoods on the grounds of terrorism, for instance, as happened in Birmingham in 2010.[138] Young people might enjoy formal equality, but this might not be self-evident to those affected by police profiling practices that, with the help of remote monitoring through CCTV, tend to target subjects on the basis of gender, age and ethnicity.[139] Women might be treated equally by the electronic eye, but as long as their experience of surveillance is different from that of men, this formal equality remains secondary.[140]

Social integration is intimately linked to equality, freedom and identity. However, conceptions of what is appropriate and normal or inappropriate and abnormal depend upon a variety of contextual factors,[141] and as a socio-technical practice surveillance tends to reflect the values of the society that determines that some things or some people need to be monitored and watched.[142] Thus, several authors have observed that surveillance systems are often used in discriminatory ways. Focusing on CCTV – which is by far the surveillance technology that has received most academic attention, and in terms of its social impact – Coleman describes how surveillance can be used to exclude and remove undesirable groups from public space, and how this is linked to the broader process of increasing control and regulation in the social and urban sphere.[143] Moreover, while studying the watchers' attitudes towards the watched, Norris and Armstrong found that their practices were often exclusionary, filled with stereotypes (and sometimes plain racist).[144] Helten and Fisher are among the many scholars to have found an extensive use of external, stereotype-based cues by CCTV operators to decide on who is suspicious or deserves to be monitored in shopping malls.[145] Seabrook and Wattis,[146] Koskela[147] and Helten and Fischer[148] have shown how women experience anxiety and negativity when faced with surveillance. As Seabrook and Wattis point out, "CCTV represents a heightened manifestation of the male gaze with technological advancements allowing men [operators] to put women under surveillance yet

---

138 *The Guardian*, "Police under fire over Muslim CCTV surveillance scheme", 18 June 2010.

139 OSI, *Police Profiling in Europe: Pervasive, Ineffective, and Discriminatory*, Open Society Institute, New York, 2009.

140 Dixon, John, Mark Levine and Rob McAuley, *Street Drinking Legislation, CCTV and public space: exploring attitudes towards public order measures*, Home Office, London, 2003.

141 Lyon, David, *Surveillance after September 11*, Polity Press, Cambridge, 2003.

142 Hadjiyanni, Tasoulla, and Jain Kwon, J., "The Social Dimension of Security: Exploring How Surveillance Systems Relate to Interior Design", *Journal of Interior Design*, Vol. 34, No. 3, 2009, pp. 1-15.

143 Coleman, Roy, *Reclaiming the Streets: Surveillance, Social Control and the City*, Willan Publishing, Cullompton, Devon, 2004.

144 Norris, Clive, and Gary Armstrong, *The maximum surveillance society: The rise of CCTV*, Berg, Oxford, 1999.

145 Helten, Frank, and Bernd Fischer, "Reactive attention: Video surveillance in Berlin shopping malls", *Surveillance & Society*, Vol. 2, Nos. 2/3, 2004, pp. 323-345.

146 Seabrook, Tamara, and Louise Wattis, "The techno-flâneur. Tele-erotic re-presentation of women's life spaces", in E. Leigh Keeble and Brian D. Loader (eds.), *Community informatics: Shaping computer-mediated social relations*, Routledge, London, 2001, pp. 240-259.

147 Koskela, Hille, "Video surveillance, gender, and the safety of public urban space: 'Peeping Tom' goes high tech? ", *Urban Geography*, Vol. 23, 2002, pp. 257-278.

148 Helten, Frank, and Bernd Fischer, "Reactive Attention: Video Surveillance in Berlin Shopping Malls", *Surveillance & Society*, Vol. 2, Nos. 2/3, 2004, pp. 323-345.

again as the sexualized 'other'", and so call for a better understanding of the "subjective nature in which young women come to negotiate their use of public space". [149]

The need to understand the subjective, contextual and diverse negotiation of one's relation to the environment is key to linking surveillance to "informal" social integration or disintegration. Surveillance often has an effect on the way public life is experienced by certain groups, and especially CCTV, as described above, clearly affects some groups' degree of access to public space, with a direct impact on social integration: research shows that exclusionary spatial practices contribute to social exclusion and intolerance.[150] Moreover, CCTV can affect social responsibility by promoting bystander indifference and reducing people's propensity to report crimes to the police.[151]

In their study of CCTV in a shopping mall and a transport centre, Saetnan et al. found a strong link between commercial interests and exclusionary practices, pointing to a further effect of surveillance on social integration that emerges from the relationship between consumption, public space and surveillance.[152] As some authors have highlighted, "mass consumer culture [is] a primary means of social integration and, in the broadest sense, social control in postmodern society".[153] Lyon says, "Social order – and thus a soft form of social control – is maintained through stimulating and channelling consumption, which is where consumer surveillance comes in."[154] If surveillance is used as a way of "sorting" the appropriate from the inappropriate, particularly in commercial public space, this control immediately affects the way different groups use public space and benefit from its qualities, especially the possibility of social integration and community building.[155]

In the formal and physical sphere, surveillance can be said to play a positive role in the sense of being used to extend rights and thus reinforce the institutional elements that enable social integration – or, as Monahan et al. put it, contribute to "individual autonomy and dignity, fairness and due process, community cooperation, social equality, and political and cultural visibility".[156] This understanding of surveillance, still relatively uncommon in the surveillance literature (with some exceptions, such as Ceyhan,[157] Murakami Wood and Firmino,[158] Bruno

---

[149] Seabrook, Tamara, and Louise Wattis, "The techno-flâneur. Tele-erotic re-presentation of women's life spaces", in E. Leigh Keeble and Brian D. Loader (eds.), *Community informatics: Shaping computer-mediated social relations*, London, Routledge, 2001, pp. 240-259 [pp. 258, 259].

[150] Madanipour, Ali, "Social Exclusion and Space", in Richard T. LeGates and Frederic Stout (eds.), *City Reader*, Routledge, New York, 2003, pp. 181-188; Flint, Colin, *Spaces of Hate. Geographies of Discrimination and Intolerance in the USA*, Routledge, New York, 2004; Fyfe, Nicholas R., and Jon Bannister, "City watching: Closed circuit television surveillance in public spaces", *Area*, Vol. 28, No.1, 1996, pp. 37-46.

[151] Fyfe, Nicholas R., and Jon Bannister, "City watching: Closed circuit television surveillance in public spaces", *Area*, Vol. 28, No. 1, 1996, pp. 37-46.

[152] Saetnan, Ann Rudinow, Heidi Mork Lomell and Carsten Wiecek, "Controlling CCTV in Public Spaces: is privacy the (only) issue? Reflections on Norwegian and Danish observations", *Surveillance & Society*, Vol. 2, Nos. 2-3, 2004, pp. 296-414.

[153] Bauman, Zygmunt, *Intimations of postmodernity*, Routledge, New York, 1992; Staples, William G., *Everyday surveillance. Vigilance and visibility in postmodern life*, Rowman & Littlefield, Lanham, MD, 2000.

[154] Lyon, David, *The Electronic Eye: The Rise of Surveillance Society*, Polity Press, Cambridge, 1994, p. 137.

[155] Saetnan, Ann Rudinow, Heidi Mork Lomell and Carsten Wiecek, "Controlling CCTV in Public Spaces: Is Privacy the (Only) Issue? Reflections on Norwegian and Danish Observations", *Surveillance & Society*, Vol. 2, Nos. 2-3, 2004, pp. 296-414.

[156] Monahan, Torin, David J. Phillips and David Murakami Wood, "Editorial. Surveillance and Empowerment", *Surveillance & Society*, Vol. 8, No. 2, 2010, pp. 106-112.

[157] Ceyhan, Ayse, "Téchnologie et sécurité: une gouvernance libérale dans un context d'incertitudes", *Cultures & Conflits*, Vol. 64, Winter 2006, pp. 11-32.

et al.[159]), emphasises the relationship between surveillance-enabled identification and citizenship and/or between identification and increased ease in the use of public resources and facilities. The latter can be found in the case of IDs being issued to previously ostracised communities or land property titles being provided to those once considered illegal and therefore not recognised by the state. Studying an instance of identity fraud in Brazil, Murakami Wood and Firmino compellingly show how in some instances not being part of a national identification scheme can result in fear of exclusion, or "to disappear as the victim of arbitrary forces".[160] In this sense, specific forms of surveillance can be seen as enablers of social integration as they can extend citizenship rights, and therefore an expectation of equality, a shared identity and a sense of belonging, to certain groups of people.

Therefore, while some surveillance mechanisms have been shown to have a positive impact on the enjoyment of specific rights (property, citizenship) and contribute to a more inclusive social infrastructure, in the case of video-surveillance in public space, the tendency to stereotype, discriminate and socially select those who end up being scrutinised by the electronic eye points to a weakening of mutual trust, sense of belonging, connectedness and, to use Durkheim's words, society's ability to resist differentiation and specialisation.

As mentioned above, however, a great deal of surveillance these days is not physical surveillance but dataveillance – that is, "the systematic monitoring of people's actions or communications through the application of information technology".[161] The fact that most people use computers and social networks on a regular basis means that large amounts of data are generated and scrutinised through data-mining processes for policing, commercial or administrative purposes. There is much literature that points to the benefits of social networks for social integration, mainly by facilitating the creation of online support groups and enabling long-distance communication on a regular basis.[162] With the proliferation of RFID, databases and mobile phones, the possibilities for dataveillance escape the computer to enter everyday activities such as getting on a bus, shopping at the supermarket, or going for a walk. However, there is less material to draw from in relation to the benefits and risks of dataveillance. In his early account of dataveillance, Clarke mentions the detection and prevention of various forms of error, abuse and fraud, as well as increased efficiency, as the most noteworthy benefits of such practice. On the other hand, the same author lists a series of dangers that in some instances overlap with those observed in the case of physical surveillance, such as profiling and discrimination. In terms of its impact on social integration, however, the most relevant negative externalities of dataveillance would be, in Clarke's view, the need for some individuals to escape the official radar and opt-out of society and "the weakening of society's moral fibre and cohesion". Others have mentioned how the creation of data profiles can affect people's confidence and ability to succeed in work and life when they

---

158 Murakami Wood, David, and Rodrigo Firmino, "Empowerment or repression? Opening up questions of identification and surveillance in Brazil through a case of 'identity fraud'", *Identity in the Information Society (IDIS)*, Vol. 2, No. 3, 2009, pp. 297-317.

159 Bruno, Fernanda, Marta Kanashiro and Rodrigo Firmino, *Vigilância e Visibilidade. Espaço, Tecnologia e Identificaçâo*, Editora Sulina, Porto Alegre, 2010.

160 Murakami Wood, David, and Rodrigo Firmino, "Empowerment or repression? Opening up questions of identification and surveillance in Brazil through a case of "identity fraud"", *Identity in the Information Society (IDIS)*, Vol. 2, Issue 3, 2009, pp. 297-317 [p. 299].

161 Clarke, Roger, "Information Technology and Dataveillance", in *Communications of the ACM*, 1988, pp. 498-512.

162 See, inter alia, Woolgar, Steve, *Virtual Society? Technology, Cyberbole, Society*, Oxford University Press, Oxford, 2002.

are labelled wrongly or inaccurately.[163] Finally, Amoore and De Goede stress how dataveillance promotes a culture of suspicion and the fact that risk classification designed to trace terrorist financing tends to focus on migrants, students and the unemployed, promoting their financial exclusion, criminalising whole sectors of society and impacting on their well-being and ability to lead normal lives, as well as on society's inclusive character.[164]

Overall, both in the case of physical surveillance and dataveillance, the literature shows that the monitoring of people's activities has social externalities that need to be taken into account. Surveillance can have an impact at the formal or informal levels (rights and practices), and sometimes advances in the formal protection of social inclusion might be overridden by informal, exclusionary practices. Also, some of these externalities can be positive and contribute to people's inclusion in society. Others, however, hinder people's possibilities of social integration, full development and effective enjoyment of rights, and usually do so in discriminatory ways, affecting certain groups more than others. As the literature suggests, there is a need to understand and prevent these social externalities, both at the policy and technological levels, and to re-balance technological possibilities with the need for technological innovation to be put at the service of society's needs in terms of equality and integration.

6.7 EFFECTS OF SURVEILLANCE ON THE RULE OF LAW, AND ON THE PRESUMPTION OF INNOCENCE

Paul De Hert and Antonella Galetta, VUB

The rule of law has been seen as "a system for imposing legal accountability and objectively verifiable standards on activities by public and executive bodies that interfere with people's private activities".[165] This means that only those exercises of authority are legitimate that are carried out under legal authorisation; 'due process of law' forms part of this meaning.

Although surveillance is not a product of modernity, it is a distinctive product of the modern world[166] and a main institutional component.[167] Surveillance is applied in almost every sector of human activity. It suffices to recall that since 9/11, western democracies have carried on the fight against terrorism through a heavy reliance on surveillance technologies. These have been widely accepted in the name of national security in time of emergency, although they are

[163] Donahue, Joseph, Nicholas Whittemore and Ashley Heerman, "Ethical Issues of Data Surveillance", Ethica Publishing, [n.d.] http://www.ethicapublishing.com/ethical/3CH20.pdf

[164] Amoore, Louise, and Marieke De Goede, 'Governance, risk and dataveillance in the war on terror', *Crime, Law & Social Change*, Vol. 43, 2005, pp. 149-173.

[165] Professor David Feldman, reply to Q519, in UK House of Lords, Select Committee on the Constitution, 2nd Report of Session 2008-09, *Surveillance: Citizens and the State*, HL Paper 18-II, Volume II: Evidence, The Stationery Office, London, 2009, p. 196. For further discussion of the rule of law as a concept, its sources and ramifications, and its development in case law, see Turpin, Colin, *British Government and the Constitution: Text, Cases and Materials*, 4th edn., Butterworths, London, 1999, pp. 57-80.

[166] Lyon, David, "Surveillance Technology and Surveillance in Modernity and Technology", in Thomas Misa, Philip Brey and Andrew Feenberg (eds.) *Modernity and Technology*, The MIT Press, Cambridge, MA, 2003, p. 161.

[167] Giddens, Anthony, *The Consequences of Modernity*, Polity Press, Cambridge, 1990, p. 57, and Haggerty, Kevin D., and Richard V. Ericson, "The Surveillant Assemblage", *The British Journal of Sociology*, Vol. 51, No. 4, December 2000, pp. 605-620 [p. 606].
http://www2.lse.ac.uk/BJS/pastVolumes/vol51/sur400.aspx

indiscriminate, pervasive, fluid and invisible, and share this with the phenomenon of terrorism that they are intended to combat.[168]

These features of surveillance – indiscriminate, pervasive, fluid and invisible – evidently raise democratic and human rights concerns. Even though critiques of surveillance are most frequently framed in terms of privacy,[169] an assessment of the pervasive effects of surveillance on the principles of the presumption of innocence and the due process of law has also to be taken into account, considering that criminal law can be considered as one of the battlefields on which surveillance and human rights confront each other.

This subsection focuses on the impact of surveillance on due process and the presumption of innocence, two key values in criminal law. In doing so, it highlights the legal documents and some of the case law that has clarified the nature and extent of these rights and principles. First, the nature of this field of law is briefly discussed, paying attention to recent changes that have occurred.

6.7.1 New trends in criminal law

The rise of modern surveillance societies has reshaped criminal law and particularly its function and methodologies. In turn, this development has had significant consequences for the principle of due process and on the presumption of innocence. Three main trends in criminal law result from the use of modern surveillance.

First, criminal law has been greatly affected by the introduction of new crime investigation methodologies and techniques. The use of biometrics in criminal investigations and for criminal purposes has increased over the time and the use of and reliance on biological samples for purposes of criminal law enforcement has expanded significantly. These new methodologies of evidence collection have therefore contributed to adducing criminal evidence, alongside the 'traditional' tools of crime detection, such as witness evidence.

Second, policing and investigative techniques have profoundly changed since new surveillance technologies have been deployed massively as means of law enforcement. Policing practices and methods have expanded their scope, while relying on specific surveillance techniques such as databases, profiling and data mining. The role of policing has stretched from crime control to crime deterrence, and intelligence has come to the fore in criminal law.[170]

Finally, the extensive deployment of surveillance technologies in criminal proceedings has shifted the focus from "post-crime"to "pre-crime" situations. As a consequence, policing and crime-prevention overshadow the corrective and rehabilitative function of punishment in criminal law. Often there is no need to go to court, since the "problem" is detected at a very

---

[168] Simon, Bart, "The Return of Panopticism: Supervision, Subjection and the New Surveillance", *Surveillance & Society*, Vol. 3, No. 1, pp. 1-20, 2005. See also Lyon, D., "Liquid Surveillance: The Contribution of Zygmunt Bauman to Surveillance Studies", *International Political Sociology*, Vol. 4, Issue 4, December 2010, pp. 325-338.

[169] Surveillance Studies Network, *A Report on the Surveillance Society*, Office of the Information Commissioner, Wilmslow, 2006, p. 12. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf .

[170] McCulloch, Jude, and Sharon Pickering, "Pre-crime and Counter-terrorism: Imagining Future Crime in the 'War on Terror'", *British Journal of Criminology*, Vol. 49, 2009, pp. 634-635.

early stage and addressed by policing. As van Brakel and De Hert note, a shift to a more proactive, predictive and pre-crime society is one of the main trends emerging in policing, criminology and surveillance studies.[171] It has not only enhanced a preventative approach to crime detection, but has also led to a pre-emptive trend in policing.[172] Surveillance technologies have been introduced not only to prevent but also to deter crime. In a proactive, predictive, pre-emptive and pre-crime society, every single person is a target of surveillance systems and practices. The maximum surveillance society reaches its pre-emptive goal only if it is capable of foreseeing any criminal or social offence.[173] Consequently, everybody is considered as a potential offender in a pre-emptive society.

6.7.2 The effects of surveillance on due process of law

The principle of due process of law is rooted in the constitutional traditions of European judicial systems[174] and is mainly governed by Art. 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) (right to a fair trial)[175] and Art. 47 of the Charter of Fundamental Rights of the European Union (right to an effective

---

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

[172] Surveillance Studies Network, *A Report on the Surveillance Society*, Office of the Information Commissioner, Wilmslow, 2006, p. 6. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf .

[173] McCulloch, Jude, and Sharon Pickering, "Pre-crime and Counter-terrorism: Imagining Future Crime in the 'War on Terror'", *British Journal of Criminology*, Vol. 49, 2009, pp. 632-638, and De Goede, Marieke, "The Politics of Preemption and the War on Terror in Europe", *European Journal of International Relations*, Vol. 14, No. 1, 2008, p. 164. The expression "maximum surveillance society" was used in Norris, Clive, and Gary Armstrong, *The Maximum Surveillance Society: the Rise of CCTV*, Berg, New York, 1999. It recalls the broader concept of "maximum security society" used by Gary T. Marx in "La societé de Securité Maximale", *Déviance et Societé*, Vol. 12, No. 2, 1988, pp. 147-166, in which the maximum security prison is considered as the paradigm of the controlling power exercised in modern societies.

[174] Trechsel, Stephen, *Human Rights in Criminal Proceedings*, Collected Courses of the Academy of European Law, Oxford University Press, 2005.

[175] Article 6 of the ECHR – Right to a fair trial – is as follows:

1. In the determination of his civil rights and obligations or of any criminal charge against him, everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal established by law. Judgment shall be pronounced publicly but the press and public may be excluded from all or part of the trial in the interests of morals, public order or national security in a democratic society, where the interests of juveniles or the protection of the private life of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice.
2. Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law.
3. Everyone charged with a criminal offence has the following minimum rights:
    a. to be informed promptly, in a language which he understands and in detail, of the nature and cause of the accusation against him;
    b. to have adequate time and facilities for the preparation of his defence;
    c. to defend himself in person or through legal assistance of his own choosing or, if he has not sufficient means to pay for legal assistance, to be given it free when the interests of justice so require;
    d. to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;
    e. to have the free assistance of an interpreter if he cannot understand or speak the language used in court.

remedy and to a fair trial).[176] The principle of due process is wide in its juridical nature and includes a set of rights which can be summarised as follows: the right to be presumed innocent; the right to be informed of the accusation; the right to adequate time and facilities; the right to defend oneself and to have the assistance of Counsel; the right to test witness evidence; the right to free assistance of an interpreter; the right to appeal; the right to compensation for wrongful conviction; the protection against double jeopardy and the privilege against self-incrimination.[177]

The use of and reliance on surveillance measures in criminal proceedings have significant impacts on the principle of due process and on the rights of the accused in criminal proceedings. Given the broad meaning of the principle of due process of law, surveillance practices affect many of the human rights enclosed within this principle. The main effects of surveillance on due process are discussed: the reversal of the burden of proof; the individual's right not to incriminate oneself (*nemo tenetur edere contra se*); and the right to defence and the creation of suspicion, before going on to consider the principle of the presumption of innocence in more detail. Of course, in order to activate these rights it is necessary to make them "visible", notably enforceable according to Art. 13 of the ECHR.[178]

First, the use of surveillance technologies and practices causes a reversal of the burden of proof in criminal law.[179] When surveillance evidence is dealt with in criminal proceedings, the burden of proof tends to be shifted from the claimant to the accused or suspected. This creates a heavier burden of proof on the defendant and so increases the "innocence threshold" to overcome in order to be acquitted. In this circumstance, the cross-examination stage of the trial focuses on the surveillance evidence and on evidences the defendant is able to provide in order to prove himself innocent. Moreover, the final judgement basically relies on the capability and ability of the defendant to demolish the claimant's accusations. The reversal of the burden of proof in criminal proceedings is apparent in the use of new surveillance technologies and practices. The UK National DNA Database (NDNAD) provides a good example in this regard. DNA profiles of more than 4 million people are registered on the NDNAD.[180] It contains the samples not only of people convicted of crimes, but also of people suspected of crimes but not convicted. Every time a new sample is collected, the NDNAD is

---

[176] Article 47 of the Charter of Fundamental Rights of the EU – Right to an effective remedy and to a fair trial – states that:

> Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.
>
> Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.
>
> Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.

[177] For a detailed analysis on the legal safeguards in criminal proceedings, see Trechsel, Stephen, *Human Rights in Criminal Proceedings*, Collected Courses of the Academy of European Law, Oxford University Press, 2005.

[178] Art. 13 of the ECHR – Right to an effective remedy – states:

> Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

[179] Gary T. Marx was one of the first surveillance scientists to analyse the phenomenon of the reversal of the presumption of innocence. See, for example, Marx, Gary T., *Undercover: Police Surveillance in America*, University of California Press, Berkeley, 1989 and Marx, Gary T., "Seeing Hazily, But Not Darkly, Through the Lens: Some Recent Empirical Studies of Surveillance Technologies", *Law and Social Inquiry*, Vol. 30, No. 2, Spring 2005.

[180] In April 2009, 4.5 million people were on the National DNA Database, of whom 21.5 per cent had no previous conviction or caution. See the BBC News website: http://news.bbc.co.uk/2/hi/uk_news/8375567.stm

searched against the new evidence so that to match it to the existing profile or to create a new one. Once inside the database, people whose DNA samples are contained in the NDNAD may become suspects in a criminal investigation.[181] The NDNAD is just an example of how surveillance technologies and practices can infringe the principle of due process of law. People whose DNA samples are retained are not aware of how their profiles will be used and this surveillance pattern can result in false positives and false negatives.[182] This, in turn, has significant impacts on the right to defence in a criminal trial and on the presumption of innocence (see the following paragraph). In *Barberà, Messegué and Jabardo v. Spain* the ECtHR recalled that Art. 6.2 of the ECHR requires that the "burden of proof is on the prosecution", "any doubt should benefit the accused" and that it is for the prosecution to adduce evidence sufficient to convict the accused.[183] However, the ECtHR has not explained how the Convention can cope with the reversal of the burden of proof triggered by the use of surveillance technologies and practices.

Second, the effects of surveillance on due process of law concern the right not to incriminate oneself, which is a corollary of the right to be presumed innocent. It is widely recognised that the *nemo tenetur* principle provides two main safeguards within a legal proceeding, namely, to protect the accused against torture and against false statements or false criminal charges.[184] From a procedural point of view, silence is considered a guarantee against any kind of pressure on the accused, whereas it is a form of defence from a substantial viewpoint. Neither the European Convention for the Protection of Human Rights and Fundamental Freedoms nor the EU Charter of Fundamental Rights explicitly protect the individual's right to remain silent in a trial.[185] Still, the ECtHR recognised in *Funke v. France* that Art. 6, paragraph 1 of the ECHR safeguards the right to remain silent and not to contribute to incriminating oneself.[186] In this case, the Court stated that the compelling measures against the accused "to provide the evidence of offences he had allegedly committed", infringed the principle of *nemo tenetur* and so Art. 6 of the ECHR.[187] As Butler underlines, the judgment left room for ambiguities and wide interpretations as to whether the right to remain silent prohibited the collection of

[181] Dahl, Johanne Y., and Ann Rudinow Sætnan, "'It all happened so slowly': On controlling function creep in forensic DNA databases", *International Journal of Law, Crime and Justice*, Vol. 37, No. 3, 2009, pp. 83-103.
[182] Gutwirth, Serge, and Mireille Hildebrandt, "Some Caveats on Profiling", in *Data Protection in a Profiled World*, in Serge Gutwirth, Yves Poullet and Paul De Hert (eds.), Dordrecht, Springer, 2010, p. 34.
[183] The case of *Barberà, Messegué and Jabardo v. Spain* concerned three individuals who were arrested following a killing. After having admitted their culpability, they retracted their confessions during the trial. Following the judgments of the Criminal Division of the Audiencia Nacional and of the Spanish Supreme Court which confirmed accusations, the case was submitted before the ECtHR. The applicants claimed that Spain had violated Art. 6.1 and 6.2 of the Convention and that they had been convicted without any evidence. *Barberà, Messegué and Jabardo v. Spain*, application no. 10590/83, Strasbourg, 6 December 1988, para. 77.
[184] De Hert, Paul, "Balancing Security and Liberty within the European Human Rights Framework. A Critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11", *Utrecht Law Review*, Vol. 1, Issue 1, September 2005, p. 86.
[185] By contrast, Art. 14.3 (g) of the UN International Covenant on Civil and Political Rights safeguards this right saying that everyone shall be entitled "not to be compelled to testify against himself or to confess guilt".
[186] After having searched Mr Funke's home without a warrant looking for tax evasion claims, the French custom authorities ordered Mr Funke to produce specific financial statements. When the applicant refused to issue them, he was prosecuted and fined. He appealed the orders unsuccessfully and then applied to the ECtHR claiming that his conviction for a refusal to produce the required documents was a breach to his right to a fair trial (Art. 6.1 ECHR) and disregarded his presumption of innocence (Art. 6.2 ECHR). He also claimed a violation of Art. 8 of the ECHR. *Funke v. France*, application no. 10828/84, Strasbourg, 25 February 1993.
[187] *Funke v. France*, application no. 10828/84, Strasbourg, 25 February 1993, para. 44.

evidence acquired against the will of the accused in criminal proceedings (such as biometric samples). [188]

The ECtHR later clarified this doubt in the *Saunders v. United Kingdom* case in 1996.[189] It stated that the right not to incriminate oneself "does not extend to the use in criminal proceedings of material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, documents acquired pursuant to a warrant, breath, blood and urine samples and bodily tissue for the purpose of DNA testing".[190] Despite this clarification, the content of the right to remain silent and not to incriminate oneself is still a matter of great debate on which limited and wide interpretations confront each other. The extensive use of surveillance technologies and the dynamics exacerbated by this use contribute to trigger this debate. In fact, if considered as the "absence of any direct or indirect physical or psychological pressure from the investigating authorities",[191] the right to remain silent ends up challenging some of the most common surveillance practices in criminal proceedings, such as the collection of biometric data.

Third, there is the issue of trust and the creation of a climate of suspicion regarding persons. The use of profiles obtained through DNA sampling or drug testing[192] shows the added technological potential of current surveillance practices and their impact on due process of law. Moreover, the use of these practices causes broader consequences on a social and political level. As Dahl and Sætnan underline, they create forms of differentiation between "we, the normal, trusted citizens" and "they, the others, the non-trustworthy".[193] Indeed, the shift from a post-crime to a pre-crime surveillance society has a great impact on the relationship between citizens and the state (especially in its executive and judicial manifestations). The pre-emptive approach in policing exacerbated by the use of surveillance technologies spreads a widespread sense of suspicion within democratic societies.[194] As the 2009 report of the House of Lords recognised, the use of surveillance may disturb some of the preconditions that underpin the relationship between the individual and the state.[195] The use of technologies of suspicion[196] threatens the typical relationship of trust that links citizens to the state, as well as the presumption of the individual's innocence.[197]

---

[188] Butler, Andrew S., *Funke v. France and the Right Against Self-Incrimination: A Critical Analysis*, Criminal Law Forum, Vol. 11, No. 4, 2000.

[189] In *Saunders v. United Kingdom*, the applicant complained that his trial of statements given under legal compulsion were admitted as evidence against him at his subsequent criminal trial and thus violated Art. 6 of the ECHR. *Saunders v. United Kingdom*, application no. 19187/91, Strasbourg, 17 December 1996.

[190] Ibid., para. 69.

[191] This is the interpretation of the right to remain silent and not to incriminate oneself given by the UN Human Rights Committee. See *Berry v. Jamaica*, Communication No. 330/1988, U.N. Doc. CCPR/C/50/D/330/1988 (1994), para. 11.7.

[192] Marx, Gary T., "Seeing Hazily, But Not Darkly, Through the Lens: Some Recent Empirical Studies of Surveillance Technologies", *Law and Social Inquiry*, Vol. 30, No. 2, Spring 2005, and Hildebrandt, Mireille, "Profiling and the Rule of Law", *Identity in the Information Society*, Vol. 1, No. 1, 2008.

[193] Dahl, Johanne Y., and Ann Rudinow Sætnan, "'It all happened so slowly': On controlling function creep in forensic DNA databases", *International Journal of Law, Crime and Justice*, Vol. 37, Issue 3, 2009, pp. 83-103 [p. 91].

[194] Lyon, David, *Surveillance after September 11*, Polity Press, Cambridge, UK, 2003, pp. 45-49.

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

[196] Campbell, Nancy D., "Technologies of Suspicion: Coercion and Compassion in Post-disciplinary Surveillance Regimes", *Surveillance & Society*, Vol. 2, No. 1, 2004, pp. 78-92.

[197] The citizens' distrust of democratic institutions has been widely observed in surveillance studies. See, for example, Lyon, David, *Surveillance Society. Monitoring Everyday Life*, Open University Press, London, UK,

6.7.3 The effects of surveillance on the presumption of innocence

The presumption of innocence guarantees the innocence of a person charged with a criminal offence until proved guilty according to law. This principle is endorsed by Art 6.2 of the ECHR and Art. 48.1 of the EU Charter of Fundamental Rights[198] and provides a legal guarantee in criminal proceedings whose nature and purpose lie in the right to a fair trial. According to Art. 6.2 of the ECHR, the presumption of innocence applies to *everyone who has been charged* with a criminal offence, not only to persons labelled as 'suspects' in the framework of a criminal proceeding.[199] As a consequence, the presumption of innocence does not benefit persons who are not charged with a criminal offence, nor persons who are suspected of a crime but not charged before a court.[200] The limited applicability of the presumption of innocence represents a great issue of concern in our surveillance societies, given the widespread and massive use of surveillance technologies and their potential intrusiveness. Indeed, as explained above, surveillance technologies and practices do not target only criminals but the whole society and their purposes go far beyond criminal proceedings. Surveillance practices are implemented both within and outside the scope of criminal trials and this causes a gap in the application and enforceability of the principle of the presumption of innocence.

Given that the presumption of innocence operates only in criminal proceedings, there are three crucial stages in which an infringement of the presumption of innocence may substantially occur, namely before a charge is formally submitted, after an acquittal judgement and after a penalty has been served. From a legal perspective, these stages are grey areas in which the presumption of innocence can be threatened and individuals could not plead it successfully. Legislation does not provide adequate legal safeguards to the applicability of the presumption of innocence in these three circumstances. By contrast, the jurisprudence of the ECtHR has erected some legal barriers to the indiscriminate and unlimited use of surveillance technologies outside the framework of criminal trials. In *Adolf v. Austria* and *Lutz v. Federal Republic of Germany* the ECtHR stated that judicial decisions that do not contain any finding of guilt but that only describe a state of suspicion do not call into question the presumption of the individual's innocence.[201] Moreover, in *Barberà, Messegué and Jabardo v. Spain*, the ECtHR said that the presumption of innocence requires that "the members of the court should not start with the preconceived idea that the accused has

---

2001, and Wright, David, Serge Gutwirth, Michael Friedewald, Paul De Hert, Marc Langheinrich and Anna Moscibroda, "Privacy, trust and policy-making: Challenges and responses", *Computer Law & Security Review*, Vol. 25, No. 1, 2009, pp. 69-83. Clive Norris clearly described this dynamic in his evidence to the House of Lords: "Mass surveillance promotes the view … that everybody is untrustworthy. If we are gathering data on people all the time on the basis that they may do something wrong, this is promoting a view that as citizens we cannot be trusted", House of Lords, Select Committee of the Constitution, *Surveillance: Citizens and the State*, HL Paper 18-I, 2nd Report of Session 2008-2009, Volume I: Report, para. 107.

[198] Art. 6 of the ECHR is recalled at supra note 10. Art. 48.1 of the Charter states: "Everyone who has been charged shall be presumed innocent until proved guilty according to law."

[199] In fact, Art. 6.2 of the ECHR states: "Everyone charged with a criminal offence shall be presumed innocent until proved guilty according to law."

[200] As the ECtHR underlined in *Adolf v. Austria*, "The prominent place held in a democratic society by the right to a fair trial favours a 'substantive', rather than a 'formal', conception of the 'charge' referred to by Article 6 (art. 6); it impels the Court to look behind the appearances and examine the realities of the procedure in question in order to determine whether there has been a 'charge' within the meaning of Article 6", *Adolf v. Austria*, application no. 8269/78, Strasbourg, 26 March 1982, para. 30.

[201] *Adolf v. Austria*, application no. 8269/78, Strasbourg, 26 March 1982, par. 40 and *Lutz v. Federal Republic of Germany*, application no. 9912/82, Strasbourg, 25 August 1987, para. 62.

committed the offence charged"[202] and that this procedural guarantee is violated whenever "without the accused's having previously been proved guilty according to law, a judicial decision concerning him reflects an opinion that he is guilty".[203]

Therefore, in the reasoning of the ECtHR, culpability has to be proved in order to safeguard the individual's right to be presumed innocent and mere suspicions do not result in a violation of this right. In *Sekanina v. Austria*, the Court made a clearer distinction between accusations and suspicions and clarified how they relate to the presumption of innocence. The ECtHR pointed out that "the voicing of suspicions regarding an accused's innocence is conceivable as long as the conclusion of criminal proceedings has not resulted in a decision on the merits of the accusation" and that "it is no longer admissible to rely on such suspicions once an acquittal has become final".[204] Most of all, the Court said that no authority or court may rely on charges that have been proved to be unfounded.[205] This approach was followed also in *Asan Rushiti v. Austria* when the Court argued that "following a final acquittal, even the voicing of suspicions regarding the accused's innocence is no longer admissible".[206]

A significant step towards an extension of the scope and applicability of the presumption of innocence was made by the ECtHR in *Allenet de Ribemont v. France.*[207] The Court admitted that a violation of Art. 6.2 of the ECHR may occur not only in the context of a judicial decision but also before a charge is formally submitted before a court. The ECtHR found that a statement made on television by a high-ranking police officer infringed Art. 6.2 of the ECHR. This declaration concerned the applicant's guilt and, "firstly, encouraged the public to believe him guilty and, secondly, prejudged the assessment of the facts by the competent judicial authority".[208] As a consequence, the ECtHR recognised that "the presumption of innocence may be infringed not only by a judge or court but also by other public authorities".[209] The widening of the definition and application of the presumption of innocence in the *Allenet de Ribemont* case has been related to the fact that according to EU law, this principle has a reputation-related aspect.[210] As a consequence, the presumption of

[202] *Barberà, Messegué and Jabardo*, application no. 10590/83, Strasbourg, 6 December 1988, para. 77.
[203] Ibid., para. 91. This finding was also reached in *Minelli v. Switzerland*, application no. 8660/79, Strasbourg, 25 March 1983.
[204] In *Sekanina v. Austria*, the applicant claimed that the judicial decision refusing compensation for unjustified detention violated his presumption of innocence (Art 6.2 ECHR). *Sekanina v. Austria*, application no. 13126/87, Strasbourg, 25 August 1993, para. 37.
[205] "No authority may treat a person as guilty of a criminal offence unless he has been convicted by the competent court and in the case of an acquittal the authorities may not continue to rely on the charges which have been raised before that court but which have been proved to be unfounded. This rule also applies to courts which have to deal with non-criminal consequences of behaviour which has been subject to criminal proceedings. They must be bound by the criminal court's finding according to which there is no criminal responsibility for the acts in question although this naturally does not prevent them to establish, eg a civil responsibility arising out of the same facts", *Sekanina v. Austria*, application no. 13126/87, Strasbourg, 25 August 1993 para. 37.
[206] *Asan Rushiti v. Austria*, application no. 28389/95, Strasbourg, 21 March 2000, para. 31.
[207] In *Allenet de Ribemont v. France*, the ECtHR was asked to decide whether specific statements made by politicians and high-ranking police officers on television during a murder investigation infringed Art. 6 of the ECtHR and particularly the applicant's presumption of innocence. *Allenet de Ribemont v. France*, application no. 15175/89, Strasbourg, 10 February 1995.
[208] *Allenet de Ribemont v. France*, application no. 15175/89, Strasbourg, 10 February 1995. paras. 33-36.
[209] *Allenet de Ribemont v. France*, application no. 15175/89, Strasbourg, 10 February 1995.
[210] Trechsel, Stephen, *Human Rights in Criminal Proceedings*, Collected Courses of the Academy of European Law, Oxford University Press, 2005, p. 164, and Campbell, Liz, "A rights-based analysis of DNA retention: "non-conviction" databases and the liberal state", *Criminal Law Review*, Vol. 12, 2010, pp. 889-906.

innocence extends beyond a strictly procedural guarantee to protect the image of the person deemed to be innocent and so must be interpreted together with Art. 8 of the ECHR.[211]

This close link between Art. 6.2 and Art. 8 of the ECHR emerged even more clearly in *S. and Marper v. United Kingdom*. The case concerned two individuals, Mr S. and Mr Marper. The former, 11 years old, was arrested in January 2011 and acquitted in June of the same year. The latter was arrested in March 2011 and then his case was formally discontinued in June 2011. Once arrested, their fingerprints and DNA samples were taken, according to the provisions of the Police and Criminal Evidence Act of 1984. The applicants complained under Art. 8 of the ECHR about the retention of their fingerprints, cellular samples and DNA profiles pursuant to section 64 (1A) of the Police and Criminal Evidence Act.[212] Although they did not invoke Art. 6.2 of the ECHR and the judgement was not centred on this article, the ECtHR referred to the presumption of innocence in the context of an acquittal judgement and case dismissal. The Court found that, given these circumstances, the indefinite retention of the applicants' fingerprints, cellular samples and DNA profiles resulted in the fact that the claimants were treated like convicted persons and created the perception that they were not innocent.[213] Thus, in *S. and Marper*, the Court provided a legal safeguard to the individual's right to be presumed innocent through Art. 8 of the ECHR. Moreover, the ECtHR used Art. 8 tentatively to extend the applicability of the right not to be presumed guilty beyond the framework of criminal proceedings, considering the increased threat to the presumption of innocence due to surveillance systems and practices.

6.7.4 Conclusion

The jurisprudence of the ECtHR has still to be developed in order to provide an adequate safeguard against the effects of surveillance technologies and practices on due process of law and the presumption of innocence in surveillance societies. Art. 6 of the ECHR, concerning the right to a fair trial, does not provide appropriate and effective answers in this regard[214] and its provisions are not capable of coping with the widespread use of surveillance technologies and practices. The cautious attempts of the ECtHR to deal with new surveillance practices by extending the applicability of the presumption of innocence outside the context of criminal trials highlight the anachronistic character of Art. 6 of the ECHR. The bulk of the effects of surveillance technologies and practices on due process of law and the presumption of innocence are also not countered by legislation. However, while acknowledging the effects of surveillance, it is imperative for legislation to address the many human rights concerns, for – as we have shown – like terrorism,[215] surveillance is often contemptuous of human rights. It

[211] Art. 8 of the ECHR safeguards the individual's right to respect for private and family life and states that:
1. Everyone has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[212] Section 64 (1A) of the Police and Criminal Evidence Act prescribed that fingerprints or samples taken from a person in connection with the investigation of an offence might be retained after they had fulfilled the purposes for which they were taken.

[213] *S. and Marper v. United Kingdom*, applications 30562/04 and 30566/04, Strasbourg, 4 December 2008, paras. 122 and 125. Note that the retention periods are less extensive in Scotland.

[214] Bellanova, Rocco, and Paul De Hert, "Le cas S. et Marper et les donnees personnelles : l'horloge de la stigmatisation stoppee par un arret Europeen", *Cultures & Conflicts*, No. 76, 2009, pp. 101-114 [p. 109].

[215] Sorell, Tom, "Preventive Policing, Surveillance, and European Counter-Terrorism", *Criminal Justice Ethics*, Vol. 30, No. 1, April 2011, pp. 1-22 [p. 7].

brings into question the relationship between security and the exercise of civil and political rights, such as those governed by Art. 6 of the ECHR.

6.8 THE EFFECTS OF SURVEILLANCE ON THE RIGHTS AND VALUES OF PARTICULAR PEOPLE (EQUALITY OF TREATMENT)

Gemma Galdon Clavell, UB

Surveillance works at different levels, as do categories such as rights and values. Rights are moral or legal entitlements, and can be formal (granted by law) or informal understandings embedded in a particular society or culture. Values, however, usually refer to principles or standards of behaviour[216] and usually inform rights, but are developed individually and sometimes independently of legal prescription. Equality of treatment, in turn, is a general principle of community that states that similar situations must be treated identically and prohibits discrimination and discriminatory treatment. Equality of treatment may be recognised as a right, and it is also understood that steps will be taken to prevent or remove differences in treatment.[217] Equality of treatment may therefore be guaranteed by law but also enforced when discriminatory practices and values are identified.

For those who are situated at the watching, listening, locating, detecting and monitoring side of surveillance, those that appear before the lens or the data-gathering mechanism are usually just "data subjects", the term used in data protection or information privacy law. They are the sources of pieces of information that can be used or analysed both individually and in aggregated form to reach a given objective, be it market analysis, community safety and security or more efficient management of resources, mobility, sustainability, or other aims.[218] This utilitarian take on surveillance, however, fails to address issues related to the social impact of surveillance, and specifically how surveillance may or may not interact with power dynamics, social relations, identities, cultural values, historical factors or expectations. It also tends to overlook the *surveilled* as a relevant actor in understanding the externalities of the surveillance society. In order to deepen the understanding of the relationship between attitudes, values and rights, we must address issues linked to social sorting and profiling as concomitants of surveillance, the relationship between surveillance and the right to equal treatment, and surveillance as a practice that may reinforce certain social values and the discrimination of specific groups.

Many authors have pointed to the need to go beyond Foucauldian understandings of surveillance,[219] but ideas of self-policing, domination and disciplining continue to be echoed by popular discourses on surveillance, and not enough is yet known about the reactions, opinions and attitudes of those subject to the "electronic eye".[220] Nonetheless, an emerging body of work helps to enrich the understanding of surveillance's impact on rights, values and equal treatment, and of how that impact might depend upon other variables including culture, socio-economic background, gender and ethnicity. Categories such as social sorting, digital

[216] Definitions from Oxford dictionaries.
[217] Watson, Philippa, "Equality of Treatment: A Variable Concept?", *Industrial Law Journal*, Vol. 24, No. 1, 1995, pp. 33-48.
[218] Lyon, David, *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge, London, 2003.
[219] Foucault, Michel, *Discipline and punish. The birth of the prison*, Vintage Books, New York, 1977.
[220] The literature on the "watchers" is abundant. See, inter alia, Norris, Clive, and Gary Armstrong, *The maximum surveillance society: The rise of CCTV*, Berg, Oxford, 1999.

discrimination, privacy invasion, and racial profiling[221] are useful for understanding how surveillance may promote unequal treatment among different categories of people and may tend particularly to affect the young and the poor.

The surveillance literature has dealt at length with the issue of discrimination, framed as profiling or social sorting by most authors. "Surveillance today sorts people in categories, assigning worth or risk, in ways that have real effects on their life-chances. Deep discrimination occurs, thus making surveillance not merely a matter of personal privacy but of social justice", says Lyon.[222] Everyday surveillance is based on the use of databases and classification;[223] in this process of abstraction, discrimination can emerge in the sense of one's being pre-emptively singled out because of one's appearance, behavioural routines, financial transactions, genetic information, consumption habits or many other criteria employed in particular sectors and domains where surveillance is carried out.

The Open Society Institute finds that ethnic police profiling in Europe is not only "pervasive, ineffective and discriminatory", but also a widespread practice that overwhelmingly affects immigrant and minority communities, and that is often conducted with the help of surveillance technologies. The report finds that "32 percent of British Muslims report being subjected to discrimination at airports", and that "the personal data of 8,3 million people were searched in a massive German data mining exercise which targeted ... people who were Muslim, and which did not identify a single terrorist", the report found.[224] In his study of ID cards, Lyon emphasises that the social sorting associated with IDs touches the lives of the weakest, most marginalised members of the population. Many of these IDs increasingly incorporate biometric data, which classifies people according to their bodily and behavioural characteristics, thus abstracting their identities from their everyday "struggles and stories".[225] As Lomell suggests, "categorical suspicion and social exclusion are the basis of much of the surveillance practices", both in relation to physical surveillance and dataveillance, and in both the formal sphere of rights and the informal sphere of values and practices.[226]

This surveillance-enabled social sorting, however, does not only work against marginalised groups, but also in favour of those who are deemed to be trustworthy because of their social or economic status. In these cases, individuals are subjected to increased surveillance to allow for expedited border crossing, for instance, but "the surveillance of socially privileged populations seems to be driven by a different set of objectives and consequences than the surveillance of those on the bottom of the social hierarchy".[227] Inequality of treatment, thus,

---

[221] Gandy, Oscar H., *The Panoptic Sort: A Political Economy of Personal Information*. Westview, Boulder, CO, 1993; Lyon, David, *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge, London, 2003; Monahan, Torin, "Editorial: Surveillance and Inequality", *Surveillance & Society*, Vol. 5, No. 3, 2008, pp. 217-226; Regan, Priscilla M., *Legislating Privacy: Technology, Social Values, and Public Policy*, University of North Carolina Press, Chapel Hill, NC, 1995.

[222] Lyon, David, *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, Routledge, London, 2003, p. 1.

[223] See Bowker, Geoffrey C., and Susan Leigh Starr, *Sorting Things Out: Classification and its Consequences*, The MIT Press, Cambridge, MA, 1999.

[224] OSI, *Police Profiling in Europe: Pervasive, Ineffective, and Discriminatory*, Open Society Institute, New York, 2009.

[225] Lyon, David, "National ID Cards: Crime-Control, Citizenship and Social Sorting", *Policing*, Vol. 1, No. 1, 2007, pp. 111-118.

[226] Lomell, Heidi Mork, "Targeting the Unwanted: Video Surveillance and Categorical Exclusion in Oslo, Norway", *Surveillance & Society*, Vol. 2, Nos. 2-3, 2004, pp. 346-360.

[227] Aas, Katja Franko, "'Crimmigrant' bodies and bona fide travelers: Surveillance, citizenship and global governance". *Theoretical Criminology*, Vol. 15, No. 3, 2011, pp. 331-346.

does not always mean that discrimination is used against the subjects of surveillance, but surveillance can also provide avenues of privilege and freedom from further scrutiny to those who have been able to pay for the benefits associated with being watched, or those who comply with the prerequisites of status.

While paying for a right or for specially favoured treatment is a way of differentiating oneself from other persons or groups, the relationship between wealth and surveillance is not always so evident, and some surveillance technologies have been shown to reproduce and reinforce social values related to status in less obvious ways. In their study of surveillance in schools, McCahill and Finn find that class and gender are important factors influencing the way surveillance is perceived, appropriated and resisted. They describe how students from more privileged backgrounds did not consider themselves to be under surveillance, for they understood the CCTV cameras to be directed at 'Them' (young people from economically deprived backgrounds and with a certain aesthetic), and not at 'Us'. They conclude that "the social impact that surveillance might have on children's lives is highly dependent upon existing social relations, identities, and cultural traditions.... The various surveillance practices [observed] reaffirmed young people's social positionings as privileged, marginalised and gendered."[228]

Similarly, in their study of the night-time economy in Lancaster, England, Dixon et al. show how attitudes towards CCTV are dependent on variables such as age (older people tend to be more supportive of camera schemes), gender (women are more favourable to CCTV and less concerned about its impact on individual rights) and previous attitudes toward social inclusion (those who favoured CCTV tend also to agree that certain groups should be kept out of specific public areas). While these categories shed light on the values of those asked about their opinion on CCTV, the survey also points to one unintended consequence: the possibility that videosurveillance discourages feelings of social responsibility and that "responsibility for the welfare of others is handed over to the CCTV cameras".[229] In a study of CCTV in Spain, Galdon Clavell[230] also finds that there is a tendency for municipalities to install CCTV in places where young people meet, such as public squares, libraries and schools. This underlines that the electronic eye is often directed at groups that are perceived to be problematic, thus reinforcing discrimination and stigmatisation both socially and in police practice.[231]

As these examples show, inequality of treatment and discrimination do not only occur in the formal process of categorisation and differentiation that surveillance technologies require in order to classify those who are surveilled. They also occur more informally by reproducing and reinforcing pre-existing values, prejudices, power relations and social relations between individuals or groups. In this sense, the literature shows that surveillance technologies, because of their involvement with categories, tend to normalise discrimination based on race, gender, income, appearance, age, behaviour or other cues picked up by surveillance technologies. This may engage Articles 20 and 21 of the EU Charter of Fundamental Rights, which state that "[e]veryone is equal before the law", and that "any discrimination based on

[228] McCahill, Michael, and Rachel Finn, "The Social impact of Surveillance in Three UK Schools: 'Angels', 'Devils' and 'Teen Mums'', *Surveillance & Society*, Vol. 7, Nos. 3-4, 2010, pp. 273-289, at pp. 266, 268.

[229] Dixon, John, Mark Levine and Rob McAuley, *Street Drinking Legislation, CCTV and public space: exploring attitudes towards public order measures*, Home Office, London, 2003, p. 21.

[230] Galdon Clavell, Gemma, "Local surveillance in a global world: Zooming in on the proliferation of CCTV in Catalonia', *Information Polity*, Vol. 16, No. 4, 2011, pp. 319-338.

[231] Norris, Clive, and Gary Armstrong, *The Maximum Surveillance Society: The Rise of CCTV*, Berg, Oxford, 1999.

any ground such as sex, race, colour, ethnic or social origin, genetic features, language, religion or belief, political or any other opinion, membership of a national minority, property, birth, disability, age or sexual orientation shall be prohibited".

Bennett and Raab argue that existing laws, paradigms and regimes for the protection of individual information privacy are, unfortunately, scarcely able to contemplate the principle of equality that surveillance threatens. They show that there is a need to re-frame the conception of privacy protection in terms of social policy, beyond its importance in defending a crucial individual right.[232] Similarly, Raab and Wright indicate the shortcoming of existing models of privacy impact assessment (PIA) in failing to incorporate wider social values than individual privacy in their routines for assessing the impact of surveillance technologies and systems.[233] While there have been recent attempts to incorporate concerns over the social externalities and ethics of surveillance both in policy design and technological development, the mechanisms to enforce equality of treatment when surveillance-related discriminatory practices are identified do not exist yet, as the interaction between rights and practices, and between values and socio-technical devices continue to be uncharted territory at the regulatory and technological levels.

6.9 EFFECTS OF RIGHTS AND FREEDOMS ON SYSTEM DESIGN

Dara Hallinan, Fraunhofer ISI

As we have just shown at some length, technological innovation has the capacity to affect rights and values. However, the opposite is also true. Having discussed the effects of surveillance on a host of rights and values, we now reverse the direction and enquire into the effect of rights and values on surveillance and on the technologies and systems that are involved in it. The development and use of technology is shaped and directed by the social contexts and norms of the society from which it emerges and in which it is used. Accordingly, as tools of power and control, surveillance technologies also meet the necessity to conform to the limits set by fundamental rights.

The society-shaping potential and thus the impact of surveillance, and surveillance technologies, on fundamental rights is not only found in the specific action, or moment, of surveillance. The mechanisms and logic of the technologies, the systems in which they are deployed and the institutional context they create also play a significant role. Accordingly, these broader features of surveillance technology and systems become areas of significance for the protection of fundamental rights. The set of principles and systems attempting to mitigate the fundamental rights impact of technologies through influencing technological, system and organisational design is known as privacy by design (PbD).[234]

[232] Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, The MIT Proess, Cambridge, MA, 2006, chapter 2.
[233] Raab, Charles, and David Wright, "Surveillance: Extending the Limits of Privacy Impact Assessment", in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012, pp. 363-383.
[234] Cavoukian, Ann, *Privacy by Design ... Take the Challenge*, Information and Privacy Commissioner of Ontario, Toronto, 2009, p. 4. Whilst surveillance can influence a number of rights, it is the rights to privacy and data protection that have been most relevant in attempts to influence the design of technology.

Whilst this term has been variously defined, the constant idea is that technology can be enlisted to protect privacy.[235] To achieve this, concepts of privacy and data protection should be included in the design and operation of systems (technological or organisational) so that the likelihood of privacy infringements is minimised or even made impossible from the outset.[236] Thus, PbD principles would mandate that surveillance systems would need to be designed and deployed with the principles of privacy and data protection in mind at each stage – as opposed to being applied as an afterthought.[237] As privacy principles would be embedded in the design and operation of systems, fundamental rights would thus be protected on an individual level, with each individual enjoying a strengthened level of privacy protection in relation to each system interacted with, or used; and on a structural level, as the context of design, deployment and use would all need to be configured to ensure compliance with privacy and data protection principles. This would create an institutional context and a technological, informational and organisational environment most amenable to the protection of privacy.[238]

Initially, PbD-described technologies and design principles (including privacy enhancing technologies, or PETs).[239] However, with growing recognition of its relevance, and an awareness of different features of development, operation and deployment with potential privacy impact, its ambit has grown broader. Principles of PbD now extend to building privacy into operational practice and even into physical design.[240] PbD is thus aimed at all actors with a role in the design and implementation of potentially privacy-infringing systems and technologies. This is a broad group, extending through systems designers and programmers at the design phase to eventual data controllers and processors at the use phase.

---

[235] The idea of technical data protection was already developed by Andreas Pfitzmann and others in the late 1980s and entered the (academic) mainstream during the 1990s. See Bizer, Johann, "Datenschutz als Gestaltungsaufgabe: Das Konzept des proaktiven Datenschutzes", *DuD - Datenschutz und Datensicherheit*, Vol. 31, No. 10, 2006, pp. 725-730. Se also Lessig, Lawrence, *Code and Other Laws of Cyberspace*, Basic Books, New York, NY, 1999; Reidenberg, Joel, "Lex Informatica: The Formulation of Information Policy Rules Through Technology", *Texas Law Review*, Vol. 76, 1998, pp. 552-593.

[236] Hornung, Gerrit, "Privacy by Design in Europe: Seizing the Opportunity of the Reform of the Data Protection Directive", *Innovation: The European Journal of Social Science Research*, Vol. 26, No. 1, 2013 [forthcoming].

[237] In turn, the principles applied to other data collection and processing technologies would ensure transparency and the return of control over personal data to the individual, practically limiting the possibilities for that individual's data to be used as surveillance material. See London Economics, "Study on the economic benefits of privacy-enhancing technologies (PETs)", Final Report to the European Commission DG Justice, Freedom and Security, London, 2010.

[238] EDPS, "Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy", European Data Protection Supervisor, Brussels, 2010. Hornung also suggests privacy by design principles would allow the precautionary principle to gain importance for data protection and would provide a more structural form of cover for aspects of data processing with significant individual effect, but which are not covered by the current framework – for example, surveillance and profiling based on data which do not fulfil the "personal" criteria of the current framework. See Hornung, Gerrit, "Privacy by Design in Europe: Seizing the Opportunity of the Reform of the Data Protection Directive", *Innovation: The European Journal of Social Science Research*, Vol. 26, No. 1, 2013 [forthcoming].

[239] There are various forms of privacy by design, of which privacy enhancing technologies are one sub-category. Even within this sub-category, there are a wide range of technologies pursuing the overall goal of privacy in a range of ways, including technologies aimed at anonymisation, protection from network invasions or superior identity management. PETs can act as stand-alone solutions or as integrated system elements. Considering the context dependant aspect of privacy and the difference in function, goal, cost and efficacy of each PET, it is not possible to identify a one-size-fits-all PET solution; therefore, one cannot identify one single technological approach to the deployment of PETs or PbD in the surveillance context. See Shen, Yun, and Siani Pearson, "Privacy Enhancing Technologies: A Review", HPL-2011-113, HP Laboratories, 2011. http://www.hpl.hp.com/techreports/2011/HPL-2011-113.html

[240] Cavoukian, Ann, *Privacy by Design ... Take the Challenge*, Information and Privacy Commissioner of Ontario, Toronto, 2009, p.5.

Despite demonstrations that PbD measures can increase privacy without detriment to the functionality of systems, and perhaps as a result of the lack of legislative impetus, there has been little uptake. This is exemplified by the poor uptake of PETs.[241]

Ideas related to the philosophy behind PbD have been observable in legislation at European and Member State level for some time. At the European level, for example, the concept of data minimisation as a principle of data processing is closely related to PbD thinking, whilst it has even been argued that there is already an obligation to implement certain forms of PbD: for example, flowing from Article 17, which requires appropriate technical and organisational measures to be taken to protect personal data against all unlawful forms of processing.[242] However, despite these references, the thrust of legislation has not focused on the design and implementation of technology, focusing rather on the provision of rules for the end act of data processing. Accordingly, the principles of PbD have, up to now, played a relatively minor role in regulation.[243]

However, classical command-and-control regulatory approaches have proven inflexible and have demonstrated an inability to deal with the complexity, interconnectedness, speed and dynamism of technological progress and, being tied to traditional national enforcement authorities, have lost their effectiveness when dealing with the "disembodied" data environment. In light of these difficulties, considering technology as a potential ally in securing privacy provides a regulatory option circumventing these issues, turning the technology itself into an instrument to achieve regulatory ends and embedding privacy principles into the substance at the core of the problems.[244]

A foreseeable recalibration of the legislative significance of technology design and deployment in European data protection legislation may be on the verge of overcoming the sluggish uptake of PbD and PETs. In January 2012, the European Commission released its proposal for a Data Protection Regulation as part of a process of review of the current Data Protection Directive. The proposal contains a more holistic, fundamental-rights focused approach to data protection. The proposal recognises the significance of technological design as a key tool in the protection of privacy.[245] This thinking laid the foundation for the inclusion, in Article 23, of PbD as a specific principle, potentially (depending on the eventual outcome of the review process) creating a legal obligation to design privacy and data

---

[241] London Economics, "Study on the economic benefits of privacy-enhancing technologies (PETs)", Final Report to the European Commission DG Justice, Freedom and Security, London, 2010, pp. 29-64.

[242] European Parliament and the Council, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data on the free movement of such data, Official Journal of the European Communities, L 281, 23 November 1995, pp. 31-50; Hustinx, Peter, "Privacy by design: delivering the promises", *Identity in the Information Society*, Vol. 3, Issue 2, August 2010, pp. 253–255. http://link.springer.com/journal/12394/3/2/page/1

[243] Bygrave, Lee A., *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International, Den Haag, London, New York, 2002, pp. 21-68.

[244] Hornung, Gerrit, "Privacy by Design in Europe: Seizing the Opportunity of the Reform of the Data Protection Directive", *Innovation: The European Journal of Social Science Research*, Vol. 26, No. 1, 2013 [forthcoming].

[245] Other ideas closely associated with PbD appear throughout the proposal. Article 22 takes account of the debate on accountability, while Article 39 contains provisions regarding data protection seals and certification. 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, 2012, Article 3(2). See also Kuner, Christopher, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", *Privacy and Security Law Report*, 6 February 2012, pp. 1-15; Richter, Philipp, "Datenschutz durch Technik und die Grundverordnung der EU-Kommission", *DuD – Datenschutz und Datensicherheit*, Vol. 36, No. 8, 2012, pp. 576-580.

protection principles into surveillance technologies, deployment and organisational practices.[246] However, it will be several years before a new Regulation – if in fact, it will be a Regulation and not a new general Directive – will be adopted and implemented, so one should not look for PbD to gain critical momentum in the near future.

6.9.1 Good practice: some examples

Richard Jones and Charles Raab, University of Edinburgh

Whatever the challenges facing the realisation of PbD on an extensive scale within the EU in the near future, various examples of best practice in this approach can already be identified from around the world.

In the context of Internet use in general, the Privacy and Electronic Communications (EC Directive) Regulations 2003 regulate websites' use of small "cookie" files downloaded by a user's computer when browsing the website – a widespread practice used by website owners to track users in various ways. Users are often unaware of the extent to which their Internet usage is tracked this way, and hence unaware that their web browsing may be less private than they thought. The regulations require that websites must "tell people that the cookies are there, explain what the cookies are doing, and obtain their consent to store a cookie on their device"[247]. The regulations, cookie usage in practice, and technologies involved are complex, and practice is still evolving in these areas.

Nevertheless, two recent possible developments of better practice are worth noting. First, many websites now use "pop-ups" to alert new visitors that the site uses cookies. Whereas there are limitations to this approach – for example, users may quickly simply ignore such warnings – it can contribute to greater transparency and awareness. Second, and perhaps more powerfully, users can adjust their web-browser settings to control whether cookies are downloaded automatically or not, including third-party cookies that are often used by advertising networks. Since many users rarely or never adjust their browser settings, the default settings of the browser software are very important. From a privacy perspective, best practice involves a browser-setting default of rejecting third-party settings. This is a good example of the difference between default settings of "opt in" versus "opt out".

In the context of individual identification systems – for example, national ID card systems – one interesting means of making the systems useful for third parties, such as retailers, while protecting individuals' privacy, is to employ a "verification-only" system. In this system, an alcohol retailer (for example) can check whether the customer is of legal age to make such a purchase, but instead of supplying the customer's date of birth to the retailer, the system simply answers Yes or No to the question "Is the purchaser over the age of [for example]

[246] This step has not been received uncritically. For example, commentators have observed the absolute lack of clarification as to what the definitions or obligations set out in the proposal could mean in practice. There are equally large, although more general, objections as to the role of technology as a regulatory tool. See, for example, Phillips, David J., "The Influence of Policy Regimes on the Development and Social Implications of Privacy Enhancing Technologies", Paper presented at: Telecommunication Policy Research Council 29th Research Conference on Communication, Information and Internet Policy, 2001; Brownsword, Roger, *Rights, Regulation and the Technological Revolution*, Oxford University Press, Oxford, 2008, pp. 240-283.

[247] UK Information Commissioner's Office, "Guidance on the rules on use of cookies and similar technologies", May 2012, V.3, p. 11. http://bit.ly/MCjint

18?" Such a system gives assurance to the third party, but provides only the key answer required while protecting personal information.[248]

A related example of the encouragement of good practice is the set of privacy principles for public-service identity management, promulgated by the Scottish Government. They illustrate the way in which privacy protection can be designed into management systems and routines, and not only into technological devices as such. For example, one principle states that, for frequently used services for which identification is needed, people should be given a simple way to register once. Thereafter, in many cases, it will enough if the person can authenticate herself with a token, such as a bus pass or library card, that proves entitlement without revealing personal information. Another principle stipulates that the authentication methods used should take convenience to the individual and respect for privacy into account, and should be sufficiently reliable to avoid false acceptances and rejections, and should "ensure that people are not discriminated against unfairly (for example, on grounds of disability, age or ethnicity) or socially excluded as a result of the approach to identification or authentication".[249]

Finally, whereas the first generation of full body scanners to be used at airports to scan passengers for concealed weapons or other items effectively showed the passengers' underwear and naked body to security staff operating the scanner, newer scanners take the scan results and represent the locations of any items detected on a schematic diagram of a human body. In this way, the purpose of the scanner – to detect illegal items – is fulfilled while ensuring that the personal imagery most passengers would consider deeply private are not unnecessarily visible.

In the above cases, various wider considerations still apply: for example, is the information being requested actually necessary at all? If so, is the system being used the best or most appropriate one? It may be, for example, that airport full body scanners should be rejected from use on the grounds of a combination of high cost, low effectiveness, and health concerns. However, the point here is simply that insofar as a given surveillance system is employed, there are often ways in which the system can be designed to operate effectively for the stated purpose while minimising the impact on privacy.

6.10 EFFECTS OF RIGHTS AND VALUES ON OVERSIGHT OF SYSTEMS

Charles Raab, University of Edinburgh

We have seen how rights and values can have a powerful effect on surveillance if they are taken into account in the design of information systems that deal with personal data, and in the way they are implemented in practice. One avenue to the oversight of surveillance is through Privacy Impact Assessment (PIA). Although PIA in practice largely concerns compliance with data protection rules and principles, these are themselves founded on rights and values, particularly privacy. PIA is increasingly called for, and even mandated, in many countries as an essential practice for the deployment of surveillance technologies and

[248] Naumann, Ingo, and Giles Hogben [European Network and Information Security Agency (ENISA)], "Privacy Features of European eID Card Specifications", Elsevier Network Security Newsletter, August 2008, pp. 9-13. http://bit.ly/Ts9P2R.

[249] Scottish Government, *Identity Management and Privacy Principles: Privacy and Public Confidence in Scottish Public Services*, Version 1.0, The Scottish Government, Edinburgh, December 2010, p. 6.

information systems. Whereas privacy audits operate *ex post facto*, PIA forms part of a precautionary strategy for the oversight of surveillance in the name of rights and values prior to the implementation of these technologies and systems.[250]

Flaherty regards PIA as "a risk-assessment tool for decision makers to address not only the legal, but the moral and ethical, issues posed by whatever is being proposed".[251] This points the way towards an extension of PIA into Surveillance Impact Assessment (SIA) by means of a broader consideration of a range of values than individual privacy, as Wright and Raab have advocated.[252] SIA would enable a precautionary assessment of whether the broader inventory of values, rights and freedoms discussed earlier in this chapter are affected by a given surveillance proposal.

Whether PIA or SIA – or beyond those techniques – the extent to which rights and values can become part of surveillance oversight routines may be strongly restricted. It is important that assessment and oversight be based on thought and judgement, rather than becoming a perfunctory box-ticking bureaucratic exercise. An institutional tendency towards the latter would blunt the effect of rights and values upon oversight because it would reduce the procedure to items in a questionnaire rather than keeping a focus upon the reasons for limiting surveillance. Satisfactory oversight therefore faces the prospect of dilution, although that is not only a danger for PIA or SIA. Privacy, insofar as it is reflected in data protection, seems to be a right and value that is better served by oversight routines within organisations, and even when exercised by external regulatory bodies, than would be the fuller range of rights and values; there is a limit to what can be subsumed under "privacy".

A further illustration of the restriction of the efficacy of oversight can be found in the UK's attempt to improve data handling in government in the wake of many breaches of databases that disclosed sometimes highly sensitive personal information to those who ought not to have it, or that lost such data through careless stewardship of hardware and software. Steps were taken to tighten up the systems of internal governmental oversight concerning the handling of personal data. A major report from the then Head of the Civil Service strongly endorsed PIA for use in all government departments and pledged that future reviews of information and communication technology projects would check that PIAs have been carried out as part of risk management assessment. It also highlighted the link between human rights (e.g., privacy) and data protection in its call for improving the administrative culture within which databases are used.[253] However, this did not seem to extend to the collection of information in the first place, and the emphasis placed on data *security* – although a valuable safeguard and principle of oversight – also fell short of a more robust incorporation of rights- and values-based oversight, or even of the full range of data protection principles that bear upon the privacy of personal data. Moreover, the implementation of cultural change in government organisations, for example, through better training about the importance of the responsible handling of data as an information asset under the stewardship of officials, did not imply a grounding in the deeper reasons why information is valuable beyond its importance to government in its

[250] Bennett, Colin J., and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, pp. 260-262.
[251] Flaherty, David H., "Privacy Impact Assessments: An Essential Tool for Data Protection", in Stephanie Perrin, Heather Black, David H. Flaherty and T. Murray Rankin, *The Personal Information Protection and Electronic Documents Act: An Annotated Guide*, Irwin Law, Inc. Toronto, p. 266.
[252] Wright, David, and Charles Raab, "Constructing a surveillance impact assessement", *Computer Law & Security Review*, Vol.28, No. 6, December 2012.
[253] Cabinet Office, *Data Handling Procedures in Government: Final Report June 2008* ['The O'Donnell Report'], The Stationery Office, London, 2008, p. 19.

public-policy implementation, and to the necessary trust relationship between citizens and the state.

Data protection authorities (DPAs) as external overseers and regulators typically focus upon the privacy-related implications of surveillance and find it difficult to embrace a wider perspective of values in their regulatory exhortations and enforcement practice. The laws within which they operate do not normally give them a licence to roam across the range of values to invoke when they seek to limit surveillance. Yet they sometimes do recognise, and warn against, affronts to the freedoms and rights to which privacy or data protection legitimately extend.

Some instances of this can be cited. The Article 29 Working Party, comprised of all EU Member States' DPAs, typically invokes not only the specific right of privacy but the "larger gamut" of "fundamental rights and freedoms" of EU citizens, to which Article 1(1) of the EU Data Protection Directive 95/46/EC refers, in reinforcing its views.[254] With regard to the surveillance of employees in the workplace, it pointed to principles for safeguarding individuals' rights, freedoms and dignity, sometimes showing how privacy and dignity were linked in the employment laws of some EU countries.[255] It also quoted, with approval, the *Niemitz v. Germany* case's expansive conception of the social value of privacy: "Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings". With regard to video surveillance, the Article 29 Working Party gave consideration to

> the right to free movement of individuals…which is safeguarded by Article 2 of Additional Protocol No. 4 to the European Convention for the Protection of Human Rights and Fundamental Freedoms.
>
> This freedom of movement may only be subject to such restrictions as are necessary in a democratic society and proportionate to the achievement of specific purposes. Data subjects have the right to exercise their freedom of movement without undergoing excessive psychological conditioning as regards their movement and conduct as well as without being the subject of detailed monitoring…[256]

A further instance of this can be found in the observation of the Article 29 Working Party and The Working Party on Police and Justice (set up as a working group of the Conference of the European Data Protection Authorities) about a shift in emphasis within law enforcement towards new ways of working with personal information and the new use of technologies that "may have a profound impact on the privacy and data protection of all citizens and on the very possibility for them to really enjoy and be able to exercise their *fundamental rights*, in particular whenever *freedom of movement, freedom of speech, and freedom of expression* are at issue."[257]

---

[254] Article 29 Working Party, "Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance", WP 89, 11 February 2004, p. 5.
[255] Article 29 Working Party, "Working Document on the Surveillance of Electronic Communications in the Workplace", WP 55, 29 May 2002; The Niemitz case quotation is at ECHR, 23 November 1992, Series A No. 251/B, para. 29.
[256] Article 29 Working Party, "Working Document on the Surveillance of Electronic Communications in the Workplace", WP 55, 29 May 2002, p. 6.
[257] Article 29 Working Party and Working Party on Police and Justice, "The Future of Privacy", WP 168, 01 December 2009, p. 25; emphasis added.

Thus, there is at least some indication that, amongst regulators, a broader sense of values, rights and freedoms, and/or their close relationship with privacy and data protection in a stricter sense, has been recognised as important in the oversight of surveillance. Surveillance has a demonstrable effect on individuals or on categories of persons, and not only on their privacy, but whether this toehold of recognition of a wide array of rights, freedoms and values in data protection and privacy oversight is broad enough in practice to counter the wide-ranging effects of surveillance is not certain.

7 FINDINGS AND RECOMMENDATIONS

In this last chapter, we have collated and present here the findings and recommendations from the preceding chapters. The findings and recommendations have been organised according to the chapter from which they have been extracted.

7.1 THE CO-EVOLUTION OF SURVEILLANCE TECHNOLOGIES AND SURVEILLANCE PRACTICES

Findings

Surveillance is (and has always been) a normal element of modern society. Registering and identifying citizens began in the 18th century and was an important prerequisite for a modern centralised government. The data was necessary for taxation, provision of public infrastructure and the modern welfare state. In the 19th and early 20th century, surveillance became an important element in industrialism's division of labour. In the post-industrial age, information and surveillance have become a lubricant of the information society. Histories, culture, legislative legacies, administrative rules and procedures, and vested interests, all play a role in shaping the use of surveillance technologies.

Surveillance seems to make life more predictable and calculable. It synchronises behaviour and provides a platform for social interaction in a modern, anonymous world. These are useful things, but the belief that greater surveillance can overcome problems such as the incompleteness of information or the partiality of abstraction is a dangerous delusion. Most of the examples from the different historical periods show that each useful application of surveillance also bears the danger of totalitarianism. Information and its use create an even greater need for information for even more beneficial purposes. The naïve thinking that those "who have nothing to hide, have nothing to fear" and that people "would be happy to give up a little privacy in return for more convenience, security, etc." leads to a situation where the abuse potential exceeds any real or perceived benefits. In the current scenario, it is an illusion to believe that one can erase personal information stored in a networked system.

There are numerous open questions about the usefulness and effectiveness of surveillance technologies and their possible rebound effects, specifically in relation to surveillance measures introduced to fight terrorism and organised crime without knowledge of their effectiveness and consideration of their negative side effects (such as false positive matches, the inversion of the presumption of innocence, and costs of intensified security checks). The question of what impact greater surveillance has on an open society is still under debate. While counter-surveillance movements show that citizens are not always willing to follow the rationale of government agencies and industry, the case of surveillance cameras illustrates that citizens are gradually becoming accustomed to these measures.

Another important trend that can be observed while studying the history of modern surveillance is the gradual multi-directional function creep (as exemplified by the dragnet investigation in Germany which shows how an instrument originally intended for analysing and fighting the societal root of criminality turned into a law enforcement tool that was finally perceived as oppressive). Recent years yield evidence of a trend toward using crime fighting technologies to address anti-social and undesirable behaviour as tool for community development. Related to this is the expanding role of surveillance in law enforcement and a

shift in its use in identifying offenders before they have committed a crime. This has affected the presumption of innocence in way that citizens are now considered suspects (a shift to a presumption of guilt).

Recommendations

There is a need to address the assumption that greater surveillance can overcome current security threats.

The implementation and use of surveillance technologies and measures must be preceded by an impact assessment that particularly addresses concerns and potential problems in relation to them.

Cases of function creep in the implementation and use of surveillance technologies must be taken more seriously. Particularly, there is a need to do something to reverse the notion of "suspect till proven innocent" that the current use of surveillance technologies fosters.

There is a need for greater transparency, accountability and purpose-based use of surveillance technologies.

7.2 THE SURVEILLANCE INDUSTRY IN EUROPE

Findings

The European surveillance industry is developing at a rapid pace, supplying increasing demands in the public and private sector, across a range of areas. It is characterised by a vast diversity of companies (based on organisational history, revenues, size, location, operation and organisational focus) providing a variety of surveillance solutions and a portfolio of expanding applications. The industry is characterised by the presence of a large number of non-European companies, particularly from the USA. Conversely, European companies, driven by the economic downturn in Europe, the huge potential of foreign markets and their receptiveness to surveillance solutions, are investing heavily in non-European markets.

The future of surveillance is set. Most surveillance reports predict an increasing demand for surveillance solutions (stand-alone and integrated), rapid growth for the industry and strong market growth prospects. From our research, we have identified the following trends: (1) a substantial growth of public sector demand for surveillance bolstered by the adoption of identity schemes and terrorist detection technologies and markets, (2) an increase in the demand for civil and commercial surveillance, (3) the development of a global industry in surveillance, (4) an increase in integrated surveillance solutions, and (5) a rise in the government use of cross-border surveillance solutions. Surveillance companies from Europe will face stiff competition from companies from outside the European Union.

Despite the positive outlook for the surveillance industry, of the future presents various challenges. One challenge is the lack of security awareness and attitudes, resulting from a decreased demand for security and surveillance products and services. Another challenge is stricter government regulation that might stifle the industry's development and growth. Financial challenges – higher duties and costs applicable to surveillance products – might deter the industry's future prospects and growth. Some surveillance technologies may be

rejected by the public due to privacy, ethics and other human rights concerns. Competition is another challenge facing the surveillance industry in Europe; if the industry is to flourish, it must learn to deal with this.

Surveillance companies have courted controversies such as unethical and even illegal business practices, privacy and security concerns, sale of technologies to authoritarian and undemocratic regimes, human rights abuses, conflict zone profiteering, general surveillance-related profiteering and pro-surveillance thrusts, misleading consumers, and anti-competitive practices. Overall, these controversies have affected the industry's reputation.

Though some surveillance companies offer assurances that they act in conformity with legal and social obligations and values, these are inadequately expressed and followed through. A majority of companies neglect these obligations and values. Civil society organisations, advocacy groups, academics and the media have expressed concerns about companies' attitudes to fundamental rights – privacy, data protection, freedom of expression and freedom of movement, in particular. While some good practices exist, they are inadequate compared to the potential for abuse of some of the surveillance technologies that the industry is developing and marketing.

In addition to (generally inadequate) government oversight, the media, civil society, academia and individuals can play a role in watching over the surveillance industry. Nevertheless, each of these watchers is limited by their motivations and activities and this affects somewhat the effectiveness of their impact.

Recommendations

Based on our findings, and given the economically significant role played by the European surveillance industry, overall, we recommend a cautious approach in any actions or measures to regulate the surveillance industry. This is particularly so that European surveillance companies are not put at an undue disadvantage through hastily introduced legislation and other requirements not borne by surveillance industry players based elsewhere.

Europe requires a multi-level strategy to address surveillance concerns and build resilience. In this, we recommend that industry associations (which our research reveals are powerful entities) are taken on board and included to enhance the effectiveness of resilience. Industry associations can regulate members to a reasonably good degree and can develop surveillance-related guidelines and codes of ethics, foster greater corporate social responsibility practices, develop standards and so on.

Legal regulation might be the most effective solution to help curb the sale of surveillance solutions to non-acceptable entities and countries.

Greater transparency and accountability for the surveillance industry might come through the adoption of privacy impact assessments (PIAs) or surveillance impact assessments (SIAs) and through the development of standards and certification requirements for surveillance technologies.

There is a need to officially recognise the increasing privatisation of state surveillance, the military-industrial complex, and its impact upon society. Civil society organisations and

academia also have an important role to play here (e.g., in recognising this effect, keeping a watch over its impact and acting to maintain its healthy nature).

Finally, there is a need to fund and create multi-stakeholder platforms or forums and even a European surveillance industry observatory (either within existing platforms or as a fresh initiative) to continuously monitor the industry.

7.3 THE EFFECTIVENESS OF SURVEILLANCE IN PREVENTING AND DETECTING CRIME AND TERRORISM

Findings

Crime is not a natural kind but a socially defined legal-bureaucratic category. All data about the volume of crime in a society are the product of a complex administrative procedure. Therefore, when assessing the effects of different surveillance technologies on preventing and detecting crime, the data have to be interpreted with great caution.

Surveillance technologies are not evenly applied to prevent and detect all sorts of crimes and not all technologies lend themselves to all types of crimes. This makes it difficult to produce an overall conclusive assessment of the effectiveness of surveillance in preventing and detecting crime and terrorism. Systematic evaluation studies conducted by independent researchers about the use and effectiveness of surveillance technologies are rare. Technologies that have been evaluated, e.g., CCTV, show mixed evidence. Long-term effects may counter short-term effects; external effects, such as displacement, have been reported in the literature.

The use of surveillance technologies in the field of law enforcement has to be understood as being embedded in the emergence of the modern bureaucratic state. Individuals and the social world have become “machine readable” as a consequence of the application of surveillance technologies (e.g., ANPR). An important aspect in the development of surveillance technologies is the introduction of electronically mediated digital forms of data processing. With the growth of data collected through surveillance (e.g., finger prints) the management and retrieval of information becomes time consuming. When this information is available in a digitized format, and search procedures can be performed automatically, the use of the stored data in the context of fighting crime (e.g., comparing data from crime scenes with information stored in police data files) is easy.

Digitizing the processing of data from surveillance technologies creates new assemblages, combining information from different sources to identify or describe an individual. These data can be communicated and made available wherever there is access to a computer.

The growth of modern digitized surveillance technologies fosters a shift in the orientation of policing from a reactive form of “thief-taking” to a proactive approach, focussing on prevention and early identification of potentially suspicious individuals. This again promotes a shift from the focus on the criminal to control of the so-called “pre-criminal”. With the growth of encompassing preventive surveillance, the presumption of innocence as an important legal safeguard is gradually hollowed out.

Surveillance technologies also affect the working routines of law enforcement personnel. Doing police work in an information-intensive environment creates new forms of policing, with new tasks, requiring new capabilities and competences typically not available to the traditional street cop. The emerging new forms of intelligence-led policing require a new type of professional police officer.

When considering shifts in the general orientation of crime control and criminal justice, the spread of surveillance seems to be an element in a new regime of actuarial justice or flexible normalism. There is a reorientation from the focus on manifest norm-breaking behaviour to a focus on preventive risk assessment. This shift of focus and the decoupling of norm and behaviour is paving the way for massive surveillance as a new gold standard of crime control, which nicely fits with a major societal trend of dangerisation.

Very often, new surveillance systems are introduced without any prior evaluation or assessment. System providers implement new technologies in local pilots without considering that changes in technology almost always imply an organisational change. The problem is that law enforcement agencies operate in a strict legal context, defining duties, responsibilities and accountability of the agency. Further, rather than law determining the use of the technology, law is reactive and adapted post-hoc; it often legalises current practice rather than shaping practice on the basis of a principled approach. This system is particularly susceptible to function creep as the range of applications and use of surveillance technologies gradually expands. The law is often incapable of regulating these interactions or synergy effects, as different isolated technologies get integrated into a greater surveillance assemblage. Law is lagging behind and the main mode of regulation is what legal scholars refer to as “post-hoc legalistion”.

Recommendations

A comprehensive understanding of surveillance requires a multidimensional approach, looking at instruments, tools and parameters and, above all, the analysis of surveillance practices has to consider the social embedded-ness of technologies (or tools).

Heretofore, it is extremely rare for surveillance measures to be properly evaluated before implementation. This is a highly problematic situation. We recommend that surveillance measures are subject to prior assessment and evaluation not only on the basis of their ‘processual’ efficiency but also on the basis of their impact or outcomes.

7.4 SOCIAL AND ECONOMIC COSTS OF SURVEILLANCE

Findings

Important social costs of surveillance include the social damage caused by false positives of suspects of criminal and terrorist activities, the categorical suspicion and discrimination of members of certain social or ethnic groups, the marginalising effects and social inequalities caused by invasive monitoring of those of lower social status, the inhibitory effects of surveillance which can undermine social and democratic activities, or the erosion of trust in society.

Direct economic costs of surveillance include the costs of developing, implementing and operating surveillance technologies, the increase of costs in sectors and activities where such technologies are built into the normal operation (transport, travelling, financial transactions), while the several indirect economic costs include the reduced level of innovation due to increased conformity, the impact of changes in behaviour on welfare, the costs of decreasing individual responsibility for security due to reliance on surveillance systems.

These various social (and economic) costs do not have the same effect in all societies; these costs may have different significance in societies based on their priorities, different political and historical traditions and dissimilar levels of resilience towards surveillance.

For the legitimization, or more precisely, for guaranteeing the legitimate nature, of a decision to introduce, extend, or even discontinue the use of surveillance methods and tools, both social and economic costs must be considered and evaluated. An analysis of social costs is indispensable to set the scope of the power in general, and to mark the boundaries of surveillance in concrete cases. If a decision (or the lack of it) implies social costs, it has to be justified that the costs are worth the end result, consequently the decision is permissible. If such a justification is missing, the decision is arbitrary. Mapping and analysing social costs is necessary not only for making an adequate decision about the permissibility of surveillance but also to ensure the possibility of justifying the decision retrospectively.

The mere fact that surveillance may have negative social or economic impacts does not mean that such surveillance is not permissible; its costs should always be compared to its legitimate aim. A minimum requirement of a decision on surveillance is that a publicly accessible and reasonable argument should counterbalance the social and economic costs resulting from surveillance.

We acknowledge that certain social and economic costs may have long lasting effects which exert an impact on society beyond the actual costs of a particular case of surveillance.

Recommendations

Therefore, we make the following recommendations for decision-makers while taking into account of the social and economic costs of surveillance:

- The decision-making process must duly consider and evaluate the social and economic costs of surveillance, make an unbiased representation of interests and values, and guarantee the use of adequate expertise of stakeholders.
- When restriction of fundamental rights is at stake, the principle of proportionality and the tests of necessity, suitability and proportionality should be applied.
- A decision implying social costs must be justifiable on grounds of whether the costs are worth the end result, and if such a deliberation is missing, it makes the decision unjustifiable and illegitimate in itself.
- Empirical data regarding social costs should be used with precaution.
- A wide range of stakeholders should be involved in the process, according to the scale and characteristics of the subject of the decision; the opinion of information technology professionals is particularly relevant.
- While it is advisable to use a formalised methodology, such as surveillance impact assessment (SIA), such methodologies should not be used in a casual or bureaucratic manner.

- While these requirements may impose additional burdens on decision-makers, such a process may result in improved, substantiated decisions and will ensure the possibility of justifying the decision from the legal and ethical points of view, even retrospectively.

Further, we note that, on one hand, there is the relevance, magnitude and importance of social and economic costs of surveillance and, on the other, there is the difficulty of identifying, assessing and quantifying them. To deal with this, we make two recommendations. First, further research on methodological improvements on the analyses of social and economic aspects of surveillance is needed to improve the reliability and comparability of such assessments. Second, we need to recognise the complexity of the involved issue, the danger of domination by individual interests, demands for the representation of different interests and perspectives in any surveillance-based decision-making.

7.5 IMPACTS OF SURVEILLANCE ON CIVIL LIBERTIES AND FUNDAMENTAL RIGHTS

Findings

Our analysis of the impacts of surveillance on civil liberties and fundamental rights yielded several provisional themes and findings:

- Surveillance technologies and practices have an actual or potential impact (mainly negative, but sometimes positive) upon a wide range of individual and trans-individual rights, freedoms and values.
- The effects of surveillance go beyond those that concern individual privacy, dignity, autonomy, and the presumption of innocence, and can also be seen in terms of a number of dimensions of social and political life.
- There are gaps and deficiencies in the law and in jurisprudence as they struggle to keep pace with technological development and institutional practice, perhaps especially in an online environment and in a climate of enhanced law enforcement and counter-terrorist policy.

Discussing the impact of surveillance on a host of rights and values, and the impact of rights and values on surveillance requires conceptual disaggregation and clarity, detailed and systematic analysis, and empirical evidence. The degree to which all these *desiderata* are currently available is uneven, but our analysis of the impacts of surveillance on civil liberties and fundamental rights has shown how they can be brought to bear on a subject that is sometimes ambiguous (e.g., the concepts of privacy and surveillance) and sometimes not easily amenable to reliable empirical research (e.g., social and psychological effects), but with reasonable prospects of making subsequent judgements about the resilience of societies in the context of surveillance.

Data protection authorities (DPAs) as external overseers and regulators typically focus upon the privacy-related implications of surveillance and find it difficult to embrace a wider perspective of values in their regulatory exhortations and enforcement practice. The laws within which they operate do not normally give them a licence to roam across the range of values to invoke when they seek to limit surveillance.

Thus, there is at least some indication that, amongst regulators, a broader sense of values,

rights and freedoms, and/or their close relationship with privacy and data protection in a stricter sense has been recognised as important in the oversight of surveillance. Surveillance has a demonstrable effect on individuals or on categories of persons, and not only on their privacy, but whether this toehold of recognition of a wide array of rights, freedoms and values in data protection and privacy oversight is broad enough in practice to counter the wide-ranging effects of surveillance is not certain.

Recommendations

It is important that assessment and oversight be based on thought and judgement, rather than becoming a perfunctory box-ticking bureaucratic exercise. An institutional tendency towards the latter would blunt the effect of rights and values upon oversight because it would reduce the procedure to items in a questionnaire rather than keeping a focus upon the reasons for limiting surveillance. Satisfactory oversight therefore faces the prospect of dilution, although that is not only a danger for PIA or SIA. Privacy, insofar as it is reflected in data protection, seems to be a right and value that is better served by oversight routines within organisations, and even when exercised by external regulatory bodies, than would be the fuller range of rights and values; there is a limit to what can be subsumed under privacy.

More effective regulation requires that existing regulatory philosophies, practices, laws and enforcement incorporate better development of anticipatory regulatory strategies that include design-stage controls, governance and evaluative instruments.

8 REFERENCES

3M, Annual Report 2011. http://media.corporate-ir.net/media_files/irol/80/80574/Annual_Report_2011.pdf

Aas, Katja Franko, "'Crimmigrant' bodies and bona fide travelers: Surveillance, citizenship and global governance", *Theoretical Criminology*, Vol. 15, No. 3, 2011, pp. 331-346.

ABI Research, "The RFID Market Will be Worth over $70 Billion Across the Next Five Years", 16 April 2012. http://www.abiresearch.com/press/the-rfid-market-will-be-worth-over-70-billion-acro

ABI Research, RFID Market by Application and Vertical Sector, Research Report. 2012. http://www.abiresearch.com/research/product/1006085-rfid-market-by-application-and-vertical-se/

Abrams, Philip, *Historical sociology*, Cornell University Press, Ithaca, New York, 1982.

Abu-Laban, Yasmeen, "The politics of surveillance, Civil liberties, human rights and ethics", in Kirstie Ball, Kevin D. Haggerty, and David Lyon (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, London, 2012, pp. 420-427.

Acxiom Corporation, Annual Report 2012. www.acxiom.com/about-acxiom/investor-info/reports/

Adey, P., "Facing Security Airport: Affect, Biopolitics, and the Preemptive Securitisation of the Mobile Body", Environment and Planning D: Society and Space, No. 27, February 2009, pp. 274-295.

Agamben, Giorgio, *Qu'est-ce qu'un dispositif?*, Payot & Rivages, Paris, 2007.

Akdeniz, Yaman, "Freedom of Expression on the Internet: A study of legal provisions and practices related to freedom of expression, the free flow of information and media pluralism on the internet in OSCE participating states", Report, OSCE, Office of the Representative on Freedom of the Media, 2010. http://www.osce.org/fom/80723.

Almunia, Joaquín, "Policy Statement of VP Almunia on the Google antitrust investigation," Press room Brussels, SPEECH/12/372 21 May 2012. http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/372&format=HTML&aged=0&language=EN&guiLanguage=en

Aly, Götz, Karl Heinz Roth, Edwin Black, and Assenka Oksiloff, *The Nazi census: Identification and control in the Third Reich*, Temple University Press, Philadelphia, 2004.

American Civil Liberties Union, "ACLU Opposes Use of Face Recognition Software in Airports Due to Ineffectiveness and Privacy Concerns," American Civil Liberties Union, 29 Nov. 2002. http://archive.aclu.org/issues/privacy/FaceRec_Feature.html

American Civil Liberties Union, "Surveillance Under the USA/PATRIOT Act", New York, last updated 23 October 2001. http://www.aclu.org/technology-and-liberty/surveillance-under-usapatriot-act

Amicelle, Anthony and Gilles Favarel-Garrigues, "Financial surveillance: Who cares?", *The Journal of Cultural Economy*, Vol. 5, No. 1, January 2012, pp. 105-124.

Amicelle, Anthony and Gilles Favarel-Garrigues, "La lutte contre l'argent sale au prisme des libertés fondamentales: Quelles Mobilisations?", *Cultures & Conflits*, No. 76, 2009, pp. 39-66.

Amicelle, Anthony, "The Great (Data) Bank Robbery: The Terrorist Finance Tracking Program & the SWIFT Affair", Research Questions, CERI, No. 36, May 2011, pp. 1-27.

Amicelle, Anthony, "Towards a 'new' political anatomy of financial surveillance", *Security Dialogue*, Vol. 42, No. 2, May 2011, pp. 161-178.

Amicelle, Anthony, “Trace my money if you can: European Security Management of Financial Flows”, in Ulrika Morth and Karin Svedberg Helgesson (eds.), *Transforming the Public Domain: Privatization, Securitization and Accountability in the Field of AML*, Routledge, London, 2012, pp. 110-131.

Amoore, Louise, and Marieke De Goede (eds.), *Risk and the War on Terror*, Routledge, London, 2008.

Amoore, Louise and Marieke De Goede, “Governance, risk and dataveillance in the war on terror”, *Crime, Law & Social Change*, Vol. 43, 2005, pp. 149-173.

Amoore, Louise, and Marieke De Goede, “Introduction. Data and the war by other means”, *Journal of Cultural Economy*, Vol. 5, No. 1, 2012, pp. 3-8.

Amoore, Louise, Stephen Marmura and Mark Salter, “Editorial: smart borders and mobilities: spaces, zones, enclosures”, *Surveillance & Society*, Vol. 5, No. 2, 2008, pp. 96-101.

Anderson, Margo J., *The American Census: A Social History*, Yale University Press, New Haven and London, 1988.

Andreas, Peter, and Timothy Snyder (eds.), *The Wall around the West: State Borders and Immigration Control in North America and Europe*, Rowman & Littlefield, Lanham, 2000.

Andronikou, Vassiliki, Angelos Yannopoulos and Theodora Varvarigou, "Biometric Profiling: Opportunities and Risks", in Mireille Hildebrandt, and Serge Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer, Dordrecht, 2008, pp. 131-145.

ANSA (Agenzia Nazionale Stampa Associata), “Finmeccanica chairman steps down amid slush-fund probe: Guarguaglini bows to pressure, CEO Orsi takes over”, 1 December 2011.
http://www.ansa.it/web/notizie/rubriche/english/2011/12/01/visualizza_new.html_111180804.html

Aradau, Claudia, Luis Lobo-Guerrero and Rens Van Munster, “Security, technologies of risk, and the political: guest editors’ introduction”, *Security Dialogue*, Vol. 39, No. 2-3, September 2008, pp. 147-154.

Ardizzone, Georgia, “The British government knows more about surveillance exports than it is letting on”, Privacy International, 17 July 2012.
https://www.privacyinternational.org/blog/the-british-government-knows-more-about-surveillance-exports-than-it-is-letting-on

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.

Armstrong, K., A. Wilson, B. Watson, J. Freeman, and J. Davey, “Evaluation of ANPR trials for Traffic Policing in Queensland, Report to the Queensland Police Service” State Traffic Support Branch, Queensland: The Centre for Accident Research and Road Safety, Queensland, 2010.

Ars Technica, “Facial regonition tech is rocketing ahead of laws that can control it”, 19 July 2012. http://arstechnica.com/business/2012/07/facial-regonition-tech-is-rocketing-ahead-of-laws-that-can-control-it/

Arteaga Botello, Nelson, “Surveillance and Urban Violence in Latin America: Mega-Cities, Social Division, Security and Surveillance”, in Kirstie Ball, Kevin Haggerty and David Lyon (eds.), *Routledge handbook of surveillance studies*, Routledge, New York, 2012, pp. 259-266.

Article 29 Working Party and Working Party on Police and Justice, “The Future of Privacy”, WP 168, 01 December 2009.

Article 29 Working Party, "Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance", WP 89, 11 February 2004.

Article 29 Working Party, "Working Document on the Surveillance of Electronic Communications in the Workplace", WP 55, 29 May 2002.

Aufhauser, D., "Terrorist financing: foxes run to ground", *Journal of Money Laundering Control*, Vol. 6, No. 4, 2003, pp. 301-305.

Aycock, Alan, "The confession of the flesh: disciplinary gaze in casual bodybuilding", *Play and Culture,* Vol. 5, No. 4, 1992, pp. 338–357.

Backhouse, James, and Ana Canhoto, "General Description of the Process of Behavioural Profiling", in Serge Gutwirth and Mireille Hildebrandt (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer science, Brussels, 2008, pp. 47-63.

Backhouse, James and Ana Canhoto, "Profiling under conditions of ambiguity: an application in the financial services industry", *Journal of Retailing and Consumer Services,* Vol. 14, No. 6, 2007, pp. 408-419.

BAE Systems, Annual Report 2011. http://www.baesystems.com/cs/groups/public/documents/document/mdaw/mdu2/~edisp/baes_045566.pdf

Ball, Kirstie, "Workplace surveillance: An overview", *Labor History,* Vol. 51, No. 1, 2010, pp. 87-106.

Ball, Kirstie, Elizabeth Daniel, Sally Dibb and Maureen Meadows, "Democracy, surveillance and 'knowing what's good for you': the private sector origins of profiling and the birth of 'citizen relationship management'", in Kevin Haggerty and Minas Samatas (eds.), *Surveillance and Democracy*, Routledge, New York, 2010, pp. 111-126.

Ball, Kirstie, Kevin Haggerty and David Lyon (eds.), *Routledge handbook of surveillance studies*, Routledge, New York, 2012.

Ball, N., "Civil Society Actors in Defence and Security Affairs", in M. Caparini, P. Fluri & F. Molnar (eds.), *Civil Society and the Security Sector: Concepts and Practices in New Democracies*, DCAF, Geneva, 2006.

Balzacq, T., "The policy tools of secuyritization: Information exchange, EU foreign and interior policies", *Journal of Common Market Studies*, Vol. 46, No. 1, January 2008, pp. 75-100.

Banisar, David, *Speaking of Terror. A survey of the effects of counter-terrorism legislation on freedom of the media in Europe,* Media and Information Society Division, Directorate General of Human Rights and Legal affairs Council of Europe, 2008.

Bannister, Jon , Simon Mackenzie, and Paul Norris, "Space CCTV in Scotland: Results of a National Survey of Scotland's Local Authorities", Public Report 03/09, The Scottish Centre for Crime and Justice Research, Glasgow, 2009.

Barak, Greg (ed.), *Media, Process, and the social construction of crime: studies in newsmaking criminology*, Garland Publ., New York, London, 1994.

Barthe, Yannick, Michel Callon and Pierre Lascoumes, *Agir dans un monde incertain : essai sur la démocratie technique,* Editions du Seuil, Paris, 2001.

Bartlett, Jamie and Carl Miller, *The power of unreason. Conspiracy theories, extremism and counter-terrorism*, Demos, London, 2010.

Bauman, Zygmunt, *Intimations of postmodernity*. Routledge, New York, 1992

BBC News, "Boy's eyes gouged in Birmingham bus attack", *BBC News*, 25 September 2012. http://www.bbc.co.uk/news/uk-england-birmingham-19711598

BBC News, "Man in dress exposes himself on Lincoln-Grimsby train", *BBC News*, 19 October 2012. http://www.bbc.co.uk/news/uk-england-lincolnshire-20003183

BBC News, “Phone-hacking scandal: Timeline”. http://www.bbc.co.uk/news/uk-14124020.
BBC News, “Probe into data left in car park”, BBC News, 2 November 2008. http://news.bbc.co.uk/2/hi/7704611.stm
BBC News, “PSNI urged to wear body cameras to tackle domestic abuse”, *BBC News,* 18.10.2012. http://www.bbc.co.uk/news/uk-northern-ireland-19987607
BBC News, “Qinetiq listings probe launched,” BBC News, 26 January 2006. http://news.bbc.co.uk/2/hi/business/4651440.stm
BBC News, “Sobriety orders to be piloted by government”, *BBC News* 2012. http://www.bbc.co.uk/news/uk-17407493
BBC News, “Southampton City Council appeals to keep taxi cameras”, *BBC News,* 16 August 2012. http://www.bbc.co.uk/news/uk-england-hampshire-19290688
BBC News, “Swansea traffic wardens to wear cameras to record abuse”, *BBC News,* 22 September 2012. http://www.bbc.co.uk/news/uk-wales-south-west-wales-19673860
BBC News, “US style tests to be used for problem drinkers”, *BBC News* 2012. http://www.bbc.co.uk/news/uk-england-london-16970501
BCC Research, “Smart Card Technologies and Global Markets - Focus on Europe”, July 2012. http://www.bccresearch.com/report/smart-card-europe-markets-ift097a.html
Beck, Ulrich, “Risk Society and the Provident State”, in Scott M. Lash, Bronislaw Szerszynski, and Brian Wynne (eds.), *Risk, Environment and Modernity: Towards a New Ecology*, Sage Publications, London, 1996, pp. 27–43.
Becker, Howard, *Outsiders*, Free Press, New York, 1963.
Beckett, Katherine, *Making Crime Pay: Law and order in Contemporary American Politics,* Oxford University Press, New York, 1997.
Bell, Mebbie, “Re/Forming the anorexic ‘prisoner’: Inpatient medical treatment as the return to panoptic feminity”, *Cultural Studies ⇔ Critical Methodologies*, Vol. 6 No. 2, 2006, pp. 282–307.
Bellanova, Rocco, and Paul De Hert, “Le cas S. et Marper et les donnees personnelles : l’horloge de la stigmatisation stoppee par un arret Europeen”, *Cultures & Conflicts* Vol. 76, 2009, pp. 101-114.
Bellanova, Rocco, and Denis Duez, “A different view on the 'making' of European security: The EU Passenger Name Record System as a socio-technical assemblage”, *European Foreign Affairs Review*, No. 17, 2012, pp. 109-124.
Bellanova, Rocco, and Michael Friedewald (eds.), *Deliverable 1.1: Smart Surveillance – State of the Art*, FP7 Sapient Project, Brussels, 2011. http://www.sapientproject.eu/
Bellizzi, Joseph A., and Terry Bristol, “An assessment of supermarket loyalty cards in one major US market”, *Journal of Consumer Marketing*, Vol. 21, No. 2, 2008, pp. 144–154.
Bendrath, Ralf, and Milton Mueller, “The End of the Net as we know it? Deep Packet Inspection and Internet Governance”, *New Media & Society*, Vol. 13, No. 7, 2011, pp. 1142–1160.
Beniger, James R., *The Control Revolution: Technological and Economic Origins of the Information Society*, Harvard University Press, Cambridge, Mass., 1986.
Benn, Stanley I., “Privacy, freedom and respect for persons”, in Pennock, J. Roland and John W. Chapman (eds.), *Nomos XIII: Privacy*, Atherton Press, New York, 1971, pp. 1-26.
Bennett, Colin J. and Charles D. Raab, *The Governance of Privacy Policy Instruments in Global Perspective*, MIT Press, Cambridge MA, 2006.
Bennett, Colin, and Priscilla Regan, “Editorial: Surveillance and mobilities”, *Surveillance & Society*, Vol. 1, No. 4, 2004, pp. 449-455.

Bentham, Jeremy, *Panopticon or the Inspection-House*, T. Payne, London, 1791.
BHE, "BHE policies for video surveillance systems". http://www.bhe.de/die-fachbereiche/videoueberwachung/bhe-richtlinien-fuer-video-ueberwachungsanlagen.html
Bickford Smith, Will "The Surveillance State: Now Even Universities Are At It", 26 May 2011. http://www.bigbrotherwatch.org.uk/home/2011/05/the-surveillance-state-now-even-universities-are-at-it.html
Biersteker, Thomas and Sue Eckert (eds.), *Countering the Financing of Terrorism*, Routledge, London, 2007.
Biersteker, Thomas, "Targeting terrorist finances: the new challenges of financial market globalization", in Ken Booth and Tim Dunne (eds.), *Worlds in Collision: Terror and the Future of Global Order*, Palgrave/St. Martins, London, 2002, pp. 74-84.
Big Brother Watch, "The Price of Privacy: How local authorities spent £515m on CCTV in four years", A Big Brother Watch report, February 2012. http://www.bigbrotherwatch.org.uk/home/2012/02/price-privacy-councils-spend-521m.html
Bigo, Didier, and Elspeth Guild (eds.), "La logique du visa Schengen: la mise à l'écart des étrangers", *Cultures & Conflits* (special issue), No. 49, 2003.
Bigo, Didier, and Elspeth Guild (eds.), *Controlling Frontiers: Free Movement into and within Europe*, Ashgate, London, 2005.
Bigo, Didier, "Du panoptisme au ban-optisme. Les micro-logiques du contrôle dans la mondialisation", in Pierre-Antoine Chardel and Gabriel Rockhill (eds.), *Technologies de contrôle dans la mondialisation. Enjeux politiques, éthiques et esthétiques*, Editions Kimé, Paris, 2009, pp. 59-80.
Bigo, Didier, "Security, Surveillance and Democracy", in Kirstie Ball, Kevin Haggerty and David Lyon (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, New York, 2012, pp. 277-284.
Bigo, Didier, "Security: a field left fallow", in Michael Dillon and Andrew Neal (eds.), Foucault on Security, Politics and War, Palgrave Macmillan, Basingstoke, 2008, pp. 93-114.
Bigo, Didier, and Pierre Piazza, "Les conséquences humaines de l'échange transnational des données individuelles", *Cultures & Conflits*, No. 76, December 2009, pp. 7-14.
Bigo, Didier, Laurent Bonelli and Thomas Deltombe (eds.), *Au nom du 11 septembre… Les démocraties à l'épreuve de l'antiterrorisme*, La Découverte, Paris, 2008.
Bigo, Didier, Philippe Bonditti, Julien Jeandesboz and Francesco Ragazzi, *Security technologies and society: A state of the art on security, technology, borders and mobility*, INEX Deliverable D.1.1, Oslo: PRIO, 2008.
Bigo, Didier, Ricardo Bocco and Jean-Louis Piermay, "Introduction. Logiques de marquage: murs et disputes frontalières", *Cultures & Conflits*, No. 73, 2009, pp. 7-13.
Bigo, Didier, Sergio Carrera, Gloria González Fuster, Elspeth Guild, Paul de Hert, Julien Jeandesboz, and Vagelis Papakonstantinou, "Towards a New EU Legal Framework for Data Protection and Privacy", European Parliament, Brussels, 2011.
Bingham, John, "Universities to carry out 'police-like' surveillance", *The Telegraph*, 10 November 2008. http://www.telegraph.co.uk/education/universityeducation/3416269/Universities-to-carry-out-police-like-surveillance.html
Bits of Freedom, "Dutch proposal to search and destroy foreign computers". 18 October 2012. https://www.bof.nl/2012/10/18/dutch-proposal-to-search-and-destroy-foreign-computers/

Blencowe, T., A. Pehrsson, and P. Lillsunde, “Driving under the Influence of Drugs, Alcohol and Medicine: Analytical evaluation of oral fluid screening devices and preceding selection procedures”, FP7 DRUID project, 2010. www.druid-project.eu/

Blomberg, Stephen Brock, and Adam Z. Rose, "Editor’s Introduction to the Economic Impact of the September 11, 2001, Terrorist Attacks", *Peace Economics, Peace Science, and Public Policy*, Vol. 15, No. 2, 2009, pp. 1-14.

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. http://www.surveillance-and-society.org/articles4(3)/escalating.pdf

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.

Blythe, P. T., P. Knight, and J. Walker, “The Technical and Operational Feasibility of Automatic Number-Plate Recognition as the Primary Means for Road User Charging”, *The Journal of Navigation*, 54 , 2001, pp 345-353.

Boeing, 2011 Annual Report. http://www.envisionreports.com/BA/2012/14427FE12E/5aeaf07f40c94540856bcbf8d53d7e39/Boeing_AR_3-9-12_SECURED_2-reduced.pdf

Boglioli-Randall, Bonnie, “Local co. Narus reportedly sold technology to Egypt”, Examiner.com,5 February 2011. http://www.examiner.com/article/local-co-narus-reportedly-sold-technology-to-egypt

Bölsche, Jochen, *Der Weg in den Überwachungsstaat*, Rowohlt, Reinbek bei Hamburg, 1979.

Bond, David, and Melinda McDougall (Dir). “Erasing David”, Green Lions, UK, 2009. http://erasingdavid.com/

Bonditti, Philippe, “Biométrie et maîtrise des flux: vers une ‘geo-technopolis du vivant-en- mobilité’? ”, *Cultures & Conflits*, No. 58, 2005, pp. 131-154.

Bonditti, Philippe, *L’antiterrorisme aux Etats-Unis* (1946-2007), PhD dissertation, Sciences Po Paris, 2008.

Bonham, Carl, Christopher Edmonds, and James Mak, "The Impact of 9/11 and Other Terrible Global Events on Tourism in the U.S. and Hawaii", *Journal of Travel Research*, Vol. 45, No. 1, 2006, pp. 99-110.

Bonsor, K. and R. Johnson, “How Face Recognition Systems Work”, 2008. http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition3.htm

Borisov, Nikita, Ian Goldberg and David Wagner, “Intercepting Mobile Communications: The Insecurity of 802.11”, *Proceedings of the Seventh Annual International Conference on Mobile Computing And Networking*, July 16–21, 2001.

Böttger, Andreas and Christian Pfeiffer, *Der Lauschangriff in den USA und Deutschland*, Empirische Befunde und kriminalpoliitische Folgerungen zu Überwachungsmaßnahmen der Strafjustiz, KFN-Forschungsbereicht, Hannover, 1993.

Bowker, Geoffrey, and Susan Leigh Starr, *Sorting Things Out: Classification and its Consequences*, MIT Press, Cambridge, MA, 1999.

Bowling, Ben, “The rise and fall of New York murder: zero tolerance or crack's decline?”, *British Journal of Criminology*, Vol. 39, Iss. 4, 1999, pp. 531-554.

Brandtzæg, Petter B., Marika Lüders and Jan H. Skjetnem, “Too many Facebook ‘friends’?: Content sharing and sociability versus the need for privacy in social network sites”, *International Journal of Human-Computer interaction*, Vol. 26, 2010, pp. 1006–1030.

Brennan, Elliot, “Is “Big Brother” always watching us?”, *The Beginner*, 1 June 2011**.** http://www.thebeginner.eu/technology/all-in-innovation/531-privacy-in-the-21st-century

Brewer, Neil, and Tim Ridgeway, “Effects of supervisory monitoring on productivity and quality of performance” *Journal of Experimental Psychology: Applied*, Vol. 4 No. 3, 1998, pp. 211-227.

Brewer, Neil, “The effects of monitoring individual and group performance on the distribution of effort across tasks”, *Journal of Applied Social Psychology*, Vol. 25, No. 9, 1995, pp. 760–777.

Brewster, Tom, “BBC Under Fire For Secret Use Of RIPA Surveillance Powers” *TechWeekEurope*, 22 August 2012. http://www.techweekeurope.co.uk/news/bbc-ripa-surveillance-bbw-big-brother-90086

Brewster, Tom, “Skype Surveillance Claims Denied” *TechWeekEurope*, 27 July 2012. http://www.techweekeurope.co.uk/news/skype-sp-claims-denied-87703

British Psychological Society, “A review of the current scientific status and fields of application of Polygraphic Deception Detection”, 2004. http://www.bps.org.uk/content/review-current-scientific-status-and-fields-application-polygraphic-deception-detection

BROAD Project, Broadening the Range Of Awareness and Data protection, 2009-2010. http://www.broad-project.eu.

Broeders, Dennis, “The new digital borders of Europe: EU databases and the surveillance of irregular migrants”, *International Sociology*, Vol. 22, No. 1, 2007, pp. 71-92.

Brouwer, Evelien, *Digital Borders and real rights: Effective remedies for Third-country national in the Schengen information system*, Martinus Nijhoff Publishers, Leiden 2008.

Brown, B., “Closed Circuit Television in Town Centres: Three Case Studies”, *Crime Prevention and Detection*, Series Paper 73, Great Britain Home Office, London, 1995.

Brown, Sheila, “The criminology of Hybrids. Rethinking crime and law in technosocial networks”, *Theoretical Criminology*, Vol 10, May 2006, pp. 223-244

Brownsword, Roger, *Rights, Regulation and the Technological Revolution*, Oxford University Press, Oxford, 2008.

Bruguière, Jean-Louis, *Second report on the processing of EU-originating personal data by the United-States Treasury Departement for Counter Terrorism purposes: Terrorist Finance Tracking Program*, Brussels, 2010.

Bruno, Fernanda, Marta Kanashiro and Rodrigo Firmino, *Vigilância e Visibilidade*., Espaço, Tecnologia e Identificaçâo, Editora Sulina, Porto Alegre, 2010.

Bryant, Susan, "Electronic Surveillance in the Workplace", *Canadian Journal of Communication*, Vol. 20, No. 4, 1995. http://www.cjc-online.ca/index.php/journal/article/view/893/799

Bryce, T.G.K., M. Nellis, A. Corrigan, H. Gallagher, P. Lee and H. Sercombe, “Biometric Surveillance in Schools: Cause for concern or case for curriculum?”, *Scottish Educational Review*, Vol. 42, Iss. 1, 2010, pp. 3-22.

Bureau of Justice Assistance, *Intelligence-Led Policing: The New Intelligence Architecture*, Washington D.C., 2005

Busch, Christophe, “Facing the future of biometrics: Demand for safety and security in the public and private sectors is driving research in this rapidly growing field”, *EMBO Rep.* 2006 July, 7 (SI), S23–S25.
http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1490310/

Buse, Uwe, and Marcel Rosenbach, "The Transparent State Enemy Western Surveillance Technology in the Hands of Despots," *Der Speigel*, 12 August 2011. http://www.spiegel.de/international/world/the-transparent-state-enemy-western-surveillance-technology-in-the-hands-of-despots-a-802317.html

Business Pundit, "The 25 Most Vicious Iraq War Profiteers", 22 July 2008. http://www.businesspundit.com/the-25-most-vicious-iraq-war-profiteers/

Bussolini, J., "What is a dispositive?", *Foucault Studies*, No. 10, 2010, pp. 85-107.

BVerfGE, "Dragnet Investigation II", 4 April 2006. http://www.bverfg.de/entscheidungen/rs20060404_1bvr051802.html.

Bygrave, Lee A., *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International, Den Haag, 2002.

Cabinet Office, *Data Handling Procedures in Government: Final Report*, The Stationery Office, London, 2008.

Cajani, Francesco, "Technologies and Business vs. Law - Cloud computing, transborder access and data retention: a legal perspective from the State which is conducting an investigation", Paper presented to Workshop 4: Transborder access and jurisdiction, Octopus Conference on Cooperation against Cybercrime, Strasbourg, 2012.

Callaghan, George, and Paul Thompson, "We recruit attitude: The selection and shaping of routine call centre labour", *Journal of Management Studies*, Vol. 39, No. 2, 2002, pp. 233–254.

Cameron, A., E. Kolodinski, H. May and N. Williams, "Measuring the effects of Video Surveillance on Crime in Los Angeles", Californian Research Bureau, University of Southern California: School of Policy Planning and Development, 2008. http://www.cctvusergroup.com/Public%20Support%20for%20CCTV.htm

Campbell, Duncan, "Inside Echelon: The History, Structure, and Function of the Global Surveillance System Known as Echelon", in Thomas Y. Levin, Ursula Frohne and Peter Weibel (eds.), *CTRL [SPACE]: Rhetorics of Surveillance from Bentham to Big Brother*, MIT Press, Cambridge, MA, 2002, pp. 158-169.

Campbell, N., "Technology of Suspicion: Coercion and Compassion in Post-Disciplinary Surveillance Regimes", *Surveillance & Society*, Vol. 2, No. 1, January 2004, pp. 78-92.

Campbell-Kelly, Martin, and William Aspray, *Computer: A History of the Information Machine*, Basic Books, New York, 1996.

Campbell-Kelly, Martin, *From Airline Reservation to Sonic the Hedgehoc: A History of the Software Industry*, MIT Press, Cambridge, Mass., 2003.

Carayon, Pascale, "Effects of electronic performance monitoring on job design and worker stress: results of two studies", *International Journal of Human Computer Interaction*, Vol. 6, No. 2, 1993, pp. 177–190.

Carlisle Duncan, Margaret, "The politics of women's body images and practices; Foucault, the Panopticon and 'Shape' magazine," *Journal of Sport and Social Issues*, Vol. 18, 1994, pp. 48–65.

Carr, Timothy, "One U.S. Corporation's Role in Egypt's Brutal Crackdown", *Huffington Post*, 28 January 2011. http://www.huffingtonpost.com/timothy-karr/one-us-corporations-role-_b_815281.html

Castells, Manuel, *The rise of the network society* (3 volumes), Blackwell, Oxford, 1996.

Cavoukian, Ann, *Privacy by Design ... Take the Challenge*, Information and Privacy Commissioner of Ontario, Toronto, 2009.

Ceyhan, A., "Enjeux d'identification et de surveillance à l'heure de la biométrie", *Cultures & Conflits*, No. 64, Winter 2006, pp. 33-47.

Ceyhan, Ayse, "Téchnologie et sécurité: une gouvernance libérale dans un context d'incertitudes", *Cultures & Conflits*, Vol. 64, winter, 2006, pp. 11-32.
Channel 4 News, "'Black boxes' to monitor all internet and phone data", 29 June 2012. http://www.channel4.com/news/black-boxes-to-monitor-all-internet-and-phone-data
Chapman, Gwen E., "Making weight: Lightweight rowing, technologies of power and technologies of the self", *Sociology of Sport Journal*, Vol. 14, No. 3, 1997, pp. 205-223.
Chow, James, James Chiesa, Paul Dreyer, Mel Eisman, Theodore W. Karasik, Joel Kvitky, Sherrill Lingel, David Ochmanek and Chad Shirley, "Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat", Occasional Paper, Rand Corporation, Santa Barbara, CA, 2005. http://www.rand.org/pubs/occasional_papers/2005/RAND_OP106.pdf
Cicourel, Aaron V., *The social organization of juvenile justice*, New York, 1967.
Clark, Liat, "UK must stall export of surveillance tech to brutal regimes, or face legal action," *Wired.co.uk*, 25 July 2012. http://www.wired.co.uk/news/archive/2012-07/25/privacy-international-surveillance
Clarke, Roger, "Dataveillance – 15 Years On", Paper presented at: Privacy Issues Forum run by the New Zealand Privacy Commissioner, Wellington, 28 March 2003. http://www.rogerclarke.com/DV/DVNZ03.html
Clarke, Roger, "Information Technology and Dataveillance", *Communications of the ACM*, Vol. 31, No. 5, 1988, pp. 498-512.
Clarke, Roger, "Introduction to Dataveillance and information privacy, and definition of terms", 2006. http://www.rogerclarke.com/DV/Intro.html
Cochoy, F., "Les effets d'un trop-plein de traçabilité", *La Recherche*, No. 339, 2001, pp. 66-68.
Cohen, J., "Examined Lives: Informational Privacy and the Subject as Object", *Stanford Law Review*, No. 52, May 2000, pp. 1373-1436.
Cohen, Stanley, *Folk Devils and Moral Panics*, Routledge, New York, 2002.
Cole S. A., "More than Zero: Accounting For Error In Latent Fingerprint Identification", *The Journal of Criminal Law and Criminology*, Vol. 95, No. 3., 2005.
Cole S. A., *Suspect Identities: A History of Fingerprinting and Criminal Identification*, Harvard University Press, USA, 2002.
Cole, S. A., "The 'Opinionization' of Fingerprint Evidence", *BioSocieties* 3, 2008, pp. 105-113.
Cole, S. A., "Where the rubber meets the road: Thinking about expert evidence as expert testimony", *Villanova Law Review*, 52, 2007, pp. 803–842.
Coleman, Roy, and Michael McCahill, *Surveillance and Crime*, Sage, London, 2011.
Coleman, Roy, *Reclaiming the Streets: Surveillance, Social Control and the City*, Willan Publishing, Cullompton, Devon, 2004.
Council for Responsible Genetics (CRG), National DNA Datebases, 2011. http://www.councilforresponsiblegenetics.org/dnadata/index_high.html
Council of Europe, European Convention of Human Rights, Council of Europe, 1950. http://www.echr.coe.int.
Council of the European Union, "Council adopts new EU-US agreement on Passenger Name Records (PNR)", Press Release, Luxembourg, 2012. http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/129806.pdf
Council of the European Union, Note on the EU Action Plan on combating terrorism, Doc. 7233/1/07 REV 1, Brussels, 29 March 2007. http://register.consilium.europa.eu/pdf/en/07/st07/st07233-re01.en07.pdf

Council of the European Union, Note on the European Counter-Terrorism Strategy, Doc. 14469/4/05 REV 4, Brussels, 30 November 2005. http://register.consilium.europa.eu/pdf/en/05/st14/st14469-re04.en05.pdf

Council of the European Union, Note on the Prüm Convention, Doc. 10900/05, Brussels, 7 July 2005. http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf

Crawford M., "Facial Recognition Progress Report", 28 Sept. 2011. http://spie.org/x57306.xml

Curry, Michael R., "The Profiler's Question and the Treacherous Traveller: Narratives of Belonging in Commercial Aviation", *Surveillance & Society*, Vol. 1, No. 4, 2004, pp. 475-499.

Dahl, Johanne Y., and Ann Rudinow Sætnan, "'It all happened so slowly': On controlling function creep in forensic DNA databases", *International Journal of Law, Crime and Justice*, Vol. 37, No. 3, 2009, pp. 83-103.

Dandeker, Christopher, "Surveillance and Military Transformation", in Kevin D. Haggerty and Richard V. Ericson (eds.), *The New Politics of Surveillance and Visibility*, University of Toronto Press, 2006, pp. 225-249.

Dandeker, Christopher, *Surveillance, Power and Modernity*, Polity, Cambridge, 1990.

Danna, A., and Gandy, Jr., O., "All that Glitters is Not Gold: Digging Beneath the Surface of Data Mining", *Journal of Business Ethics*, Vol. 40, No. 4, 2002, pp. 373-386.

Darley, Mathilde, "Le contrôle migratoire aux frontières Schengen: pratiques et représentations des polices sur la ligne tchéco-autrichienne", *Cultures & Conflits*, No. 71, 2008, pp. 13-30.

Data Protection Commissioner, "Report of Review of Facebook Ireland's Implementation of Audit Recommendations Published – Facebook turns off Tag Suggest in the EU", 21 September 2012. http://dataprotection.ie/viewdoc.asp?DocID=1233&m=f

De Goede, Marieke, "Hawala Discourses and the War on Terrorist Finance", *Environment and Planning D: society and Space*, 2003, Vol. 21, pp. 513-532.

De Goede, Marieke, "Risk, Preemption and exception in the war on terrorist financing", in Louise Amoore and Marieke De Goede (eds.), *Risk and the War on Terror*, Routledge, London, 2008, pp. 97-112.

De Goede, Marieke, "The Politics of Preemption and the War on Terror in Europe", *European Journal of International Relations*, Vol. 14, No. 1, 2008, p. 164.

De Goede, Marieke, *Speculative security. The politics of pursuing terrorist monies*, University of Minnesota Press, Minnesota, 2012.

De Hert, Paul, "Balancing Security and Liberty within the European Human Rights Framework. A Critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11", *Utrecht Law Review*, Vol. 1, Issue 1, September 2005, p. 86.

De Hert, Paul, and Serge Gutwirth, "Regulating Profiling in a Democratic Constitutional State?", in Serge Gutwirth and Mireille Hildebrandt (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer science, Brussels, 2008, pp. 271-293.

Defy-Id, *Identity Cards - Who Profits? A guide to corporate involvement in the government's Identity Card Scheme*. www.defy-id.org.uk/greasypalms.htm

Delac, Kresimir, Mislav Grgic and Marian Stewart Bartlett (eds.), *Recent Advances in Face Recognition*, In-teh, Croatia, 2008.

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

Deleuze, Gilles, and Félix Guattari, *A Thousand Plateaus*, University of Minnesota Press, Minneapolis, 1987.

Den Boer, Monica, and Jelle Van Buuren, "Security clouds: towards an ethical governance of surveillance in Europe", *The Journal of Cultural Economy*, Vol. 5, No. 1, January 2012, pp. 85-103.

Detector Project, "Human Rights Risks of Selected Detection Technologies Sample Uses by Governments of Selected Detection Technologies", University of Birmingham, 2009. http://www.detecter.bham.ac.uk/documents.html

Di Tella, R. and E. Schargrodsky, Criminal Recidivism after prison and electronic monitoring, U.S. National Bureau of Economic Research, Working Paper No. 15602, 2009.

Diffie, Whitfield, and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, MIT Press, Cambridge, Mass., 2007.

Digital Rights Ireland Limited v The Minister for Communication Marine and Natural Resource et al, High Court, Record No. 2006/3785P, http://www.scribd.com/doc/30950035/Data-Retention-Challenge-Judgment-re-Preliminary-Reference-Standing-Security-for-Costs

Ditton, J. and E. Short, "Yes, It Works, No, It Doesn't: Comparing the Effects of Open CCTV in Two Adjacent Scottish Town Centres" in , K. Painter and and N. Tilley (eds.), *Crime Prevention Studies*, Vol. 10, 1999, pp. 201-224.

Dixon, John, Mark Levine and Rob McAuley, *Street Drinking Legislation, CCTV and public space: exploring attitudes towards public order measures*, Home Office, London, 2003.

Donahue, Joseph, Nicholas Whittemore and Ashley Heerman, "Ethical Issues of Data Surveillance", Ethica Publishing http://www.ethicapublishing.com/ethical/3CH20.pdf

Douglas, Jeremy, "Disappearing Citizenship: surveillance and the state of exception", *Surveillance and Society*, Vol. 6, No. 1, 2009, pp. 32-42. http://www.surveillance-and-society.org/ojs/index.php/journal/article/view/disappearing/disappearing

Drummer, O. H., D. Gerostamoulos, M. Chu, P. Swann, M. Boorman and I. Cairns, "Drugs in oral fluid in randomly selected drivers", *Forensic Sci Int*, 2007, 170, 105, p. 10.

Dubbeld, L., *The regulation of the observing gaze: privacy implications of camera surveillance*, PrintPartners Ipskamp, Enschede, 2004.

Durkheim, Emile, *The Division of Labour in Society*, The Free Press, New York, 1997/1933.

Dworkin, Ronald, *Taking Rights Seriously*, Harvard University Press, 1978.

EBIC (European Banking Industry Committee), *Recommendations for improvements to EC regulations in the field of embargo measures and financial sanctions*, Brussels, August 2004.

EDRi, "Belgian Big Brother Awards 2012" *EDRi-gram*, 1 February 2012, http://www.edri.org/edrigram/number10.2/belgian-bba-2012

EDRi, "Winners of the Dutch Big Brother Awards announced" *EDRi-gram*, 14 March 2012. http://www.edri.org/edrigram/number10.5/bba-netherlands-2012

Edwards, Paul N., *The Closed World: Computers and the Politics of Discourse in Cold War American*, MIT Press, Cambridge, Mass., 1996.

Electronic Frontier Foundation, "And the Privacy Invasion Award Goes To …" 11 May 2012. https://www.eff.org/deeplinks/2012/05/and-privacy-invasion-award-goes-to

Electronic Frontier Foundation, "Defensive Technology". https://ssd.eff.org/tech

Electronic Frontier Foundation, "The Surveillance Self-Defense Project", https://ssd.eff.org/

Electronic Privacy Information Center (EPIC), "EPIC Analysis of Total Information Awareness Contractor Documents", February 2003. http://epic.org/privacy/profiling/tia/doc_analysis.html

Enzensberger, Hans Magnus, „Der Sonnenstaat des Doktor Herold", *Der Spiegel* 25/1979, pp. 68-78.

EOS, "Advocacy Successes: Common Positions for the Future Market". http://www.eos-eu.com/?Page=advocacy

Ericson, Richard. "Ten Uncertainties of Risk-Management: Approaches to Security", *Canadian Journal of Criminology and Criminal Justice*, Vol. 48, No. 3, 2006, pp. 345-357.

ESRAB, *Meeting the Challenge: the European Security Research Agenda*, *A report from the European Security Research Advisory Board*, Office for Official Publications of the European Communities, Luxembourg, September 2006, http://ec.europa.eu/enterprise/policies/security/files/esrab_report_en.pdf

ESRIF, *ESRIF Final Report*, December 2009. http://ec.europa.eu/enterprise/policies/security/.../esrif_final_report_en.pdf

EU Charter of Fundamental Rights, OJ, C 364/10, 18.12.2000

EU Network of Experts on Fundamental Rights, "Commentary of the Charter of Fundamental Rights of the European Union", 2006, pp. 124-131. http://158.109.131.198/catedra/images/experts/COMMENTARY%20OF%20THE%20CHARTER.pdf

European Digital Right Institute, "EU Surveillance: A summary of current EU surveillance and security measures," Digital Right Institute, Paper No 2, 2012. http://www.edri.org/files/2012EDRiPapers/eusurveillance.pdf

European Commission, "A European terrorist finance tracking system: available options", COM (2011) 429 final, Brussels, 2011. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0429:FIN:EN:PDF

European Commission, "Aerospace and Defence Industries Association of Europe", Transparency Register. http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=72699997886-57

European Commission, "Commission Decision C(2005) 409 of 28 February 2005 establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States (Decision not published)", 28.2.2005. http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/borders-and-visas/document-security/index_en.htm.

European Commission, "Commission Decision C(2006) 2909 of 28 June 2006 establishing the technical specifications on the standards for security features and biometrics in passports and travel documents issued by Member States (Decision not published)", 28.6.2006. http://ec.europa.eu/dgs/home-affairs/e-library/documents/policies/borders-and-visas/document-security/index_en.htm.

European Commission, "Commission implementing regulation (EU) No 1147/2011 of 11 November 2011 amending Regulation (EU) No 185/2010 implementing the common basic standards on civil aviation security as regards the use of security scanners at EU airport", *Official Journal of the European Union L 294*, Vol. 54, 12.11.2011, pp. 7-11. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:294:0007:0011:EN:PDF

European Commission, "Commission Staff Working Document accompanying the proposal for a Directive of the European Parliament and the Council on aviation

security charges: Impact Assessment", SEC 2009 (615), 2009. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2009:0615:FIN:EN:PDF

European Commission, "Confederation of European Security Services", Transparency Register. http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=61991787780-18

European Commission, "EOS", Transparency Register. http://ec.europa.eu/transparencyregister/public/consultation/displaylobbyist.do?id=32134385519-64

European Commission, "Eurosmart", Transparency Register. https://ec.europa.eu/transparencyregister/public/contact/contact.do?locale=en

European Commission, "Executive Summary of the Impact Assessment accompanying the document Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR)", SEC (2011) 1537 final, Brussels, 2011. http://eur-lex.europa.eu/staging/LexUriServ/LexUriServ.do?uri=SEC:2011:1536:FIN:EN:PDF

European Commission, "Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (EUROSUR)", SEC (2011) 1538 final, Brussels, 2011. http://eur-lex.europa.eu/staging/LexUriServ/LexUriServ.do?uri=SEC:2011:1538:FIN:EN:PDF

European Commission, "Impact Assessment on the possible use of security scanners at EU airports (Draft)", Commission Staff Working Paper, Brussels, Brussels, 2011. http://ec.europa.eu/governance/impact/ia_carried_out/docs/ia_2011/sec_2011_1327_en.pdf

European Commission, "Proposal for a Regulation of the European Parliament and of the Council Establishing the European Border Surveillance System (EUROSUR)", COM (2011) 873 final, Brussels, 2011. http://ec.europa.eu/home-affairs/doc_centre/borders/docs/eurosur final.pdf - zoom=100

European Commission, "Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC)", COM (2011) 225 final, Brussels, 2011. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:EN:PDF

European Commission, "Towards a European strategy for the development of Remotely Piloted Aircraft Systems (RPAS)", Commission Staff Working Document, 6 September 2012, http://register.consilium.europa.eu/pdf/en/12/st13/st13438.en12.pdf

European Commission, DG Home Affairs, "Counter-Terrorism Strategy", last updated 07.12.2011. http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_terrorism/l33275_en.htm

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, 2012.

European Council, "Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security", *Official Journal of the European Union L 215,* Vol. 55, 11.8.2012, pp. 5-14. http://register.consilium.europa.eu/pdf/en/05/st14/st14469-re04.en05.pdf

European Council, “Council Decision of 22 September 2011 on the signing, on behalf of the Union, of the Agreement between the European Union and Australia on the processing and transfer of passenger name record (PNR) data by air carriers to the Australian Customs and Border Protection Service”, *Official Journal of the European Union L186*, Vol. 55, 14.07.2012, pp. 4-15. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:186:0004:0016:EN:PDF

European Council, “Council Decision of 28 June 2010 on the signing, on behalf of the Union, of the Agreement between the European Union and the United States of America on the processing and transfer of financial messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program”, *Official Journal of the European Union L195*, Vol. 53, 27.7.2010, pp. 1-2. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:195:0001:0002:EN:PDF

European Council, “Council Regulation (EC) 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States”, *Official Journal of the European Union L 385*, Vol. 47, 29.12.2004, pp. 1-6.

European Court of Justice, "Judgement of the Court (Third Chamber) of 1 June 2006 in Joined Cases C-442/03 P and C-471/03 P", 2006. http://curia.europa.eu/juris/document/document.jsf?docid=57561&doclang=EN&mode=&part=1

European Parliament and the Council, “Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)", *Official Journal of the European Communities L 201*, Vol. 45, 31 July 2002, pp. 37-47. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:EN:PDF

European Parliament and the Council, “Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC”, *Official Journal of the European Union L 105*, Vol. 49, 15.3.2006, pp. 54-63. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

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

European Parliament, “Resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection”, B6-0562/2008, Strasbourg, 2008. http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P6-TA-2008-521

European Parliament, Commission to the Council and the European Parliament, “Evaluation report on the Data Retention Directive”, (Directive 2006/24/EC), 2011. http://www.statewatch.org/news/2011/apr/eu-com-data-retention-report-225-11.pdf

European Parliament, Committee on Civil Liberties, Justice and Home Affairs, "LIBE Committee Meeting -15:10 / 17:32 - 11-10-2012", 11 October 2012. http://www.europarl.europa.eu/ep-live/en/committees/video?event=20121011-1500-COMMITTEE-LIBE&category=COMMITTEE&format=wmv.

European Parliament, Press release, “Controlling dual-use exports” 4 April 2011. http://www.europarl.europa.eu/pdfs/news/expert/infopress/20110927IPR27586/20110927IPR27586_en.pdf

European Parliament, *Report on the existence of a global system for the interception of private and commercial communications, ECHELON interception system*, (2001/2098(INI)), 2001.

European Parliament, Report to the Directorat General for Research of the European Parliament, (Scientific and Technical Options Assessment programme office), “Interception Capabilities 2000 - PART 1”, 2001.

European Parliament, STOA Unit (ed.), *Development of Surveillance Technology and Risk of Abuse of Economic Information (5 volumes)*, Luxembourg, 1999.

European Transport Safety Council (ETSC), Drink Driving Monitor No. 16, European Transport Safety Council, No. 16, 2012. http://www.etsc.eu/documents/Drink_Driving_Monitor_June_2012.pdf

European Union Agency for Fundamental Rights, “The Use of Body Scanners: 10 Questions and Answers”, Vienna, 2010. http://fra.europa.eu/sites/default/files/fra_uploads/959-FRA_Opinions_Bodyscanners.pdf

European Union, “The prevention of and the fight against terrorist financing through measures to improve the exchange of information, to strengthen transparency and enhance the traceability of financial transactions”, Brussels, 2004.

European Union, Scientific and Technical Options Assessment, “Development of Surveillance Technology and Risk of Abuse of Economic Information”, A Working Document for the S.T.O.A Panel, PE 168.184, Vol. 2/5, Luxembourg, 1999.

European Union, Stratégie révisée de lutte contre le financement du terrorisme, Bruxelles, 11778/1/08, 17 July 2008.

Experian plc, Annual Report 2012. http://www.experianplc.com/~/media/Files/E/Experian-V2/pdf/investor/reports/2012/experian-ar-2012.pdf

Experian, Corporate Social Responsibility Report, 2012. http://crreport.experianplc.com/2012/our_global_performance/how_we_treat_consumers.aspx

Fabio, Michelle, “Is Google a Monopoly?” *LegalZoom*, 13 September 2011. https://www.legalzoom.com/legal-headlines/corporate-lawsuits/is-google-monopoly

FAD, “UK – DENMARK Defence and Security Industry Seminar and Dinner” 14 May 2012. http://fad.di.dk/About%20FAD/Newsandpress/Pages/26%20September%20UK%E2%80%93DK%20Defence%20and%20Securtiy%20Industry%20Seminar.aspx

Fallon, Richard H., *Implementing the Constitution*, Cambridge, Harvard University Press, 2001.

Faure Atger, Anaïs, “The Abolition of Internal Border Checks in an Enlarged Schengen Area: Freedom of movement or a web of scattered security checks?” CHALLENGE Research Papers, No. 8, 2008.

Favarel-Garrigues, Gilles, Thierry Godefroy and Pierre Lascoumes, *Les sentinelles de l’argent sale : les banques aux prises avec l’antiblanchiment*, La Découverte, Paris, 2009.

Favarel-Garrigues, Gilles, Thierry Godefroy and Pierre Lascoumes, “Tools and securitization: the instrumentation of AML/CFT policies in French banks”, in Karin Svedberg Helgesson, and Ulrika Mörth (eds.), *Securitization, accountability and risk management*, PRIO, Routlege, Oslo, 2012, pp. 88-109.

Federal Trade Commission, "FTC Alleges Ads For "Free" Credit Report Violate Federal Court Order", 21 February 2007. http://www.ftc.gov/opa/2007/02/cic.shtm

FEDMA, FEDMA Position Papers. http://www.fedma.org/index.php?id=55

Feeley, Malcom M. and Jonathan, Simon, "The New Penology: Notes on the emerging strategy of corrections and its implications", *Criminology*, Vol. 30, Issue 4, Nov. 1992, pp. 449-474.

Ferguson, Andrew Guthrie, "Predictive Policing and the Future of Reasonable Suspicion", *Emory Law Journal*, May 2012. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2050001

FhG IML, *RACE networkRFID, D2.1 – Market analysis consumption report*, 1 March 2009. http://www.rfidineurope.eu/sites/default/files/RACE_deliverable_D2.1.pdf

Financial Action Task Force (FATF), *Guidance on the risk-based approach to combating money laundering and terrorist financing: High level principles and procedures*, Paris, 2007, http://www.fatf-gafi.org/dataoecd/43/46/38960576.pdf

Finkenzeller, Klaus, *RFID-Handbuch: Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten*, Hanser, München, 2006.

Finmeccanica, *2011 Consolidated Annual Report*. http://www.finmecannica.com

Finn, Rachel, David Wright and Michael Friedewald, "Seven types of privacy", in Serge Gutwirth, Ronald Leenes, Paul De Hert et al. (eds.), European data protection: coming of age?, Springer, Dordrecht, 2013 [forthcoming].

Fisher, Jill, "Indoor Positioning and Digital Management: Emerging Surveillance Regimes in Hospitals", in Torin Monahan (ed.), *Surveillance and Security: Technological Politics and Power of Everyday Life*, Routledge, New York, 2006, pp. 77-88.

Flaherty, David H., "Privacy Impact Assessments: An Essential Tool for Data Protection", in Stephanie Perrin, Heather Black, David H. Flaherty and T. Murray Rankin (eds.), *The Personal Information Protection an Electronic Documents Act: An Annotated Guide*, Irwin Law, Inc. Toronto, 2001.

Fleming, Peter and Graham Sewell, "Looking for the good soldier 'Švejk': Alternative modalities of resistance in the contemporary workplace", *Sociology*, Vol. 36 No. 4, 2002, pp. 857 – 873.

Flint, Colin, *Spaces of Hate: Geographies of Discrimination and Intolerance in the USA*, Routledge, New York, 2004.

Fonio, C., F. Pruno, R. Giglietto, L. Rossi, and S. Pedriol, "Eyes on You: Analyzing User GeneratedContent for Social Science", Paper presented at the Towards a Social Science of Web 2.0 conference, York, UK, May 2007.

Ford, Davion, "Dutch police look to expand spying powers", *Radio Netherlands Worldwide*, 27 December 2011. http://www.rnw.nl/english/video/dutch-police-look-expand-spying-powers

Foucault, Michel, *Discipline and Punish*: *The birth of the prison*, Harmondsworth, Penguin, 1977.

Foucault, Michel, *Dits et écrits II. 1976-1988*, Gallimard, Paris, 2001.

Foucault, Michel, *Naissance de la biopolitique*, Cours au Collège de France. 1978-1979, Hautes études, Gallimard, Seuil, Paris, 2004.

Franklin, Ursula, *The real world of technology*, House of Anansi Press, Toronto, 1999.

Fried, Charles, "Privacy", *Yale Law Journal*, Vol. 77, 1968, pp. 475-493.

Fuchs, Christian, "Implications of Deep Packet Inspection (DPI) Internet Surveillance for Society", Privacy & Security Research Paper #11, PACT Project, Uppsala, 2012.

Fussey, Pete , and Jon Coaffee, “Urban spaces of surveillance”, in Kirstie Ball, Kevin D. Haggerty, and David Lyon (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, London, 2012, pp. 201-208.

Fussey, Pete, “New Labour and New Surveillance: Theoretical and Political Ramifications of CCTV Implementation in the UK”, *Surveillance and Society*, Vol. 2, No. 2/3, 2004, pp. 251-269.

Fyfe, Nicholas R. and Jon Bannister, “City watching: Closed circuit television surveillance in public spaces”, *Area*, Vol. 28, No. 1, 1996, pp. 37-46.

G4S plc, “CSR Checklist”. http://reports.g4s.com/csr/safeguarding-our-integrity/csr-checkllist.html

G4S plc, *Annual Report and Accounts 2011*. http://www.g4s.com/en/Investors/2011%20Annual%20Report/

Galdon Clavell, Gemma, “Local surveillance in a global world: Zooming in on the proliferation of CCTV in Catalonia”, in C. William R. Webster, Eric Töpfer, Francisco R. Klauser, and Charles D. Raab (eds.), *Video Surveillance Practices and Policies in Europe*, IOS Press, Amsterdam, 2012, pp. 17-36.

Galdon Clavell, Gemma, “Local surveillance in a global world: Zooming in on the proliferation of CCTV in Catalonia’, *Information Polity*, Vol. 16, No. 4, 2011, pp. 319-338.

Gallagher, Ryan, “How Governments and Telecom Companies Work Together on Surveillance Laws”, *Future Tense*, 14 August 2012. http://www.slate.com/articles/technology/future_tense/2012/08/how_governments_and_telecom_companies_work_together_on_surveillance_laws_.html

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

Gandy, Oscar, “Data mining, surveillance and discrimination in the post 9/11 environment”, in Haggerty, Kevin and Richard Ericson (eds.), *The new politics of surveillance and visibility*, Toronto, University of Toronto Press, 2006, pp. 363-384.

Gandy, Oscar, “Statistical Surveillance: Remote Sensing in the Digital Age”, in Kirstie Ball, Kevin Haggerty and David Lyon (eds.), *Routledge handbook of surveillance studies*, Routledge, New York, 2012, pp. 125-132.

Gandy, Oscar, *Coming to terms with chance. Engaging rational discrimination and cumulative disadvantage*, Ashgate, Farnham, 2009.

Gandy, Oscar, *Consumer protection in cyber space*, Communication Policy and Technology Section IAMCR, Istanbul, 2011.

Gandy, Oscar, *The Panoptic sort: a political economy of personal information*, Westview, Boulder, 1993.

Gannon, Theresa et al. “The evaluation of the mandatory polygraph pilot”, 2012. http://www.justice.gov.uk/publications/research-and-analysis

Gardner, Stephen, “Military spending dressed up as research”, *EU Observer*, 17 February 2012. http://blogs.euobserver.com/gardner/2012/02/17/military-spending-dressed-up-as-research/

Garfinkel, Simson, *Database Nation: The Death of Privacy in the 21st Century*, O'Reilly, Sebastopol, 2000.

Garson, Barbara, *The electronic sweatshop: How computers are transforming the office of the future into the factory of the past*, Simon & Schuster, New York, 1988.

Gartner, “Gartner Says Monitoring Employee Behavior in Digital Environments is Rising” 29 May 2012. http://www.gartner.com/it/page.jsp?id=2028215

Gatev, Ivaylo, “Border Security and the Eastern Neighbourhood: Where Bio-politics and Geopolitics Meet”, *European Foreign Affairs Review*, No. 13, 2008, pp. 97-116.

Gavison, Ruth, "Privacy and the limits of law", *Yale Law Journal*, Vol. 89, 1980, pp. 421-471.

Gerrard, Graeme, Garry Parkins, Ian Cunningham, Wayne Jones, Samantha Hill, and Sarah Douglas, *National CCTV Strategy*, Home Office, London, 2007.

Geyer, Florian, "Taking Stock: Databases and Systems of Information Exchange in the Area of Freedom, Security and Justice", CHALLENGE Research Paper, No. 9, 2008.

Giddens, Anthony, *The Consequences of Modernity*, Cambridge, Polity Press, 1990.

Gies, S., R. Gainey, M. Cohen E. Healy, D. Duplantier, M. Yeide, A. Bekelman, A. Bobnis and M. Hopps, *Maintaining high risk offenders with GPS technology: An evaluation of the California supervision programme*, National Institute of Justice, Washington, 2012. http://www.ncjrs.gov/profiles1/nij/grants/238481.pdf

Gill, M., and A. Spriggs, "Assessing the impact of CCTV", Great Britain Home Office Research, Development and Statistics Directorate, London, 2005.

Gill, Martin (ed.), *CCTV*, Perpetuity Press, Leicester, 2003.

Gill, Martin and Angela Spriggs, *Assessing the impact of CCTV,* Home Office Research, Developments and Statistics Directorate, London, 2005.

Gilmore, William C., *L'argent sale : L'évolution des mesures internationales de lutte contre le blanchiment des capitaux et le financement du terrorisme*, Editions du Conseil de l'Europe, Strasbourg, 2005.

Glover, Tony, "Spies in the sky spark privacy fears", *The National*, 19 August 2012. http://www.thenational.ae/thenationalconversation/industry-insights/technology/spies-in-the-sky-spark-privacy-fears

Gobry, Pascal-Emmanuel, "REVEALED: Palantir Technologies, The Secretive $735 Million Tech Security Company Helping Hedge Funds And Governments" *Business Insider*, 10 March 2011. http://www.businessinsider.com/palantir-technologies-revealed-2011-3?op=1#ixzz20zmtCJ7v

Goffman, Erving, *Stigma: Notes on the Management of Spoiled Identity*, Penguin Books, Harmondsworth, 1968.

Gonzalez Fuster, Gloria, Paul De Hert and Serge Gutwirth, "SWIFT and the vulnerability of transatlantic data transfers", *International Review of Law Computers & Technology*, Vol. 22, No. 1-2, May 2008, pp. 191-202.

Google Inc, *Transparency Report*. http://www.google.com/transparencyreport/

Google Inc., *Annual Report 2011*. http://sec.gov/Archives/edgar/data/1288776/000119312512025336/d260164d10k.htm

GoogleWatch, "Gmail is too creepy", *Google Watch*, 21 September 2011. http://www.webcitation.org/61rOfd8To

Goold, Benjamin, "CCTV and Human Rights", in European Forum for Urban Security, Roxana Calfa, Sebastian Sperber and Nathalie Bourgeois (eds.), STIBA, Montreuil, 2010, pp. 27-35 at pp. 31-35. http://cctvcharter.eu/fileadmin/efus/CCTV_minisite_fichier/Publication/CCTV_publication_EN.pdf

Goold, Benjamin, "How Much Surveillance is Too Much? Some Thoughts on Surveillance, Democracy, and the Political Value of Privacy", in D. W. Schartum (ed.), *Overvåkning i en rettsstat - Surveillance in a Constitutional Government*, Fagbokforlaget, Bergen, 2010, pp. 38-48.

Goold, Benjamin, "Surveillance and the political value of privacy", *Amsterdam Law Forum*, Vol. 1, No. 4, 2009. http://amsterdamlawforum.org

Gordon Diana R., *Justice Juggernaut: Fighting Street Crime, Controlling Citizens*, Rutgers University Press, New Brunswick, 1990.

Gordon, Paul, James E. Moore, JiYoung Park, and Harry W. Richardson, "The Economic Impacts of a Terrorist Attack on the U.S. Commercial Aviation System", *Risk Analysis*, Vol. 27, No. 3, 2007, pp. 505-512.

Graham, Stephen, "The software-sorted city: Rethinking the digital divide", in Stephen Graham (ed.), *The Cybercities Reader*, New York, 2004.

Graham, Stephen, and David Murakami Wood, "Digitizing surveillance: Categorization, space, inequality", *Critical Social Policy*, Vol. 23, No. 2, 2003, pp. 227-248.

Gras, Marianne L., "The Politics of CCTV in Europe and Beyond, The Legal Regulation of CCTV in Europe", *Surveillance and Society*, Vol. 2, No. 2/3, 2004, pp. 216-229.

Grayson, John, "Britain as a private security state: first they came for the asylum seeker", *OpenDemocracy.net*, 9 March 2012. http://www.opendemocracy.net/ourkingdom/john-grayson/britain-as-private-security-state-first-they-came-for-asylum-seeker

Great Britain Her Majesty's Treasury, *The financial challenge to crime and terrorism*, London, 28 Feb. 2007.

Great Britain Home Office, "DNA Expansion Programme 2000–2005: Reporting achievement", Home Office Forensic Science and Pathology Unit, London, 2006.

Great Britain Home Office, "Introduction to the Centre for Applied Science and Technology", 2011.

Great Britain Ministry of Justice, *It's complicated: The management of electronically monitored curfews: a follow up inspection of electronically monitored curfews*, Her Majesty's Inspector of Probation, Criminal Justice Joint Inspection, (HMIP), 2012. http://www.justice.gov.uk/downloads/publications/inspectorate-reports/hmiprobation/joint-thematic/electronic-monitoring-report-2012.pdf

Great Britain National Audit Office (NAO), *The Electronic Monitoring of Adult Offenders*, Report by the Comptroller and Auditor General, HC 800 Session 2005-2006, National Audit Office, 2006. http://www.nao.org.uk/publications/0506/the_electronic_monitoring_of_a.aspx

Great Britain National Police Improvement Agency (NPIA), CPO ANPR Standards, 2011. at: http://www.acpo.police.uk/documents/crime/2011/201111CBANAAS412.pdf

Great Britain National Police Improvement Agency (NPIA), National DNA Database, Basic Facts, 2012. http://www.npia.police.uk/en/13340.htm

Great Britain National Police Improvement Agency (NPIA), Practice advice on the Managements and use of Automatic Number Plate Recognition, ANPR Issue 6, 2009, pp. 44-49.

Great Britain National Police Improvement Agency, "Automated Facial Recognition: Applications within Law Enforcement", National Police Improvement Agency Report, London, 2006.

Great Britain Serious Organised Crime Agency (SOCA), *The suspicious activity reports regime annual report*, London, 2007.

Greene, Judith A., "Zero Tolerance: A Case Study of Police Policies and Practices in New York City", *Crime & Delinquency*, Vol. 45, no. 2, April 1999, pp. 171-187

Greene, Thomas C., "eBlaster spyware has Achilles heel: Well designed, yet easily defeated", *The Register*, 16 June 2003. http://www.theregister.co.uk/2003/06/16/eblaster_spyware_has_achilles_heel/

Gren, Martin, "Eyeing the future of video surveillance", 23 August 2012. http://technologyspectator.com.au/eyeing-future-video-surveillance (CCTV)

Groenendijk, Kees, Elspeth Guild and Paul Minderhoud (eds.), *In Search of Europe's Borders*, Kluwer Law International, The Hague, 2003.

Groombridge, Nic, "Crime Control or Crime Culture TV?", *Surveillance Studies*, 1(1), 2002, pp. 30-46.

Groombridge, Nic, "Stars of CCTV? How the Home Office wasted millions – a radical 'Treasury/Audit Commission' view'", *Surveillance and Society*, Vol. 5, No. 1, 2008, pp. 73-80.

Groot, Willemien, "Who's afraid of wiretap-friendly social media*?" Radio Netherlands Worldwide*, 11 May 2012. http://www.rnw.nl/english/article/who%E2%80%99s-afraid-wiretap-friendly-social-media

Gros, Frédéric, Monique Castillo and Antoine Garapon, "De la sécurité nationale à la sécurité humaine", *Raisons politiques*, Vol. 4, No. 32, 2008, p.7.

Gros, Frédéric, Monique Castillo and Antoine Garapon, "De la sécurité nationale à la sécurité humaine", *Raisons politiques*, Vol.4, No. 32, 2008, pp. 5-7.

Gross, Grant, "More firms will monitor social media use: Gartner", *IDG News Service*, 29 May 2012. http://www.computerworld.com/s/article/9227556/Gartner_sees_huge_rise_in_corporate_social_media_monitoring

Grother, Patrick, George Quinn and Jonathon Phillips, "Report on the Evaluation of 2D Still-Image Face Recognition Algorithms", NIST Interagency Report 7709, 2010.

Guggerli, David, *Suchmaschinen: Die Welt als Datenbank*, Suhrkamp, Frankfurt am Main, 2009.

Guidance Software Inc, *Form 10-K Annual Report 2011*. http://investors.guidancesoftware.com/secfiling.cfm?filingID=1104659-11-11808

Guild, E., "The Uses and Abuses of Counter-Terrorism Policies in Europe: The Case of the 'Terrorist Lists'", *Journal of Common Market Studies*, Vol. 46, No. 1, February 2008, pp. 173-193.

Guittet, E.-P. and J. Jeandesboz, "Security technologies" in Peter J. Burgess (ed.), *The Routledge Handbook of New Security Studies*, Routledge, New York, 2010, pp. 229-239.

Gutwirth, Serge and Mireille Hildebrandt, "Some Caveats on Profiling", in Serge Gutwirth, Yves Poullet and Paul De Hert (eds.), *Data Protection in a Profiled World*, Dordrecht, Springer, 2010.

Gutwirth, Serge, *Privacy and the Information Age*, Rowman and Littlefield, Lanham, MD, 2002.

Gutwirth, Serge, Rocco Bellanova, Michael Friedewald et al., *Smart Surveillance - State of the Art Report, Deliverable 1, SAPIENT Project*, 2012. http://www.sapientproject.eu/docs/D1.1-State-of-the-Art-submitted-21-January-2012.pdf

Guzik, Keith, "Discrimination by Design: predictive data mining as security practice in the United States' 'war on terrorism'", *Surveillance and society*, Vol. 7, No. 1, 2009, pp. 1-17.

Hacking, Ian, "A Tradition of Natural Kinds", *Philosophical Studies*, Volume 61, No. 1-2 1991, pp. 109-126.

Hadjiyanni, Tasoulla and Jain Kwon, J., "The Social Dimension of Security: Exploring How Surveillance Systems Relate to Interior Design", *Journal of Interior Design*, Vol. 34, No. 3, 2009, pp. 1-15.

Haggerty, Kevin and Maryam Razavy, "Hawala under Scrutiny: Documentation, Surveillance and Trust", *International Political Sociology*, Vol. 3, No. 2, 2009, pp. 139-155.

Haggerty, Kevin and Minas Samatas (eds.), *Surveillance and Democracy*, Routledge, New York, 2010.

Haggerty, Kevin and Richard Ericson (eds.), *The new politics of surveillance and visibility*, University of Toronto Press, Toronto, 2006.

Haggerty, Kevin D., and Richard V. Ericson, "The surveillant assemblage", *British Journal of Sociology*, Vol. 51, No. 4, 2000, pp. 605–622.

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

Haines, A. and H. Wells, "Persecution or protection? Understanding the differential public response to two road-based surveillance systems", *Criminology and Criminal Justice*, Vol. 12, 2012, p. 257.

Hamacher, Kay and Stefan Katzenbeisser, "Public Security: Simulations need to replace conventional wisdom", in Proceedings of the New Security Paradigms Workshop (NSPW11), ISBN 978-1-4503-1078-9, ACM, 2011, pp. 115-124.

Harbo, Tor-Inge, "The Function of the Proportionality Principle in EU Law", *European Law Journal*, Vol. 16, No. 2, March 2010, pp. 158–185.

Harris, John, "School surveillance: how big brother spies on pupils", *The Guardian*, 9 June 2011. http://www.guardian.co.uk/uk/2011/jun/09/schools-surveillance-spying-on-pupils

Harrop, Dr Peter, and Raghu Das, "RFID Forecasts, Players and Opportunities 2012-2022", June 2012. http://www.idtechex.com/research/reports/rfid-forecasts-players-and-opportunities-2012-2022-000322.asp

Hart, Herbert L. A., "The Ascription of Responsibility and Rights", in Anthony Flew (ed.), *Essays on Logic and Language*, Oxford University Press, Oxford, 1949, pp. 145-166.

Hastings, G.W., *Address on the Repression of Crime*, Spottiswoode and Co., London, 1875.

Hayes, Ben and Gavin Sullivan, *Blacklisted: Targeted sanctions, preemptive security and fundamental rights*, ECCHR: 10 years after 9/11 Publication Series, 2010.

Hayes, Ben and Mathias Vermeulen, "Borderline: The EU's New Border Surveillance Initiatives: Assessing the Costs and Fundamental Rights Implications of EUROSUR and the "Smart Borders" Proposals", Heinrich Böll Stiftung, Berlin and Brussels, 2012. http://www.statewatch.org/news/2012/jun/borderline.pdf

Hayes, Ben, "CLEAN IT: the secret EU surveillance plan that wasn't," OpenDemocracy, 9 October 2012. http://www.opendemocracy.net/ben-hayes/clean-it-secret-eu-surveillance-plan-that-wasn%E2%80%99t

Hayes, Ben, "NeoConOpticon: The EU Security-Industrial Complex", TNI/Statewatch, 2009. www.statewatch.org/analyses/neoconopticon-report.pdf

Hayes, Ben, and Gavin Sullivan, *Blacklisted: Targeted sanctions, preemptive security and fundamental rights*, ECCHR: 10 years after 9/11 Publication Series, 2010.

Hayes, Ben, *Arming Big Brother. The EU's Security Research Programme*, TNI, Amsterdam, 2006. http://www.statewatch.org/analyses/bigbrother.pdf

Heide, Lars, "Monitoring People: Dynamics and Hazards of Record Management in France, 1935-1944", *Technology and Culture*, Vol. 45, No. 1, 2004, pp. 80-101.

Heide, Lars, "Shaping a Technology: American Punched Card Systems 1880-1914"", *IEEE Annals of the History of Computing*, Vol. 19, No. 4, 1997, pp. 28-41.

Heilmann, Eric, "Video Surveillance and security policy in France: From regulation to widespread acceptance", in C. William R. Webster, Eric Töpfer, Francisco R.

Klauser, and Charles D. Raab (eds.), *Video Surveillance Practices and Policies in Europe*, IOS Press, Amsterdam, 2012, pp. 94-102.
Heilprin, John, "World Trade Organization: Boeing got $5.3 billion in illegal subsidies", *The Post and Courier*, 13 March 2012. http://www.postandcourier.com/article/20120313/PC04/303139905/1012/world-trade-organization-boeing-got-53-billion-in-illegal-subsidies
Helten, Frank and Bernd Fischer, "Reactive attention: Video surveillance in Berlin shopping malls", *Surveillance & Society*, Vol. 2, 2004, pp. 323-345.
Hempel, L. and E. Töpfer, *Urban Eye: Final Report to the European Commission*, 5th FP Urban Eye project, Technical University of Berlin, Berlin, 2004. http://www.urbaneye.net/results/ue_wp15.pdf
Hempel, Leon, and Eric Töpfer, "Urban Eye: Inception Report to the European Commission", Working Paper, Technical University Berlin, Berlin, 2002.
Heng, Yee-Kuang and Kenneth McDonagh, *Risk, Global Governance and Security: The Other War on Terror*, Routledge, New York, 2009.
Henry Gates and Son Ltd, "Mobile CCTV proving success in Bournemouth," Blogpost, 4 May 2012. http://www.hg-security-systems.co.uk/blog/mobile-cctv-proving-success-in-bournemouth/
Henry Gates and Son Ltd, "Successful CCTV Camera in Cheltenham Capturing 50 Arrests a Month", 13 July 2012. http://www.hg-security-systems.co.uk/blog/successful-cctv-camera-in-cheltenham-capturing-50-arrests-a-month/
Hermitte, Marie-Angèle, "La traçabilité des personnes et des choses. Précaution, pouvoirs et maîtrise", in Philippe Pedro (ed.), *Traçabilité et responsabilité*, Economica, Paris, 2003, pp. 1-44.
Hernanz, Nicholas, and Sergio Carrera, "More Surveillance, More Security? The Landscape of Surveillance in Europe and Challenges to Data Protection and Privacy – Policy Report on the Proceedings of a Conference at the European Parliament", Deliverable 6.4, SAPIENT Project, 2012. http://www.sapientproject.eu/docs/D6.4-Policy-Brief-submitted-January-2012-29.pdf
Hesseldahl, Arik, "Palantir's $2.5 Billion Mystery, Solved" AllthingsD.com, 7 October 2011. http://allthingsd.com/20111007/palantirs-mysterious-investors-have-been-found/
Hildebrandt, Mireille, "Defining Profiling", in Mireille Hildebrandt, and Serge Gutwirth (eds.), *Profiling the European Citizen: Cross-Disciplinary Perspectives*, Springer, Dordrecht, 2008, pp. 17-46.
Hildebrandt, Mireille, "Profiling and the Rule of Law", *Identity in the Information Society*, Vol. 1, No. 1, 2008.
Ho Park Hyeon, Gyeong Seok Oh and Seung Yeop Paek, "Measuring the crime displacement and diffusion of benefit effects of open-street CCTV in South Korea", *International Journal of Law, Crime and Justice*, 40, 2012, pp. 179-191.
Hohn, Hans-Willy, *Kognitive Strukturen und Steuerungsprobleme der Forschung: Kernphysik und Informatik im Vergleich*, Campus, Frankfurt und New York, 1998.
Home Office, "Identity cards are to be scrapped" 27 May 2010. http://www.homeoffice.gov.uk/media-centre/news/identity-cards-scrapped
Home Office, "Surveillance camera commissioner appointed" Press release, 13 September 2012. http://www.homeoffice.gov.uk/media-centre/press-releases/surv-cam-comm-appt
Home Office, Communications data. http://www.homeoffice.gov.uk/counter-terrorism/communications-data/

Homeland Security Research Corporation, *CCTV Based Remote Biometric & Behavioral Suspect Detection: Technologies & Global Markets – 2011-2016*. http://www.homelandsecurityresearch.com/2011/02/cctv-based-remote-biometric-behavioral-suspect-detection-market-2011-2016/

Homeland Security Research Corporation, *Global Standoff Terrorist Detection Technologies & Markets – 2010-2014,* March 2010. http://www.homelandsecurityresearch.com/2010/03/global-standoff-terrorist-detection-technologies-markets-2010-2014/.

Homeland Security Research Corporation, *X-Ray Security Screening: Technologies & Global Market Outlook – 2012 Edition,* http://www.homelandsecurityresearch.com/2012/05/x-ray-security-screening-technologies-global-market-outlook-2012-edition/

Hønneland, Gerd, "Compliance in the Barents Sea fisheries: How fishermen account for conformity with rules," *Marine Policy*, Vol. 24, 2000, pp. 11–19.

Hood, Christopher, Henry Rothstein and Robert Baldwin, *The Government of Risk: Understanding Risk Regulation Regimes*, Oxford University Press, Oxford, 2001.

Hope, A. "CCTV, school surveillance and social control," *British Educational Research Journal*, Vol. 35, 6, 2009, pp. 891-907.

Hornung, Gerrit, "Privacy by Design in Europe: Seizing the Opportunity of the Reform of the Data Protection Directive", *Innovation: The European Journal of Social Science Research*, Vol. 25, Nos. 3-4, 2012.

House of Commons Culture, Media and Sport Committee, *News International and Phone-hacking, Eleventh Report of Session 2010-12*, Volume 1, HC 903-I, House of Commons, 30 April 2012. http://www.publications.parliament.uk/pa/cm201012/cmselect/cmcumeds/903/903i.pdf

House of Commons Justice Committee's report on Protection of Private Data. Report of the House of Commons Home Affairs Committee on A Surveillance Society? 215th Report (2007-08): A Surveillance Society? (HC 58).

House of Lords Constitution Committee, Surveillance Citizens and the State, 2nd Report of Session 2008-09, HL Paper 18-I, 2008. http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1804.htm#a16

Howard, Robert, *Brave new workplace*, Viking, New York, 1985. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf .

http://www.technologyreview.com/news/407976/better-face-recognition-software/

Human Genetic Commission (HGC), *Nothing to Hide Nothing to Fear*, London, 2009.

Hurley D.J., B. Abab-Zawarand and M. S. Nixon, "The Ear as a Biometric", in Anil Jain, Pat Flynn and Arun A. Ross (eds.), *Handbook of Biometrics,* Springer, 2007.

Huster, Stefan, and Karsten Rudolph (eds.), *Vom Rechtsstaat zum Präventionsstaat*, Suhrkamp, Frankfurt am Main, 2008.

Hustinx, Peter, "Privacy by design: delivering the promises", *Identity in the Information Society*, Vol. 3, 2010, pp. 253–255.

Hutter, Bridget M., and Joan O'Mahoney, "The Role of Civil Society Organisations in Regulating Business," Discussion Paper, ESRC Centre for Analysis of Risk and Regulation, 26 September 2004.

Huysmans, Jef, *The politics of insecurity: fear, migration and asylum in the EU*, Routledge, London, 2006.

ICMA, “Global Card Market Reaches $17 Billion in 2011, Up Nearly 14% From 2010”, Smart Card Trends, 22 June 2012. http://www.smartcardstrends.com/det_atc.php?idu=16779

IMS Research, “For IP-based Video Surveillance, the Future is Now”, Press release, 12 June 2012. http://imsresearch.com/press-release/For_IPbased_Video_Surveillance_the_Future_is_Now

Info4Security, “HD CCTV technology risks breaching human rights”, *Info4Security*, 4 October 2012. http://www.info4security.com/story.asp?storycode=4129624

Infonetics Research, “Deep packet inspection (DPI) market a $2 billion opportunity by 2016”, 23 April 2012. http://www.infonetics.com/pr/2012/2H11-Service-Provider-DPI-Products-Market-Highlights.asp

Information Commissioner’s Office, “CCTV”. http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/cctv.aspx

Information Commissioner’s Office, “Guidance on the rules on use of cookies and similar technologies”, May 2012, V.3. http://bit.ly/MCjint

Information Commissioner’s Office, “ICO Disclosure Log Response to Request, Reference: IRQ0408803, 26 August 2011. http://www.ico.gov.uk/about_us/how_we_comply/disclosure_log/~/media/documents/disclosure_log/IRQ0408803.ashx.

Information Commissioner’s Office, *Information Commissioner’s report to Parliament on the state of surveillance,* November 2010.

Information Commissionser’s Office, “CCTV Code of Practice”, Revised edition, Information Commissioner’s Office, Wilmslow, 2008.

Innes, E., “FP identification - opinion or fact?” 2005. www.shirleymckie.com/documents/InnesopinionNov2005.rtf.pdf

Intellect, “Intellect Data Security and Data Protection Guidelines for Offshoring and Outsourcing”, 2008. http://www.intellectuk.org/publications/business-guidance/4055

Intellect, “Marketing under the privacy and electronic communications regulations 2003”,2001. http://www.intellectuk.org/publications/business-guidance/4407.

Intelligence Services Commissioner, *2011 Annual report*, Presented to Parliament pursuant to section 60(4) of the Regulation of Investigatory Powers Act 2000.

Interpol, *Interpol Handbook on DNA data exchange and practice*, Interpol, Lyon, 2009.

Introna, Lucas and David Wood, “Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems”, *Surveillance & Society*, Vol. 2, (2/3), 2004, pp. 177-198.

ITT Excelis, “Sierra Nevada Corporation and ITT Exelis Partner to Build Advanced Wide-Area Airborne Persistent Surveillance System” 8 July 2012. http://www.exelisinc.com/news/pressreleases/Pages/Sierra-Nevada-Corporation-and-ITT-Exelis-Partner-to-Build-Advanced-.aspx

Jackson, P. G. and C. J. Hilditch, *A review of evidence related to Drug Driving in the UK: a report submitted to the North Review Team, Department for Transport*, London, 2010. http://www.roadsafety.am/publication/pub_int/NorthReview-ReviewofEvidence.pdf

Jacobson, Bob, “Google and CIA Invest in a Minority Report-Like Technology That May Make Our World a Less Certain Place”, *Huffington Post*, 30 July 2010. http://www.huffingtonpost.com/bob-jacobson/google-and-cia-invest-in_b_664525.html

Jain, Anil K., Arun Ross, and Salil Prabhakar, “An Introduction to Biometric Recognition”, *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 14, No. 1, 2004, pp. 4-20.

Jeandesboz, Julien, “Logiques et pratiques de contrôle et de surveillance des frontières de l’Union européenne”, in Amandine Scherrer, Emmanuel-Pierre Guittet and Didier Bigo (eds.), *Mobilité(s) sous surveillance: Perspectives croisées UE-Canada*, Athéna, Montréal, 2010.

Jeandesboz, Julien, and Francesco Ragazzi, “Review of security measures in the Research Framework Programme”, Study PE 432.740, European Parliament, Directorate - General for Internal Policies, Policy Department C "Citizen's Rights and Constitutional Affairs", Strasbourg, 2010.
http://www.europarl.europa.eu/committees/de/libe/studiesdownload.html?languageDocument=EN&file=32851

Jeandesboz, Julien, Bigo, Didier, Bonditti, Philippe and Francesco Ragazzi, *Security technologies and society: A state of the art on security, technology, borders and mobility*, INEX Deliverable D.1.1, PRIO, Oslo, 2008.

Jones, A. W., *The relationship between blood alcohol concentration (BAC) and breath alcohol concentration: a review of the evidence*, Department for Transport, London, 2010.

Jørgensen, Magne, and Kjetil Moløkken-Østvold, “How large are software cost overruns? A review of the 1994 CHAOS report”, *Information and Software Technology*, Vol. 48, No. 2, pp. 297-301.

Jowitt, Tom, “BA Hits Privacy Turbulence Over Passenger Profiling” *TechWeekEurope*, 6 July 2012. http://www.techweekeurope.co.uk/news/ba-privacy-passenger-profiling-85310

Kaiser, Walter, "Technisierung des Lebens seit 1945", in Wolfgang König (ed.), *Propyläen Technikgeschichte Bd. 5. Energiewirtschaft, Automatisierung, Information*, Propyläen Verlag, Berlin, 1992, pp. 281-529.

Kallinikos, Yiannis, “The social foundations of the bureaucratic order”, *Organization*, Vol. 11 No. 1, 2004, pp. 13- 36.

Keizer, Gregg, “Ad industry calls IE10's 'Do Not Track' setting 'unacceptable'”, *PC Advisor*, 4 October 2012. http://www.pcadvisor.co.uk/news/security/3402037/ad-industry-calls-ie10s-do-not-track-setting-unacceptable/#ixzz28Va1VEkX

Keller, Ska , and Barbara Unmüßig, “Preface”, in Ben Hayes, and Mathias Vermeulen (eds.), *Borderline: The EU’s New Border Surveillance Initiatives: Assessing the Costs and Fundamental Rights Implications of EUROSUR and the “Smart Borders” Proposals*, Heinrich Böll Stiftung, Berlin and Brussels, 2012, pp. 4. http://www.statewatch.org/news/2012/jun/borderline.pdf

Kelley, Tina, “New Jersey Sues to Force 3 Companies to Clean Up Chromium Pollution at 106 sites," *New York Times*, 4 May 2005.
http://www.nytimes.com/2005/05/04/nyregion/04contaminate.html

Kern, Christian, *Anwendungen von RFID-Systemen*, Springer, Berlin, Heidelberg, 2007.

Kierkegaard, S., “US War on Terror SWIFT(ly) signs blank cheque on EU data”, *Computer Law & Security Review*, Vol. 27, No. 5, June 2011, pp. 451-454.

King, Eric “Selling arms and snooping technology is no way to help democracy, Cameron,” *The Guardian*, 11 April 2012.
http://www.guardian.co.uk/commentisfree/2012/apr/11/selling-arms-cameron

King, Eric, “Surveillance companies: real responsibility goes beyond the letter of the law”, Privacy International, 6 August 2012.

https://www.privacyinternational.org/blog/surveillance-companies-real-responsibility-goes-beyond-the-letter-of-the-law

King, J., D. Mulligan, S. Raphael, "Citris Report: The San Francisco Community Safety Camera Program", Berkeley School of Law, California, 2008. http://www.citrisuc.org/files/CITRIS%20SF%20CSC%20Study%20Final%20Dec%202008.pdf

Kleinz, Torsten, "CCC publishes fingerprints of German Home Secretary", Heise Online, 31 March 2008. http://www.h-online.com/newsticker/news/item/CCC-publishes-fingerprints-of-German-Home-Secretary-734713.html

Klinger, David A., "Negotiating Order in Patrol Work: An ecological Theory of Police Response to Deviance", *Criminology*, Vol. 35, Issue 2, May 1997, pp. 277-306.

König, Wolfgang, "Das Problem der Periodisierung und die Technikgeschichte", *Technikgeschichte*, Vol. 57, No. 4, 1990, pp. 285-298.

Koskela, Hille, "Video surveillance, gender, and the safety of public urban space: 'Peeping Tom' goes high tech?", *Urban Geography*, Vol. 23, 2002, pp. 257-278.

Kreissl, Reinhard and Lars Ostermeier, "Globale Trends und lokale Differenzen – Kulturen der Kontrolle und politische Steuerung in Hamburg und München", *Kriminologisches Journal*, Beiheft 9, 2007, pp. 137-151.

Krigsman, Michael, "Google Plus: Is privacy an issue?" *ZDNetNews*, 11 July 2011. http://www.zdnet.com/blog/projectfailures/google-plus-is-privacy-an-issue/13749

Kroener, I. and D. Neyland, "New Technologies, security and surveillance", in Kirstie Ball, Kevin Haggerty and David Lyon (eds.), *Routledge handbook of surveillance studies*, Routledge, New York, 2012, pp. 141-148.

Kuner, Christopher, "The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law", Privacy and Security Law Report, 6 February 2012, pp. 1-15.

Kurz, Constanze, and Frank Rieger, *Die Datenfresser: Wie Internetfirmen und Staat sich unsere persönlichen Daten einverleiben und wie wir die Kontrolle darüber zurückerlangen*, S. Fischer, Frankfurt am Main, 2011.

Lagoutte, S., H-O Sano & P. Scharff Smith, "Human Rights in Turmoil: Facing Threats, Consolidating Achievements" in Lagoutte, S., H-O. Sano & P. Scharff Smith (eds.), *Human Rights in Turmoil*, Koninklijke, Netherlands, pp. 1-6.

Lang, Melanie, "Surveillance and conformity in competitive youth swimming", *Sport, Education and Society*, Vol. 15, No. 1, 2010, pp. 19 – 37.

Larner, Wendy, "Spatial imaginaries: economic globalization and the war on terror", in Louise Amoore and Marieke De Goede (eds.), *Risk and the War on Terror*, Routledge, London, 2008.

Larson, James R. and Christine Callahan, "Performance monitoring: How it affects work productivity", *Journal of Applied Psychology*, Vol. 75, No. 5, 1990, pp. 530 – 538.

Lascoumes, Pierre and Patrick Legalès (eds.), *Gouverner par les instruments*, Presses de Sciences Po, Paris, 2005.

Lascoumes, Pierre, and Patrick Legalès, "Introduction: Understanding public policy through its instruments: From the nature of instruments to the sociology of public policy intrsumentation", *Governance*, No. 20, January 2007, pp. 1-22.

Lauer, Josh, "Surveillance history and the history of new media: An evidential paradigm", *New Media & Society*, Vol. 14, No. 4, 2012, pp. 566-582.

Lessig, Lawrence, *Code and Other Laws of Cyberspace*, Basic Books, New York, 1999.

Lettice, John, "Killing ID cards and the NIR - the Tory and LibDem plans", *The Register*, 9 July 2009. http://www.theregister.co.uk/2009/07/09/id_cards_nir_tory_lib_plans/

Levi, Michael and David Wall, "Technologies, Security, and Privacy in the Post-9/11 European Information Society", *Journal of Law and Society*, Vol. 31, No. 2, May 2004, pp. 194-220.

Levi, Michael, "Combating the Financing of Terrorism. A history and Assessment of the Control of 'Threat Finance'", *British Journal of Criminology*, Vol. 50, No.4, Winter 2010, pp. 650-669.

Levi, Michael, and David S. Wall, "Crime and Security in the Aftermath of September 11: Security, privacy and law enforcement issues relating to emerging information and communication technologies", in Ioannis Maghiros (ed.), *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*, Office for Official Publications of the European Communities, Luxembourg, 2003, pp. 163-185. http://ftp.jrc.es/pub/EURdoc/eur20823en.pdf

Lianos, Michaelis and Mary Douglas, "Dangerization and the End of Deviance. The Institutional Environment", *British Journal of Criminology*, Vol. 40, No. 2, 2000, pp. 261-278.

Liberty, Liberty's Response to the Home Office Consultation on a Code of Practice relating to Surveillance Cameras, May 2011. http://www.liberty-human-rights.org.uk/pdfs/policy11/liberty-s-response-to-the-consultation-on-a-code-of-practice-relating-to-sur.pdf

Lindner, Rudolf, Bertram Wohak, and Holger Zeltwanger, *Planen, Entscheiden, Herrschen: Vom Rechnen zur elektronischen Datenverarbeitung*, Rowohlt, Reinbek bei Hamburg, 1984.

Lindsay, David, "An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law", *Melbourne University Law Review*, Vol. 29, 2005, pp. 1-45 (online). http://www.austlii.edu.au/au/journals/MULR/2005/4.html.

Link, Jürgen, "From the 'Power of the Norm' to 'Flexible Normalism': Considerations after Foucault", *Cultural Critique*, No. 57, Spring 2004, pp. 14-32.

Lipartito, Kenneth, "The Economy of Surveillance", 10 February 2010. http://ssrn.com/abstract=1582218 or http://dx.doi.org/10.2139/ssrn.1582218

Lobo-Guerrero, L., "'Pirates', stewards, and the securitization of global circulation", *International Political Sociology*, Vol. 2, No. 3, September 2008, pp. 219-235.

Lomell, Heidi Mork, "Targeting the Unwanted: Video Surveillance and Categorical Exclusion in Oslo, Norway?" *Surveillance & Society*,Vol. 2, Nos 2-3, 2004, pp. 347-361.

London Economics, "Study on the economic benefits of privacy enhancing technologies (PETs)", Final Report to the European Commission DG Justice, Freedom and Security, London, 2010.

Lord, Steve, "Aviation Security: TSA Is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to This Effort and Other Areas of Aviation Security Remain", Testimony before the Subcmmittee on Transportation Security and Instructure Protection, Committee o Homeland Security, House of Represenattvies GAO-10-484T, U.S. Government Accountability Office, Washington, D.C., 2010. http://www.gao.gov/assets/130/124207.pdf

Los, Maria, "Post-communist fear of crime and the commercialization of security", *Theoretical Criminology* Vol. 6, No. 2, 2002.

Luebke, David Martin, and Sybil Milton, "Locating the Victim: An Overview of Census-Taking, Tabulation Technology, and Persecution in Nazi Germany", *IEEE Annals of the History of Computing*, Vol. 16, No. 3, 1994, pp. 25-39.

Luhmann, Niklas, *Soziologie des Risikos*, de Gruyter, Berlin, 2003.

Luif, Paul, “The Treaty of Prüm: A Replay of Schengen”, Deliverable 38c, EU-CONSENT Network of Excellence, 2007. http://www.eu-consent.net/click_download.asp?contentid=1400
Lum, C., l. Merola, J. Willisand B. Cave, “License Plate Recognition Technology, (LPR) Impact Evaluation and Community Assessment”, Center for Evidence-Based Crime Policy, George Mason University, 2010.
Lyon, D., “Liquid Surveillance: The Contribution of Zygmunt Bauman to Surveillance Studies”, *International Political Sociology*, Vol. 4, 2010, pp. 325-338.
Lyon, David (ed.), *Surveillance as social sorting: Privacy, risk and digital discrimination*, Routledge, London, 2003.
Lyon, David, “9/11, Synopticon, and Scopophilia: Watching and Being Watched”, in Kevin D. Haggerty, and Richard V. Ericson (eds.), *The New Politics of Surveillance and Visibility*, Toronto, University of Toronto Press, 2006, pp. 35-54.
Lyon, David, “Airports as data filters: Converging surveillance systems after September 11th”, *Journal of Information, Communication and Ethics in Society*, Vol. 1, No. 1, 2003, pp. 13-20.
Lyon, David, “Everyday Surveillance: Personal data and social classifications”, *Information, Communication & Society*, Vol. 5, No. 2, 2002, pp. 242-257.
Lyon, David, “Globalizing Surveillance”, *International Sociology*, Vol. 19, No. 2, 2004, pp. 135-1349.
Lyon, David, “National ID Cards: Crime-Control, Citizenship and Social Sorting”, Policing, Vol. 1, No. 1, 2007, pp. 111-118.
Lyon, David, “Surveillance Technology and Surveillance in Modernity and Technology”, in Thomas Misa, Philip Brey and Andrew Feenberg (eds.) *Modernity and Technology*, The MIT Press, Cambridge, MA, and London, 2003.
Lyon, David, “Why where you are matter: Mundane mobilities, technologies and digital discrimination”, in Torin Monahan (ed.), *Surveillance and security: Technological power and politics in everyday life*, Routledge, New York, 2006, pp. 209-224.
Lyon, David, Stephen Marmura, and Pasha Peroff, “Location Technologies: Mobility, surveillance and privacy”, A report to the Office of the Privacy Commissioner of Canada, 2005.
Lyon, David, *Surveillance after September 11*, Polity Press, Cambridge, 2003.
Lyon, David, *Surveillance as Social Sorting. Privacy, Risk and Digital Discrimination*, Routledge, London, 2003.
Lyon, David, *Surveillance society. Monitoring everyday life*, Open University Press, Buckingham, 2001.
Lyon, David, *Surveillance Studies: An Overview*, Polity Press, Cambridge, 2008.
Lyon, David, *The Electronic Eye. The Rise of Surveillance Society*, Polity Press, Cambridge, 1994.
Lyon, David. “Airport as data-filters: Converging surveillance systems after September 11th”, The *Journal of Information, Communication and Ethics in Society*, Vol. 1, No. 1, 2002, pp. 13-20.
Machado, Helen and Barbara Prainsack, Tracing *Technologies. Prisoners’ Views in the Era of CSI*, Ashgate, Farnham, 2012.
Macintyre, Donald, “Government asked: Why are you allowing 'tainted' G4S to handle Olympic security?” *The Independent*, 8 June 2012. http://www.independent.co.uk/news/uk/politics/government-asked-why-are-you-allowing-tainted-g4s-to-handle-olympic-security-7827988.html
MacKenzie, Donald and Judy Wajcman, “Introductory essay: the social shaping of technology”, in Donald MacKenzie and Judy Wacjman (eds.), *The Social Shaping of*

Technology: How the refrigerator got its hum, Open University Press, Milton Keynes, 1985, pp. 2-25.

Mackenzie, James, "Finmeccanica sold radio equipment to Syria: report", *Reuters*, 5 July 2012. http://www.reuters.com/article/2012/07/05/us-finmeccanica-syria-idUSBRE86410R20120705

Mackenzie, Simon and Niall Hamilton-Smith, "Measuring police impact on organised crime: Performance management and harm reduction", *Policing: An International Journal of Police Strategies & Management*, Vol. 34, Iss. 1, 2011, pp. 7-30.

Madanipour, Ali. (2003). "Social Exclusion and Space", in Richard T. LeGates and Frederic Stout (eds.), *City Reader*, Routledge, New York, 2003, pp. 181-188.

Maghiros, Ioannis, Laurent Beslay, Clara Centeno, Yes Punie, Carlos Rodríguez, Marcelo Masera, Paul de Hert, Serge Gutwirth, Michael Levi, and David S. Wall, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*, Office for Official Publications of the European Communities, Luxembourg, 2003.

Maimbo, Samuel Munzele and Nikos Passas, "The design, development, and implementation of regulatory and supervisory frameworks for informal funds transfer systems", in Thomas Bierstecker and Sue Eckert Sue (eds.), *Countering the Financing of Terrorism*, Routledge, New York, 2008, pp. 179-182.

Major, Marty, "Online Surveillance Market 2011" 6 March 2011. http://ipvm.com/report/online_surveillance_sales_2011

Makaremi, Christopher, "Pénalisation de la circulation et reconfigurations de la frontière: le maintien des étrangers en 'zone d'attente'", *Cultures & Conflits*, No. 71, 2008, pp. 55-74.

Marketsandmarkets.com, Global *Biometrics Technology Market (2010-2015) – Market forecast by Products, End-User Application and Geography,* Report Code: SE 1302, January 2011. http://www.marketsandmarkets.com/Market-Reports/biometric-market-278.html

Marketsandmarkets.com, *Global Chipless RFID Market (2011 - 2016) - Forecasts by Products (Tag, Reader, Middleware), Applications (Retail, Supply Chain, Aviation, Healthcare, Smart Card, Public Transit),* July 2012. http://www.marketsandmarkets.com/Market-Reports/chipless-rfid-market-forecasts-793.html

Marketsandmarkets.com, *Global Smart Homes Market (2010 – 2015),* Report Code: SE 1084, April 2011. http://www.marketsandmarkets.com/Market-Reports/smart-homes-and-assisted-living-advanced-technologie-and-global-market-121.html.

Marketsandmarkets.com, *Global Touchless Sensing and Gesture Recognition Market (2010-2015),* Report Code 1584, June 2011. http://www.marketsandmarkets.com/Market-Reports/touchless-sensing-gesturing-market-369.html

Marketsandmarkets.com, *Next Generation Biometric Technologies Market – Global Forecast & Analysis (2012 – 2017),* Report Code: SE 1161, June 2012. http://www.marketsandmarkets.com/Market-Reports/next-generation-biometric-technologies-market-697.html

Marketsandmarkets.com, *Unmanned Aerial Vehicles (UAV) Market - Global Forecasts, Trends and Geographical Analysis (2012 – 2017),* November 2012. http://www.marketsandmarkets.com/Market-Reports/unmanned-aerial-vehicles-uav-market-662.html

Marklund, F. and S. Holmberg, "Effects of early release from prison using electronic tagging in Sweden", *Journal of Experimental Criminology*, Vol 5, No. 1, 2009, pp. 41–61.

Markula, Pirkko H, "Firm but shapely, fit but sexy, strong but thin: the postmodern aerobicising female bodies", *Sociology of Sport Journal*, Vol. 12, No. 4, 1995, pp. 424 – 453.

Marques, P. and S. McKnight, *Evaluating Transdermal Alcohol Measuring Devices,* Washington, National Highway Traffic Safety Administration, Washingon, 2007.

Marques, P., R. Voas and A. Tippetts, "Behavioral measures of drinking: Patterns in the interlock record", *Addiction*, Vol. 98, 2003, pp. 13-19.

Marx, Gary and Valerie Steeves, "From the Beginning: Children as Subjects and Agents of Surveillance", *Surveillance & Society*, Vol. 7, Nos. 3-4, 2010, pp. 192-230.

Marx, Gary T., "La societé de Securité Maximale", *Déviance et Societé*, Vol. 12, No. 2, 1988, pp. 147-166.

Marx, Gary T., "Seeing Hazily, But Not Darkly, Through the Lens: Some Recent Empirical Studies of Surveillance Technologies", *Law and Social Inquiry*, Vol. 30, No. 2, Spring 2005.

Marx, Gary T., "What's New About the "New Surveillance"? Classifying for Change and Continuity", *Surveillance & Society*, Vol. 1, No. 1, 2002, pp. 9-29.

Marx, Gary T., *Undercover: Police Surveillance in America*, University of California Press, Berkeley, 1988.

Mathiesen, Thomas, "The viewer society: Michel Foucault's panopticon revisited", *Theoretical criminology*, Vol. 1, No. 2, 1997, pp. 215-234.

Mattera, Phil, "Honeywell International", Crocodyl.org, 27 March 2010. http://www.crocodyl.org/wiki/honeywell_international.

Mattera, Phil, "Northrop Grumman", 27 March 2010. http://www.crocodyl.org/wiki/northrop_grumman

Mayer Jacob P., *Max Weber and German Politics: A Study in Political Sociology* Faber and Faber, 1944.

Mayer-Schönberger, Viktor, "Generational Development of Data Protection in Europe", in Philip E. Agre, and Marc Rotenberg (eds.), *Technology and privacy: The new landscape*, MIT Press, Cambridge, Mass., 1997, pp. 219-241.

McCahill, M., *The Surveillance Web: The Rise of Visual Surveillance in an English City*., Willan, Devon, 2002.

McCahill, Michael and Clive Norris, "Watching the workers: Crime, CCTV and the workplace" in P Davis, P Francis and V Jupp (eds) *Invisible Crimes: Their Victims and their Regulation,* Macmillan, London,1999.

McCahill, Michael and Rachel Finn, "The Social impact of Surveillance in Three UK Schools: 'Angels', 'Devils' and 'Teen Mums'", *Surveillance & Society*, Vol. 7, Nos. 3-4, 2010, pp. 273-289.

McCahill, Mike , and Clive Norris, "Estimating the Extent, Sophistication and Legality of CCTV in London", in Martin Gill (ed.), *CCTV*, Perpetuity Press, Leicester, 2003, pp. 51-66.

McCartney, C., "The DNA Expansion Programme and Criminal Investigations", *British Journal of Criminology*, 46 (2), 2006, pp. 175-192.

McCartney, Carol, Robin Williams and Tim Wilson, "Transnational exchange of forensic DNA: viability, legitimacy, and acceptability", *European Journal of Criminal Justice Research and Policy*, Vol. 17, No. 4, 2011, pp. 305-322.

McCartney, Carol, Robin Williams and Tim Wilson, *The Future of Forensic Bioinformation,* Nuffield Foundation, London, 2010.

McCullagh, Declan, “FBI: We need wiretap-ready websites – now” *CNETNews*, 4 May 2012. http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/

McCulloch, Jude and Sharon Pickering, “Pre-crime and Counter-terrorism: Imagining Future Crime in the ‘War on Terror’”, *British Journal of Criminology*, Vol. 49, 2009, pp. 628-645.

McGloin, Tim, “Pentagon Moolah,” *NewsObserver.com*, 30 June 2012. http://www.newsobserver.com/2012/06/30/2168781/tim-mcgloin-pentagon-moolah.html

Merle, Renae "Northrop Settles Billing Case: Shipbuilding Unit Allegedly Overbilled U.S. by $72 Million" *Washington Post*, 9 August 2003. http://pqasb.pqarchiver.com/washingtonpost/access/382495171.html?dids=382495171:382495171&FMT=ABS

Milmo, Dan, “BAE's largest investor voices concerns over EADS merger”, *The Guardian*, 8 October 2012. http://www.guardian.co.uk/business/2012/oct/08/invesco-concerns-bae-eads-merger?newsfeed=true

Ministry of Defence, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, 2010. http://www.direct.gov.uk/sdsr

Minnaar, Anthony, “The implementation and impact of crime prevention/crime control open street Closed-Circuit Television surveillance in South African Central Business Districts”, *Surveillance & Society*, Vol. 4, No. 3, 2007, pp. 174-207.

Mitsilegas, Valsamis, “Countering the Chameleon Threat of Dirty Money: ‘Hard’ and ‘Soft’ Law in the Emergence of a Global Regime against Money Laundering and Terrorist Finance”, in Adam Edwards and Peter Gill (eds.), *Transnational Organised Crime: Perspectives on Global Security*, Routledge, London, New York, 2003, pp. 195-211.

Mitsilegas, Valsamis, “New Forms of Transnational Policing: The Emergence of Financial Intelligence Units in the European Union and the Challenges for Human Rights: Part 1”, *Journal of Money Laundering Control*, Vol. 3, No. 2, May 1999, pp. 147-160.

Monahan, T. & R. D. Torres (eds.) *Schools under Surveillance: Cultures of control in public education*, Rutgers University Press, London, 2010.

Monahan, T., “Editorial: Surveillance and inequality”, *Surveillance and society*, Vol. 5, No. 3, September 2008, pp. 217-226.

Monahan, Torin, “Electronic fortification in Phoenix: Surveillance technologies and social regulation in residential communities”, *Urban Affairs Review*, Vol. 42, No. 2, 2008, pp. 169 - 192.

Monahan, Torin, “Surveillance and Terrorism”, in Kirstie Ball, Kevin Haggerty and David Lyon (eds.), *Routledge handbook of surveillance studies*, Routledge, New York, 2012, pp. 285-291.

Monahan, Torin, “Surveillance as governance: social inequality and the pursuit of democratic surveillance”, in Kevin Haggerty and Minas Samatas (eds.), *Surveillance and Democracy*, Routledge, New York, 2010, pp. 91-110.

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

Mordini, Emilio, “Whole Body Imaging at airport checkpoints: the ethical and policy context”, in René von Schomberg (ed.), *Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields*, Publications Office of the European Union, Luxembourg, 2011, pp. 165-209.

Mosco, Vincent, *The Digital Sublime: Myth, Power, and Cyberspace*, MIT Press, Cambridge and London, 2004.

Mosco, Vincent, *The Political Economy of Communication.* Sage, London, 1996.

Murakami Wood, David and Rodrigo Firmino, "Empowerment or repression? Opening up questions of identification and surveillance in Brazil through a case of 'identity fraud'", *Identity in the Information Society (IDIS)*, Vol. 2, No. 3, 2009, pp. 297-317.

Murakami Wood, David, "The 'Surveillance Society': Questions of History, Place and Culture", *European Journal of Criminology*, Vol. 6, No. 2, 2009, pp. 179-194.

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.

Murakami Wood, David, Kirstie Ball, David Lyon, Clive Norris, and Charles Raab, "A Report on the Surveillance Society", Report for the Information Commissioner by the Surveillance Studies Network, 2006. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf

Nabbali, Talitha and Mark Perry, "Going for the throat: Carnivore in an Echelon World", *Computer Law and Security Report*, Vol. 19, No. 6, 2003, pp. 456-467.

Nandini, C. and C.N. Ravi Kumar, "Comprehensive framework to gait recognition", *International Journal of Biometrics*, Vol. 1, No. 1, 2008, pp. 129-137.

Naraine, Ryan, "First Look: Sentry Remote and eBlaster 6.0", *PCWorld*, 15 November 2007. http://www.pcworld.com/article/139460/first_look_sentry_remote_and_eblaster_60.html

National Research Council, "Review of the Department of Homeland Security's Approach to Risk Analysis", National Academic Press, Washington, D.C. , 2010.

Naumann, Ingo and Giles Hogben [European Network and Information Security Agency (ENISA)], "Privacy Features of European eID Card Specifications", *Elsevier Network Security Newsletter*, August 2008, pp. 9-13. http://bit.ly/Ts9P2R.

Naylor, Robin T., *Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy*, Cornell University Press (Revised Edition), Ithaca, London, 2004.

Nelson E. Roth., "The New York State Police Evidence Tampering Investigation", Confidential Report to the Governor of New York, Ithaca, New York, 1997.

Netzwerk Neue Medien, "Demo against surveillance in Berlin on Saturday 17 Juni June", 14 June 2006. http://www.nnm-ev.de/show/158205.html http://translate.google.com/translate?depth=1&hl=en&prev=/search%3Fq%3DNetzwerk%2BNeue%2BMedien%26hl%3Den%26rlz%3D1I7SVEA_enGB350%26prmd%3Dimvns&rurl=translate.google.co.uk&sl=de&u=http://www.nnm-ev.de/show/158205.html

Newman, Oscar, *Defensible space: Crime prevention through urban design*, Mac Millan Co., New York, 1972.

News Wires, "French firm Amesys probed over 'complicity in torture'" *France 24*, 22 May 2012. http://www.france24.com/en/20120522-libya-france-gaddafi-amesys-war-crimes-technology-firm-court-justice

Nishihara, Hiroshi, "Constitutional Meaning of the Proportionality Principle in the Face of 'Surveillance State'", *Waseda Bulletin of Comparative Law*, 2008 (1) pp. 1-10.

Nissenbaum, Helen, "Privacy as Contextual Integrity", *Washington Law Review*, Vol. 79, No. 1, 2004, pp. 101-139.

Nissenbaum, Helen, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, Stanford, CA, 2010.

Norris, Clive and Gary Armstrong, *The Maximum Surveillance Society: The Rise of CCTV*, Berg, Oxford, 1999.

Norris, Clive, "A Review of the Increased Use of CCTV and Video-Surveillance for Crime Prevention Purposes in Europe", EU Policy Department C Citizens' Rights and Constitutional Affairs, PE 419.588, April 2009.

Norris, Clive, "The success of failure, Accounting for the global growth of CCTV", in Kirstie Ball, Kevin D. Haggerty, and David Lyon (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, London, 2012, pp. 251-258.

Norris, Clive, Mike Mc Cahill, and David Wood, "Editorial", *Surveillance & Society*, Vol. 2, Nos. 2-3, 2004, pp. 110-135.

Norris, Clive, Mike McCahill, and David Wood, "The Growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space", *Surveillance & Society*, Vol. 2, No. 2/3, 2004, pp. 110-135.

Northern Ireland Assembly (NIA), "Drug Testing Mechanisms Used Globally", Research Paper 34/10, Research and Library Services, Northern Ireland Assembly, 2010. http://archive.niassembly.gov.uk/researchandlibrary/publications2010.htm

Nouwt, Sjaak, Berend R. de Vries, and Corien Prins (eds.), *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, TCM Asser Press, The Hague, 2005.

Nunn, Jr., Edgar S. , "The Idea of a National Data Center and the Issue of Personal Privacy", *The American Statistician*, Vol. 21, No. 1, 1967, pp. 21-27.

Nutt, D., *Written response to Department of Transport consultation paper on road safety compliance*, Advisory Council on the Misuse of Drugs, London, 2009. http://www.homeoffice.gov.uk/publications/agencies-public-bodies/acmd1/DfT-road-safety-compliance-cons?view=Binary

OECD, *Drugs and Driving: Detection and Deterrence*, OECD publishing, 2010. http://dx.doi.org/10.1787/9789282102763-en

OECD, *The Security Economy*, Organisation for Economic Co-operation and Development, 2004, http://www.oecd.org/futures/16692437.pdf.

Office of Surveillance Commissioners, *Annual Report of the Chief Surveillance Commissioner to the Prime Minister and to Scottish Ministers for 2011-2012, Presented to Parliament pursuant to section 107(3) of the Police Act 1997,* House of Commons, 13 July 2012.
http://surveillancecommissioners.independent.gov.uk/docs1/OSC-annual-report-2011-12.pdf

Omand, D., J. Bartlett and C. Miller, *#Intelligence*, Demos, London, 2011. http://www.demos.co.uk/files/_Intelligence_-_web.pdf?1335197327

Orlowski, Andrew, "Google buys CIA-backed mapping startup", *The Register*, 28 October 2004. http://www.theregister.co.uk/2004/10/28/google_buys_keyhole/

OSI, *Police Profiling in Europe: Pervasive, Ineffective, and Discriminatory*, Open Society Institute, New York, 2009.

Padgett, K., W. Bales and T. Blomberg, "Under Surveillance: An empirical test of the effectiveness and consequences of electronic monitoring", *Criminology & Public Policy,* Vol. 5, Iss. 1, 2006, pp. 61–91.

Paetow, Barbara, *Vergewaltigung in der Ehe: eine strafrechtsvergleichende Untersuchung unter besonderer Berücksichtigung des Rechts der Vereinigten Staaten*, Max-Planck-Institut für ausländisches und internationals Strafrecht, Freiburg i. Breisgau, 1987.

Parenti, Christian, *The Soft Cage: Surveillance in America, from Slave Passes to the Patriot Act*, Basic Books, New York, 2003.
Passas, Nikos, "Fighting Terror with Error: The counter-productive regulation of Informal Value Transfers", *Crime, Law & Social Change*, 2006.
Pati, Anita, "Is community safety at risk as cash-strapped councils cut CCTV?" *The Guardian*, 16 December 2011. http://www.guardian.co.uk/local-government-network/2011/dec/16/community-safety-risk-councils-cctv
Petersen, Julie K., *Understanding surveillance technologies: Spy devices, privacy, history and applications*, Auerbach Publications, Boca Raton, 2007.
Pfaff, Steven, "The limits of coercive surveillance: Social and penal control in the German Democratic Republic", *Punishment and Society* Vol. 3 No. 3, 2001, pp. 381- 407.
Phillips & Cohen LLP, "Scientist blew whistle on faulty military satellite parts; Northrop Grumman pays $325 million to settle case", Press Release, 2 April 2009. http://www.phillipsandcohen.com/2009/Scientist-blew-whistle-on-faulty-military-satellite-parts-Northrop-Grumman-pays-325-million-to-settle-case.shtml
Phillips, Coretta, "A Review of CCTV Evaluations: Crime Reduction Effects and Attitudes towards its Use", *Crime Prevention Studies*, Vol. 10, 1999, pp. 123-155.
Phillips, David J., "The Influence of Policy Regimes on the Development and Social Implications of Privacy Enhancing Technologies", Paper presented at: Telecommunication Policy Research Council 29th Research Conference on Communication, Information and Internet Policy, 2001.
Piro, Joseph M., "Foucault and the architecture of surveillance: Creating regimes of power in schools, shrines and society", *Educational Studies: A Journal of the American Educational Studies Association*, Vol. 44, 2008, pp. 30 – 46.
Posner, Richard, "Privacy, secrecy and reputation", *Buffalo Law Review*, Vol. 28, 1979, pp. 1-55.
Post, Robert, "Three concepts of privacy", *Georgetown Law Review*, Vol. 89, 2000-01, pp. 2087-2098.
Poster, Mark, *The mode of information: Poststructuralism and social context*, University of Chicago Press, Chicago, 1990.
Power, Michael, *Organized Uncertainty: Designing a World of Risk Management*, Oxford University Press, Oxford, 2007.
Preuss-Laussinotte, S., "L'Union européenne et les technologies de sécurité", *Cultures & Conflits*, No. 64, Winter 2006, pp. 97-108.
PRISE Project, Deliverable 2.2, Overview of Security Technologies, 2006/2007. http://www.prise.oeaw.ac.at/docs/PPRISE_D2.2_Overview_of_Security_Technologies-Revision1.pdf
Privacy International, "Big Brother Inc.". https://www.privacyinternational.org/projects/big-brother-inc
PRNewswire, "G4S Violates Employees' Human Rights, Says UNI Property Services Global Union", *PRNewswire*, 17 March 2012. http://www.prnewswire.co.uk/news-releases/g4s-violates-employees-human-rights-says-uni-property-services-global-union-153163355.html
Prosser, William, "Privacy", *California Law Review*, Vol. 48, 1960, pp. 338-343.
Pushpa Rani, M. and G. Arumugam "An Efficient Gait Recognition System for Human Identification Using Modified ICA", *International Journal of Computer Science and Information Technology*, Vol. 2, No. 1, 2010, pp. 55-67.
QinetiQ Group plc, *Annual Report and Accounts 2012*. http://www.qinetiq.com/investors/results-reports/AnnualReportDocuments/QinetiQ-Annual-Report-2012.pdf

Quadnetics Group plc, *Innovating, Integrating, Protecting: Annual Report and Accounts for the 12 months ended 30 November 2011*. http://www.quadnetics.com/Doc/Pdf/Financials/AnnualInterimReports/AnnualReport2011.pdf

Queensland Parliamentary Travelsafe Committee (QPTC), *Report No 51: Report on the Inquiry into Automatic Number Plate Recognition Technology*, Legislative Assembly of Queensland, Brisbane, 2008. http://rti.cabinet.qld.gov.au/documents/2009/apr/gov%20response%20to%20travelsafe%20report%20no%2051/Attachments/Travelsafe%20R51.pdf

Raab, Charles and Benjamin Goold, "Protecting Information Privacy", Research Report RR69, Equality and Human Rights Commission, London, 2011.

Raab, Charles and David Wright, "Surveillance: Extending the Limits of Privacy Impact Assessment", in Wright, David and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012, pp. 363-383.

Raab, Charles D. "Privacy, Social Values and the Public Interest", in Andreas Busch and Jeanette Hofmann (eds.) *Politik und die Regulierung von Information [Politics and the Regulation of Information]*, Politische Vierteljahresschrift Sonderheft 46, Nomos Verlagsgesellschaft, Baden-Baden, 2012, pp. 129-151.

Raab, Charles, "Governing the safety state", Inaugural Lecture at the University of Edinburgh, 7 June 2005.

Raab, Charles, and David Wright, "Constructing a surveillance impact assessment", Paper presented at the Living in Surveillance Societies (LiSS) workshop, Budapest, 1-3 October 2012.

Raab, Charles, and David Wright, "Surveillance: Extending the limits of privacy impact assessment", in David Wright and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012, pp. 363-383.

Rachels, James, "Why privacy is important", *Philosophy & Public Affairs*, Vol. 4, No. 4, Summer 1975, pp. 323-333.

Radio Netherlands Worldwide, "Dutch border police happy with CCTV cameras", *Radio Netherlands Worldwide*, 29 March 2011. http://www.rnw.nl/english/bulletin/dutch-border-police-happy-cctv-cameras

Radio Netherlands Worldwide, "Earth Beat – Born free", *Radio Netherlands Worldwide*, 25 December 2011. http://www.rnw.nl/english/radioshow/born-free

Radzinowicz, Leon, *A history of English criminal law and its administration from 1750, Vol. 4*, Stevens and Sons, London, 1948.

Rappert, Brian, "The Distribution and Resolution of the Ambiguities of Technology, or Why Bobby Can't Spray", *Social Studies of Science*, Vol. 31, No. 4, 2001, pp. 557-591.

Ratcliffe, J. and T. Taniguchi, *CCTV Camera Evaluation: The crime reduction effects of public CCTV cameras in the City of Philadelphia, PA installed during 2006*, Temple University, Philadelphia, 2008.

Razac, Olivier, *Avec Foucault, après Foucault. Disséquer la société de contrôle*, L'Harmattan, Paris, 2008.

Razac, Olivier, *Histoire politique du barbelé*, Editions Flammarion, Paris, 2009.

Reaves, Lawrence, "Honeywell Fined 11.8 Million Dollars For Environmental Violations", *Isnare.com*, 3 July 2012. http://www.isnare.com/?aid=1065026&ca=Society

Reckwitz, A. "Toward a theory of social practices: A development in culturalist theorizing", *European Journal of Social Theory*, Vol. 5, No. 2, May 2002, pp. 243-263.

Reeve, Tom, “BSIA rejects surveillance camera commissioner’s claims about CCTV” *Security News Desk,* 3 October 2012. http://www.securitynewsdesk.com/2012/10/03/bsia-rejects-surveillance-camera-commissioners-claims-about-cctv/

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

Reidenberg, Joel, “Lex Informatica: The Formulation of Information Policy Rules Through Technology”, *Texas Law Review*, Vol. 76, 1998, pp. 552-593.

Reid-Green, Keith S., “The History of Census Tabulation”, *Scientific American*, Vol. 260, No. February, 1989, pp. 98-103.

Reiman, Jeffrey H., “Privacy, intimacy and personhood”, Philosophy & Public Affairs, Vol. 6, No. 1, Fall 1976, pp. 26-44

Renzema, M. and E. Mayo-Wilson, “Can Electronic Monitoring Reduce Crime for Moderate to High Risk Offenders?”, *Journal of Experimental Criminology*, 1, 2005, pp. 215-237.

Reuters, “Arroyo suspends telecoms deal with Chinese firm”, *Reuters,* 22 September 2007. http://in.reuters.com/article/2007/09/22/idINIndia-29667620070922

Reuters, “China's ZTE admits to Telenor ethical breach”, *Reuters,* 14 October 2008, http://www.reuters.com/article/2008/10/14/zte-idUSHKG19992320081014

Richardson, Ginger D., “Honeywell to pay $5 mil in Valley-pollution settlement”, Arizona Republic, Azcentral.com, 8 August 2008. http://www.azcentral.com/arizonarepublic/news/articles/2008/08/08/20080808hazardouswaste.html

Richter, Philipp, “Datenschutz durch Technik und die Grundverordnung der EU-Kommission”, *DuD - Datenschutz und Datensicherheit*, Vol. 36, No. 8, 2012, pp. 576-580.

Ritzer, George, *Globalisation: The Essentials*, Wiley Balckwells, Chichester, 2011.

Rizzo, Carmine & Charles Brookson, “Security for ICT” –the Work of ETSI”, ETSI White Paper No 1, January 2012. http://www.scribd.com/doc/100874830/ETSI-security-for-ICT-white-paper

Robertson, Roland, “Glocalization: Time-space and homogeneity-heterogeneity”, in F. Featherstone, S. Lash, and Roland Robertson (eds.), *Global Modernities*, Sage, London, 1995.

Robinson, Lisa A., “Valuing Mortality Risk Reductions in Homeland Security Regulatory Analyses”, Final Report for U.S. Customs and Border Protection, Department of Homeland Security, 2008. http://www.regulatory-analysis.com/robinson-dhs-mortality-risk-2008.pdf

Roman, J., S. Reid, J. Reid, A. Chalfin, W. Adams and C. Knight, *The DNA Field Experiment: Cost-Effectiveness Analysis of the Use of DNA in the Investigation of High-Volume*, Urban Institute, Justice Policy Centre, Washington, 2008.

Rosendaal, Arnold, “Massive Data Collection by Mistake?”, in Jan Camenisch, Bruno Crispo, Simone Fischer-Hübner, Ronald Leenes, and Giovanni Russello (eds.), *Privacy and Identity Management for Life: 7th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6/PrimeLife International Summer School, Trento, Italy, September 5-9, 2011, Revised Selected Papers*, Springer, Heidelberg, Berlin, 2012, pp. 274-282.

Rosoff, Matt, “Is Google A Monopoly? 'We're In That Area,' Admits Schmidt”, *Business Insider*, 21 September 2011.

Ross, Alice K., “Government ramps up controls on FinSpy surveillance software”, The Bureau of Investigative Journalism, 11 September 2012.

http://www.thebureauinvestigates.com/2012/09/11/government-ramps-up-controls-on-finspy-surveillance-software/

Rossides, Gale, "Advanced Imaging Technology – Yes It's Worth It", *The Blog@Homeland Security*, 1 April 2010. http://blog.dhs.gov/

Rössler, Beate, *The Value of Privacy*, Polity Press, Cambridge, 2005.

Rozek, Dan, "Chemical company pays $3.6 mil. to settle suits", *Chicago Sun-Times*, 6 September 2003.

Rule, James B., "High-Tech Workplace Surveillance: What's Really New?", in David Lyon, and Elia Zureik (eds.), *Computers, Surveillance, and Privacy*, University of Minnesota Press, Minneapolis, 1996, pp. 66-76.

Rule, James B., *Private Lives and Public Surveillance*, Allen Lane, London, 1973.

Runciman, W.G., *Report of the Royal Commission on Criminal Justice*, Cm 2263, The Stationery Office, London, 1993.

Saetnan, Ann Rudinow, Heidi Mork Lomell and Carsten Wiecek, "Controlling CCTV in Public Spaces: is privacy the (only) issue? Reflections on Norwegian and Danish observations", *Surveillance & Society*, Vol. 2, Nos. 2-3, 2004, pp. 296-414.

Safire, W., "The Great Unwatched", *New York Times*, 18 February 2002. http://www.nytimes.com/2002/02/18/opinion/18SAFI.htm

Salter, Mark (ed.), *Politics at the Airport*, University of Minnesota Press, Minnesota, 2008.

Salter, Mark B., "Passports, Mobility, and Security: How smart can the border be?", *International Studies Perspective*, Vol. 5, No. 1, January 2004, pp. 71-91.

Salter, Mark B., "Surveillance", in J. Peter Burgess (ed.), *The Routledge Handbook of New Security Studies*, Routledge, New York, 2010, pp. 187-196.

Samatas, Minas, Chiara Fonio, Catarina Frois and Gemma Galdon Clavell, "Authoritarian Surveillance and its Legacy in South-European Societies: Greece, Italy, Spain, Portugal," in William C Webster, 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.

Sarno, C. "The Impact of Closed Circuit Television on Crime in Sutton Town Centre", in M. Bulos and D. Grant (eds.), *Towards a Safer Sutton? CCTV One Year On*, London Borough of Sutton, London, 1996.

Scheinin, Martin, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Human Rights Council, Thirteenth session. A/HRC/13/37 28 December 2009. http://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf

Schmid, Gerhard (rapporteur), *Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system)* (2001/2098(INI)), A5-0264/2001, European Parliament, Temporary Committee on the ECHELON Interception System, Luxembourg, 2001.

Schoeman, Ferdinand (ed.) *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, New York, 1984.

Schoeman, Ferdinand, "Privacy: philosophical dimensions of the literature", in Ferdinand Schoeman (ed.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, New York, NY, 1984, pp. 1-33.

Schoeman, Ferdinand, *Privacy and Social Freedom*, Cambridge University Press, Cambridge, 1992.

Schulze, Hendrik, and Klaus Mochalski, "Internet Study 2008/2009", ipoque GmbH, Leipzig, 2009.

http://www.ipoque.com/sites/default/files/mediafiles/documents/internet-study-2008-2009.pdf
Schulzki-Haddouti, Christiane, "Sicherheit im Netz und digitale Bürgerrechte", *Aus Politik und Zeitgeschichte* B49-50/2003, pp. 13-19.
Schwartz, Adina, "A 'Dogma of Empiricism' revisited: Daubert v. Merrell Dow Pharmaceuticals Inc. and the need to ressurect the philosophical insight of Frye v.United States," *Harvard Journal of Law & Technology*, Vol. 10, No. 2, Winter 1997.
Scottish Government, *Identity Management and Privacy Principles: Privacy and Public Confidence in Scottish Public Services*, Version 1.0, December 2010, The Scottish Government, Edinburgh.
Seabrook, Tamara and Louise Wattis, "The techno-flâneur. Tele-erotic re-presentation of women's life spaces", in E. Leigh Keeble and Brian D. Loader (eds.), *Community informatics: Shaping computer-mediated social relations*, Routledge, London, 2001, pp. 240-259.
Security World Magazine Online, "Behaviour Recognition: Does Someone Look Out of Place", Security World Magazine Online, 2007. http://www.securityworldmag.com/tech/tech_view.asp?idx=249&part_code=030160069&page=1
Sekula, A. "The Body and the Archive", *October* (39) Winter: 3-64, 1986, p. 27.
Senner, Wayne M., *The Origins of writing*, University of Nebraska Press, Lincoln, 1991.
Sennett, Richard, *The Fall of Public Man*, Norton, New York, 1974.
Shachtman, Noah, "'Don't Be Evil,' Meet 'Spy on Everyone': How the NSA Deal Could Kill Google", *Wired*, 4 February 2010. http://www.wired.com/dangerroom/2010/02/from-dont-be-evil-to-spy-on-everyone/
Shen, Yun and Siani Pearson, "Privacy Enhancing Technologies: A Review", HPL-2011-113, 2011.
Sheptycki, James, "Policing the virtual launderette: Money laundering and global governance", in James Sheptycki (ed.), *Issues in Transnational Policing*, Routledge, London, New York, 2000, pp. 135-176.
Shobhit, Saxena et al. "Crowd Behaviour Recognition for Video Surveillance", *Proceedings of the 10th International Conference on Advanced Concepts for Intelligent Vision Systems*, 2008, pp. 970-981.
Short, Emma, and Jason Ditton, "Does CCTV affect crime?", *CCTV Today*, Vol. 2, No. 2, 1995, pp. 10-12.
Shpayer-Makov, Haia, *The Ascent of the Detective. Police Sleuths in Victorian England*, Oxford University Press, Oxford, 2011.
Silver, Vernon, "European Union Bans Exports to Syria of Systems for Monitoring Web, Phones", *Bloomberg News*, 1 December 2011. http://www.bloomberg.com/news/2011-12-01/european-union-bans-exports-to-syria-of-systems-for-monitoring-web-phones.html
Simões, Maria João, "Surveillance: A (Potential) Threat to Political Participation?", *The Fifth International Conference on Digital Society*, 2011, pp 94-99.
Simon, B., "The Return of Panopticism: Supervision, Subjection and the New Surveillance", *Surveillance and Society*, Vol. 3, No. 1, pp. 1-20, 2005.
Singel, Ryan, "Life After Death for CAPPS II?", *Wired*, 16 July 2004. http://www.wired.com/politics/security/news/2004/07/64240
Singh Richa, Vatsa Mayank and Noore Afzel, "Recognizing Face Images with Disguise Variations", in Kresimir Delac, Mislav Grgic and , Marian Stewart Bartlett (eds.), *Recent Advances in Face Recognition*, In-teh, Croatia, 2008.

Skinns, D., "Crime Reduction, Diffusion and Displacement: Evaluating the Effectiveness of CCTV", in Clive Norris, Jade Moran and Gary Armstrong (eds.), *Surveillance, Closed Circuit Television and Social Control*, Aldershot, Ashgate, 1998.

SMART Project, "SMART Workplan Document", 2010. http://www.smartsurveillance.eu

Smith, Gavin J. D., "Behind the Screens: Examining Constructions of Deviance and Informal Practices among CCTV Control Room Operators in the UK", *Surveillance and Society*, Vol. 2, No. 2/3, 2004, pp. 376-395.

Smith, Gavin J. D., "Surveillance work(ers)", in Kirstie Ball, Kevin D. Haggerty, and David Lyon (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, London, 2012, pp. 107-115.

Smolaks, Max, "Apple Sends Out Spy Planes To Challenge Google Maps" *TechWeekEurope*, 11 June 2012. http://www.techweekeurope.co.uk/news/apple-spy-planes-google-maps-81842

Solove, D., "'I've got nothing to hide' and other misunderstandings of privacy", *San Diego Law Review*, Vol. 44, No. 475, July 2007, pp. 745-772.

Solove, Daniel, "Data mining and the security-liberty debate", *University of Chicago Law Review*, Vol. 74, 2008, pp. 343-362.
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=990030

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

Solove, Daniel, *Nothing to Hide. The False Tradeoff between Privacy and Security*, Yale University Press, Yale, 2011.

Solove, Daniel, *The Digital Person*, New York University Press, New York and London, 2004.

Solymar, Laszlo, *Getting the Message: A History of Communications*, Oxford University Press, Oxford, 1999.

Song, A., "Technology, Terrorism, and the Fishbowl Effect: An Economic Analysis of Surveillance and Searches", *The Berkman Center for Internet & Society Research Publication*, No. 5, September 2003, pp. 1-26.

Song, Andrew, "Technology, Terrorism, and the Fishbowl Effect: An Economic Analysis of Surveillance and Searches", *The Berkman Center for Internet & Society Research Publication*, No. 5, September 2003, pp. 1-26.

Sorell, Tom, "Preventive Policing, Surveillance, and European Counter-Terrorism", *Criminal Justice Ethics*, Vol. 30, No. 1, April 2011, pp. 1-22.

Spiegel Online, "Aldi Spied on Female Shoppers", *Spiegel Online*, 30 April 2012. http://www.spiegel.de/international/germany/aldi-spied-on-female-shoppers-with-hidden-cameras-a-830690.html

Spiegel Online, "Siemens Allegedly Sold Surveillance Gear to Syria," *Spiegel Online*, 4 November 2012. http://www.spiegel.de/international/business/ard-reports-siemens-sold-surveillance-technology-to-syria-a-826860.html

Spriggs, Angela, Javier Argomaniz et al, "Public attitudes towards CCTV: results from the Pre-intervention Public Attitude Survey carried out in areas implementing CCTV", Home Office Online Report, October 2006.

Stadler, Lena, Steffen Bieneck and Christian Pfeiffer, Repräsentativbefragung Sexueller Missbrauch 2011, Forschungsbericht Nr. 118, KFN, Hannover, 2012.

Stanton, Jeffrey M., "Reactions to employee performance monitoring: Framework, review and research directions", *Human Performance*, Vol. 13 No. 1, 2000, pp. 85-113.

Staples, W. G., *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*, Rowman/Littlefield, Lanham, MD, 2000.

Staples, William G., *Everyday surveillance: Vigilance and visibility in postmodern life*, Rowman & Littlefield, Lanham, MD, 2000.
Staples, William, *Everyday Surveillance: Vigilance and Visibility in Postmodern Life*, MD: Rowman & Littlefield Publishers, Lanham, 2000.
Starr, Amory, Luis A. Fernandez, Randall Amster, Lesley J. Wood and Manuel J. Caro, "The Impact of State Surveillance on Political Assembly and Association: A Socio-Legal Analysis", *Qualitative Sociology*, Vol. 31, No. 3, 2008, pp. 251-270.
Statewatch, "EU-PNR (Passenger Name Record)", 2011. http://www.statewatch.org/Targeted-issues/eu-pnr/eu-pnr-observatory.htm
Statewatch, "Observatory on the European Security Research Programme (ESRP)". http://www.statewatch.org/Targeted-issues/ESRP/security-research.html
Stecklow, Steve, "Special Report: Chinese firm helps Iran spy on citizens", *Reuters,* 22 March 2012. http://www.reuters.com/article/2012/03/22/us-iran-telecoms-idUSBRE82L0B820120322.
Stenson, Kevin and Robert R. Sullivan (eds.), *Crime, risk and justice: the politics of crime control in liberal democracies,* Willian, Cullompton, 2001.
Stewart, Mark G. , and John Mueller, "Risk and Cost-Benefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening", Research Report 280.11.2101, The University of Newcastle, Australia, 2011. http://ogma.newcastle.edu.au:8080/vital/access/manager/Repository/uon:6893
Stirling-Belin, Florence, "Traçabilité, liberté de circulation et Union européenne", *Revue de la recherche juridique, droit prospectif*, Vol. 30, No. 1, 2005, pp. 409-432.
Stoddart, Eric, *Theological Perspectives on a Surveillance Society: Watching and Being Watched*, Ashgate Publishing, Aldershot, 2011.
Strandburg, Katherine J., "Surveillance of Emergent Associations: Freedom of Association in a Network Society", in Alessandro Acquisti, Sabrina De Capitani di Vimercati, Stefanos Gritzalis and Costas Lambrinoudakis (eds.) *Digital Privacy: Theory, Technologies, and Practices,* Auerbach Publications, Boca Raton, 2007, pp. 435-459.
Ström, Pär, *Die Überwachungsmafia: Das lukrative Geschäft mit unseren Daten*, Heyne, München, 2005.
Surette, Ray, "The thinking eye: Pros and cons of second generation CCTV surveillance systems", *Policing*, Vol. 28, No. 1, 2005, pp. 152-173.
Surveillance Studies Network (SSN), *A report on the surveillance society*, prepared for the Information Commissioners Office, Wilmslow, 2006.
Swami, Praveen, "The government's listening to us", *The Hindu*, 1 December 2011. http://www.thehindu.com/news/national/article2678501.ece
Swire, Peter, "From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government to Seek Access to the Cloud", *International Data Privacy Law*, Vol. 2, No. 4, 2012, pp. 200-206.
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, London, Ithaca 2010.
Szekely, Ivan, "What Do IT Professionals Think About Surveillance?", in Christian Fuchs, Kees Boersma, Anders Albrechtslund and Marisol Sandoval (eds.), *Internet and Surveillance. The Challenge of Web 2.0 and Social Media,* Routledge, New York, 2011, pp. 198-219.

Szekely, Ivan,"Hungary", in James B. Rule and Graham Greenleaf (eds.), *Global Privacy Protection: The First Generation*, Edward Elgar Publishing Ltd., November 2008.
Taylor, Emmeline, "Surveillance in Schools" in Kirstie Ball, Kevin Haggerty, David Lyon (eds) *The Routledge Handbook of Surveillance Studies*, Routledge, London, 2012.
Taylor, Geoffrey and Martin Gill, "Preventing Money Laundering or Obstructing Business ? Financial Companies' Prespectives on 'Know your Customer' Procedures", *British Journal of Criminology*, Vol. 44, September 2004, pp. 582-594.
Taylor, Mathew and Alan Travis, "G4S chief predicts mass police privatisation", *The Guardian*, 20 June 2012. http://www.guardian.co.uk/uk/2012/jun/20/g4s-chief-mass-police-privatisation
Taylor, Matthew, "How G4S is 'securing your world'", *The Guardian*, 20 June 2012. http://www.guardian.co.uk/uk/2012/jun/20/g4s-securing-your-world-policing/
Teal Group, "Teal Group Predicts Worldwide UAV Market Will Total $89 Billion in Its 2012 UAV Market Profile and Forecast", *PR Newswire*, 11 April 2012. http://tealgroup.com/index.php/about-teal/teal-group-in-the-media/3/79-teal-group-predicts-worldwide-uav-market-will-total-89-billion-in-its-2012-uav-market-profile-and-forecast
Teal Group, *World Unmanned Aerial Vehicle Systems, Market Profile and Forecast 2012*, http://tealgroup.com/index.php/about-teal/teal-group-in-the-media/3/79-teal-group-predicts-worldwide-uav-market-will-total-89-billion-in-its-2012-uav-market-profile-and-forecast.
The Associated Press, "Court rules that Google-NSA spy ties can remain secret", *USA Today*, 11 May 2012. http://www.usatoday.com/tech/news/story/2012-05-11/court-google-nsa-spy-china/54912902/1
The Guardian, "Sex offenders face mandatory lie detector tests", *The Guardian*, 20 July 2012. http://www.guardian.co.uk/society/2012/jul/20/sex-offenders-lie-detector-tests
The Guardian, "Fingerprint evidence 'based on opinion rather than facts'", *The Guardian*, 14 Dec. 2011. http://www.guardian.co.uk/uk/2011/dec/14/fingerprint-evidence-opinion-fact
The Guardian, "Police under fire over Muslim CCTV surveillance scheme", *The Guardian*, 18 June 2010.
The Guardian, "Queen's speech 2012 – full text" *The Guardian*, 9 May 2012. http://www.guardian.co.uk/politics/2012/may/09/queens-speech-2012-full-text
The Local, "Data protector 'cannot check police spyware'", *The Local*, 12 September 2012. http://www.thelocal.de/sci-tech/20120912-44919.html
Thomas, Terry, *Criminal Records: A Database for the Criminal Justice System and Beyond*, Palgrave Macmillan, Basingstoke, 2007.
Tidd, Joe, John Bessant and Keith Pavitt, *Managing Innovation. Integrating Technological, Market and Organizational Change*, John Wiley & Sons, Chichester, 2005.
Timberg, Craig, "Skype joins hands with authorities to assist in online surveillance", The Washington Post, 27 July 2012. http://www.smh.com.au/technology/technology-news/skype-joins-hands-with-authorities-to-assist-in-online-surveillance-20120726-22v0t.html
Töpfer, E., "Network with errors. Europe's emerging web of DNA databases", *Statewatch Bulletin*, Jg. 21, Nr. 1, 2011, pp. 1-3.
Torny, D., "La traçabilité comme technique de gouvernement des hommes et des choses", *Politix*, No. 44, May 1998, pp. 51-75.

Torstar News Service, “Surveillance spyware spreading to smartphones”, *Metro News*, 31 August 2012. http://metronews.ca/news/canada/355128/surveillance-spyware-program-spreading-to-smartphones/.

Transport for London (TfL), *Congestion charging: Impacts monitoring*, Second Annual Report, April 2004. http://www.tfl.gov.uk/assets/downloads/Impacts-monitoring-report-2.pdf

Transportation Security Administration, “Advanced Imaging Technology (AIT)”, 11 October 2012. http://www.tsa.gov/traveler-information/advanced-imaging-technology-ait

Trechsel, Stephen, *Human Rights in Criminal Proceedings*, Collected Courses of the Academy of European Law, Oxford University Press, 2005.

TSecNet s.r.l, “Video Surveillance and Physical Security”. http://www.tsecnet.com/en/solutions/security-systems/1/video-surveillance-and-physical-security

Turpin, Colin, *British Government and the Constitution: Text, Cases and Materials*, 4th edn., Butterworths, London, 1999.

Tyco International, *2011 Annual Report*. http://www.tyco.com/2011annualreport/

Tyler, Richard, “Chancellor backs UK grab for data analytics market”, *The Telegraph*, 16 May 2011. http://www.telegraph.co.uk/finance/yourbusiness/8516366/Chancellor-backs-UK-grab-for-data-analytics-market.html

U.K. Motorists, “Automatic Number Plate Recognition”, 2012. http://www.ukmotorists.com/anpr.asp

U.S. Department of Defense, “Facial Recognition Vendor Test 2000 Evaluation Report”, U.S. Department of Defense Counterdrug Technology Development Program Office, 16 Feb. 2000 / 29 Nov. 2000. http://www.dodcounterdrug.com/facialrecognition/DLs/FRVT_2000.pdf

U.S. Department of Homeland Security, “FY 2011 Budget in Brief”, Washington, D.C., 2011. http://www.dhs.gov/xlibrary/assets/budget_bib_fy2011.pdf

U.S. Department of State, “Visa Waiver Program (VWP)”, Washington, D.C., last updated 2.10.2012. http://travel.state.gov/visa/temp/without/without_1990.html - vwp

U.S. International Association of Chiefs of Police Virginia (IACP), “Privacy impact assessment report for the utilization of license plate readers”, 2009. http://www.theiacp.org/LinkClick.aspx?fileticket=N%2BE2wvY%2F1QU%3D&tabid=87

U.S. National Institute of Justice (NIJ), “Secure Continuous Remote Alcohol Monitoring (SCRAM) Technology Evaluability Assessment”, The National Institute of Justice, (no date). https://www.ncjrs.gov/pdffiles1/nij/secure-continuous-remote-alcohol.pdf

U.S. Treasury Department Office of Public Affairs, Testimony of Stuart Levey, Under Secretary, Terrorism and Financial Intelligence, US Department of the Treasury, Before the House Financial Services Subcommittee on Oversight and Investigations, Washington, 11 July 2006.

U.S. Treasury Department, “Terrorist Finance Tracking Program – Factsheet”, 23 June 2006. http://ebookbrowse.com/tftp-fact-sheet-revised-2-15-11-2-pdf-d328699617

UK Department for Transport, “Impact Assessment on the use of security scanners at UK airports”, London, 2010.

UK House of Lords, Daily Hansard, 21 Nov 2011: Column WA20. http://www.publications.parliament.uk/pa/ld201011/ldhansrd/text/111121w0001.htm

UK House of Lords, Select Committee on the Constitution, *2nd Report of Session 2008-09, Surveillance: Citizens and the State,* HL Paper 18-II, Volume II: Evidence, The Stationery Office, London, 2009.

UK Select Committee on Home Affairs, *Why has the use of surveillance increased?* Fifth Report, 8 June 2008. http://www.publications.parliament.uk/pa/cm200708/cmselect/cmhaff/58/5807.htm

Ulzheimer, John, "Class Action Lawsuit Filed Against Consumerinfo.com, an Experian Company", *Smartcredit,* 29 March 2011. https://www.smartcredit.com/blog/2011/03/29/class-action-lawsuit-filed-against-consumerinfo-com-an-experian-company/

United Nations Security Council, "Letter dated 13 May 2008 from the Chairman of the Security Council Committee established pursuant to resolution 1267 (1999) concerning Al-Qaida and the Taliban and associated individuals and entities addressed to the President of the Security Council", New York, S/2008/324, 14 May 2008.

United Nations, *Recommandations figurant dans le huitième rapport de l'Équipe d'appui analytique et de surveillance des sanctions: position du Comité*, S/2008/408, New York, June 2008.

Urry, John, *Mobilities*, Polity Press, Oxford, 2007

US Department of Justice Office of the Inspector General Audit Division, *The Federal Bureau of Investigation's Terrorist Watchlist Nomination Process*, 2009.

US Department of State, "Enhanced Border Security and Visa Entry Reform Act of 2002 ALDAC No.1", Washington, D.C., May 2002. http://travel.state.gov/visa/laws/telegrams/telegrams_1403.html

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

van den Ende, Jan, "The Number Factory: Punched-Card Machines at the Dutch Central Bureau of Statistics", *IEEE Annals of the History of Computing*, Vol. 16, No. 3, 1994, pp. 15-24.

van Dijk, Pieter, Fried van Hoof, Arjen van Rijn and Leo Zwaak (eds.), *Theory and Practise of the European Convention on Human Rights*, Intersentia, Antwerpen/Oxford, 2006, pp. 773-841.

van Lieshout, Marc, Luigi Grossi, Graziella Spinelli, Sandra Helmus, Linda Kool, Leo Pennings, Roel Stap, Thijs Veugen, Bram van der Waaij, and Claudio Borean, "RFID Technologies: Emerging Issues, Challenges and Policy Options", IPTS Technical Report Series EUR 22770 EN, Office for Official Publications of the European Communities, Luxembourg, 2007. http://ftp.jrc.es/EURdoc/eur22770en.pdf

Vance, Ashley and Brad Stone, "Palantir, the War on Terror's Secret Weapon," *Businessweek*, 22 November 2011. http://www.businessweek.com/magazine/palantir-the-vanguard-of-cyberterror-security-11222011.html

Verkaik, Robert, "Credit check giant Experian accused of 'ripping off' its customers", *DailyMail*, 30 January 2011. http://www.dailymail.co.uk/news/article-1351866/Credit-check-giant-Experian-accused-ripping-customers.html#ixzz1yzYgHgsY

Visiongain, *The Biometrics Market 2012-2022*, 19 September 2012. http://www.visiongain.com/Report/898/The-Biometrics-Market-2012-2022

Visiongain, *The Military Video Surveillance Systems Market 2012-2022: Full Motion Video for ISR*, 16 April 2012. http://www.marketresearch.com/Visiongain-v1531/Military-Video-Surveillance-Systems-Full-6917014/

Visiongain, *The Unmanned Ground Vehicles (UGV) Market 2012-2022*, 10 August 2012. http://www.visiongain.com/Report/870/The-Unmanned-Ground-Vehicles-(UGV)-Market-2012-2022

Vlcek, William, "Surveillance to combat terrorist financing in Europe: whose liberty, whose security?", *European Security*, Vol. 16, No. 1, 2007, pp. 99-119.

Vlcek, William. "A Leviathan Rejuvenated: Surveillance, Money Laundering, and the War on Terror", *International Journal of Politics, Culture and Society*, Vol. 20, No. 1-4, 2008, pp. 21-40.

Voas, R. B., P. M. Marques and R. Roth, "Interlocks for first offenders: Effective?" *Traffic Injury Prevention*, Vol. 8, 2007, pp. 346-352.

von Hirsch, A., and C. Shearing, "Exclusion from Public Space," in A. von Hirsch (eds.), *Ethical and Social Perspectives on Situational Crime Prevention*, Hart Publishing, Oxford, 2000.

von Lewinski, Kai, "Zur Geschichte von Privatsphäre und Datenschutz - eine rechtshistorische Perspektive", in Schmidt, Jan-Hinrik, and Thilo Weichert (eds.), *Datenschutz: Grundlagen, Entwicklungen und Kontroversen*, Bundeszentrale für politische Bildung, Bonn, 2012, pp. 23-33.

Wagstaff, Jeremy and Lee Chyen Yee, "ZTE Confirms Security Hole In U.S. Phone," *Reuters*, 18 May 2012. http://www.Reuters.Com/Article/2012/05/18/Us-Zte-Phone-Idusbre84h08j20120518

Walby, Kevin, "Little England? The rise of open-street Closed-Circuit Television surveillance in Canada", *Surveillance & Society*, 4 (1/2), 2006, pp. 29-51.

Ware, Willis H., *Records, Computers and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, The Rand Corporation, Santa Monica, 1973.

Warren, Samuel D. and Louis D. Brandeis, "The right to privacy", *Harvard Law Review*, Vol. 4, 1890, pp. 193-220.

Watson, B and K. Walsh, "The Road Safety Implications of Automatic Number Plate Recognition", Centre for Accident Research & Road Safety, Queensland, 2008. http://eprints.qut.edu.au/13222/

Watson, Philippa, "Equality of Treatment: A Variable Concept?", *Industrial Law Journal*, Vol. 24, No. 1, 1995, pp. 33-48.

Weber, Max, *The Protestant Ethic and the Spirit of Capitalism*, Allen and Unwin, 1956.

Weber, Max, *The Theory of Social and Economic Organization*, Free Press, New York, 1947.

Webster, C. William R., "CCTV Policy in the UK: Reconsidering the Evidence Base", *Surveillance and Socety*, Vol. 6, No. 1, 2009, pp. 10-22.

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., "Cyber society or surveillance society? Findings from a national survey on closed circuit television in the UK", in John Armitage, and Joanne Roberts (eds.), *Exploring Cyber Society: Social, Political and Cultural Issues, Proceedings of the Conference, Volume 2*, University of Northumbria, Newcastle UK, 1999.

Webster, C. William R., "Public Administration as Surveillance", in Kirstie Ball, Kevin D. Haggerty, and David Lyon (eds.), *Routledge Handbook of Surveillance Studies*, Routledge, London, 2011, pp. 313-320.
Webster, C. William R., "Smart CCTV", Paper presented at: 5th Conference Computers, Privacy and Data Protection (CPDP), Brussel, 25-27 January 2012, 2012.
Webster, C. William R., "The Diffusion, Regulation and Governance of Closed-Circuit Television in the UK", *Surveillance and Society*, Vol. 2, No. 2/3, 2004, pp. 230-250.
Webster, C. William R., "The Policy Process and Governance in the Information Age: The Case of Closed Circuit Television", Unpublished PhD Thesis, Caledonian University, Glasgow, 2004.
Webster, C. William R., and J. Hood, "Surveillance in the Community: Community Development Through the Use of Closed Circuit Television", in Leigh Keeble, and Brian Loader (eds.), *Community Informatics: Shaping Computer-Mediated Social Relations*, Routledge, London, 2001, pp. 220-239.
Webster, C. William R., Doina Balahur, Nils Zurawski, Kees Boersma, Bence Ságvári, and Christel Backman (eds.), *Living in Surveillance Societies: The Ghosts of Surveillance*, University of Iasi "Alexandru Ioan Cuza" Press, Iasi, 2012.
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.
Webster, William, "CCTV policy in the UK: reconsidering the evidence base", *Surveillance & Society*, Vol. 6, No. 1, 2009, pp. 10-22.
Weiss, Richard, "Siemens to Increase R&D Spending to Retain Competitive Edge" *Bloomberg*, 23 March 2012. http://www.bloomberg.com/news/2012-03-23/siemens-to-increase-r-d-spending-to-retain-competitive-edge.html
Welsh, Brandon C., and David P. Farrington, "Crime prevention effects of closed circuit television: A systematic review", Home Office Research Study, Home Office, London, 2002.
Wesselin, Mara, Louise Amoore and Marieke De Goede, "Datawars, Surveillance and SWIFT: Opening the Black Box of SWIFT", *Journal of Cultural Economy*, Vol. 5, No. 1, January 2012, pp. 49-66.
West, M. J. and M. J. Went, "Detection of drugs of abuse by Raman spectroscopy", *Drug Test Analysis*, 3, 2011, pp. 532–538.
Westin, Alan F., *Privacy and Freedom*, Atheneum, New York, 1967.
White, Robin C.A. and Clare Ovey (eds.), *The European Convention on Human Rights*, Oxford University Press, Oxford, 2010, pp. 425-475.
Whitman, James Q., "The Two Western Cultures of Privacy: Dignity Versus Liberty", *The Yale Law Journal*, Vol. 113, 2004, pp. 1151-1221.
Wilcox, Joe, "The Google Monopoly Begins", *eWeek Microsoft Watch*, 20 December 2007. http://www.microsoft-watch.com/content/web_services_browser/the_google_monopoly_begins.html
Williams M., "Better Facial Recognition Systems", *Technology Review*, 30 May 2007.
Williams, Christopher, "Contractors dodge ID cards axe", *The Register*, 27 May 2010. http://www.theregister.co.uk/2010/05/27/id_card_contracts/
Williams, Mark, "The Total Information Awareness Project Lives On", *MIT Technology Review*, 26 April 2006. http://www.technologyreview.com/news/405707/the-total-information-awareness-project-lives-on/
Williams, R. and P. Johnson "Circuits of surveillance", *Surveillance & Society*, Vol. 2, No. 1, 2004, pp. 1-14.
Williams, Raymond, *Culture and Materialism: Selected Essays.* London: Verso, 1980.
Williams, Raymond, *The Long Revolution.* Columbia University Press 1961.

Willis, C., S. Lybrand and N. Bellamy, “Alcohol ignition interlock programmes for reducing drink driving recidivism”, *Cochrane Database of Systematic Reviews*, Issue 3, Art. No.: CD004168, 2004.

Wilson, D., D. Weisburd and D. McClure, “Use of DNA testing in police investigative work for increasing offender identification, arrest, conviction, and case clearance”, *Campbell Systematic Reviews*, 7, 2011. https://www.ncjrs.gov/App/Publications/Abstract.aspx?id=258407

Wolfram, Gerd, Birgit Gampl, and Peter Gabriel (eds.), *The RFID Roadmap: The Next Steps for Europe*, Springer, Berlin, Heidelberg, 2008.

Woll, C., “Lectures: Gouverner par les instruments”, *Pôle Sud*, No. 23, May 2005, pp. 200-202.

Woolgar, Steve, *Virtual Society? Technology, Cyberbole, Society*, Oxford University Press, Oxford, 2002.

Wright, David, and Paul De Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012.

Wright, David, Michael Friedewald, Serge Gutwirth, Marc Langheinrich, Emilio Mordini, Didier Bigo, Rocco Bellanova, Kush Wadwa, and Sergio Carrera, "Sorting out smart surveillance", *Computer Law & Security Review*, Vol. 26, No. 4, 2010, pp. 343-354.

Wright, David, Serge Gutwirth, Michael Friedewald, Paul De Hert, Marc Langheinrich and Anna Moscibroda, “Privacy, trust and policy-making: Challenges and responses”, *Computer Law & Security Review*, 25, Elsevier, 2009, pp. 69-83.

Wright, Steve, “An Appraisal of Technologies of Political Control”, Working Document, European Parliament, Scientific and Technological Options Assessment STOA, Luxembourg, 1998.

Wright, Steve, “The ECHELON Trail: An Illegal Vision”, *Surveillance & Society*, Vol. 3, No. 2-3, 2005, pp. 198-215.

Xu, Guochang, *GPS: Theory, Algorithms and Applications*, Springer, Berlin, Heidelberg, New York, 2007.

Yates, JoAnne, “Early Interactions Between the Life Insurance and Computer Industries: The Prudential’s Edmund C. Berkeley”, *IEEE Annals of the History of Computing*, Vol. 19, No. 3, 1997, pp. 60-73.

Yates, P. “'Intelligent' Fingerprinting'”, *The Billboard Magazine*, Iss., 26, 2012, pp. 44-45

Yates, P., “Drug detection from fingerprints New technology tests drug metabolites in sweat”, *Royal Canadian Mounted Police Gazette*, Vol. 74, No. 1, 2012. http://www.intelligentfingerprinting.com/news/RCMPGazetteApril2012.pdf

Zarsky, Tal Z., “Mine Your Own Business!: Making the Case for the Implications of th Data Mining of Personal Information in the Forum of Public Opinion”, *Yale Journal of Law and Technology*, Vol. 5, 2003, pp. 1-56.

Zetter, Kim, “Google Asks NSA to Help Secure Its Network”, *Wired*, 4 February 2010. http://www.wired.com/threatlevel/2010/02/google-seeks-nsa-help/

Zetter, Kim, “Nokia-Siemens Spy Tools Aid Police Torture in Bahrain”, *Wired.com*, 23 August 2011. http://www.wired.com/threatlevel/2011/08/nokia-siemens-spy-systems/

Zuboff, Shoshana, *In the age of the smart machine: The future of work and power*, Basic Books, New York, 1988.

Zuurmond, Arre, “From bureaucracy to infocracy. Are democratic institutions lagging behind”, in I. Th. M. Snellen, and W. B. H. J. van de Donk (eds.), *Public administration in an information age: A handbook*, IOS Press, Amsterdam, 1998, pp. 259-271.

Zweig, David, and Jane Webster, "Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems", *Journal of Organizational Behavior*, Vol. 23, No. 5, 2002, pp. 605 – 633.

List of cases

ECtHR (1st sect.), *Stankov a.o. v. Bulgaria*, Application no. 29221/95, judgment of 2 October 2001.

ECtHR (2nd sect.), *Süheyla Aydin v. Turkey*, Application no. 25660/94, judgment of 24 May 2005.

ECtHR (GC), *Hasan & Chaush v. Bulgaria*, Application no. 30985/96, judgment of 26 October 2000.

ECtHR (GC), *Maestri v. Italy*, Application no. 39748/98, judgment of 17 February 2004, *Rep*. 1998.

ECtHR, *Adolf v. Austria*, Application no. 8269/78, Strasbourg, 26 March 1982.

ECtHR, *Allenet de Ribemont v. France*, Application no. 15175/89, Strasbourg, 10 February 1995.

ECtHR, *Asan Rushiti v. Austria*, Application no. 28389/95, Strasbourg, 21 March 2000.

ECtHR, *Barberà, Messegué and Jabardo v. Spain*, Application no. 10590/83, Strasbourg, 6 December 1988.

ECtHR, *Ezelin v. France*, Application no. 11800/85, judgment of 26 April 1991, *Ser*. A, vol. 202-A.

ECtHR, *Funke v. France*, Application no. 10828/84, Strasbourg, 25 February 1993.

ECtHR, *Lutz v. Federal Republic of Germany*, Application no. 9912/82, Strasbourg, 25 August 1987.

ECtHR, *Minelli v. Switzerland*, Application no. 8660/79, Strasbourg, 25 March 1983.

ECtHR, *Niemietz v. Germany*, Application no. *13710/88* (1992) Series A no 251.

ECtHR, *Plattform Ärzte für das Leben! v. Austria*, Application no. 10126/82, judgment of 21 June 1988.

ECtHR, *S. and Marper v. United Kingdom*, Application nos. 30562/04 and 30566/04, Strasbourg, 4 December 2008.

ECtHR, *Saunders v. United Kingdom*, Application no. 19187/91, Strasbourg, 17 December 1996.

ECtHR, *Sekanina v. Austria*, Application no. 13126/87, Strasbourg, 25 August 1993.

Human Rights Committee, *Berry v. Jamaica*, Communication No. 330/1988, U.N. Doc. CCPR/C/50/D/330/1988 (1994).

State v. Steffen, 230 N.W. 536 (Iowa 1930) (USA).

USA v. ADT Security Sevices Inc, United States District Court Southern District of Florida, Case 9:07-cv-81051-WJZ, Federal Trade Commission. http://www.ftc.gov/os/caselist/0423091/071120adtorder.pdf

USA v. Eric Robert Rudolph, CR 00-S-0422-S, 2005. http://www.alnd.uscourts.gov/rudolph/PleaAgreement.pdf

USA v. Patrick Leroy Crisp, No. 01-4953, 2003. http://bulk.resource.org/courts.gov/c/F3/324/324.F3d.261.01-4953.html

9 ANNEXES

ANNEX 1 – COMPREHENSIVE LIST OF SURVEILLANCE COMPANIES

Country (HQ)	Name of company	Focus/specialisation
Austria	CogVis	Image processing software for live-video streams
Austria	Schiebel Corporation	Aerial surveillance - unmanned air systems
Belgium	A&E Security NV (member of Connex group)	Access control, surveillance cameras
Belgium	Traficon N.V.	Video content analysis
Brazil	Suntech Intelligence	Communications interception
Canada	Gens Software Ltd.	Iris recognition and biometric authentication application development.
Canada	AdvancedIO	Defence (radar systems, signal intelligence, cyber security); Financial (Ultra Low Latency Trading, Risk Management Controls, Market Data Capture, Latency measurements), Telecommunications (network performance and network security)
Canada	Diamond Aircraft	Aircraft manufacturing; aircrafts for surveillance
Canada	Genetec Inc	Video surveillance
Canada	March Networks Corp	High definition Video surveillance
Canada	Sandvine Incorporated	Network management/ intelligence solutions
Canada	Vineyard Networks	Internet surveillance - deep packet inspection
Canada	S.I.C Biometrics Inc	Biometric fingerprint readers, biometric proximity cards and access control solutions for commercial and government markets
Canada	EXFO NetHawk	2G/3G IMSI catching solution for mobile operations (pedestrian, vehicle, aircraft) and fixed installations (prisons)
Canada	Seon Design	Mobile video surveillance specifically for the school and transit bus and coach industries.
China	Huawei Technologies	Cloud,spanning applications & services, storage & security, and O&M.
China	Shanghai Huayuan Electronic Co.,Ltd	RFID

China	Vixtel	E2E NGN Monitoring, NGN/VoIP Lawful Interception; Mobile Packet Service Analysis and Optimization
China	ZTE Corp	Telecommunications equipment and network solutions
Colombia	Asoto Technology Group	Digital Forensics, Data Recovery and Computer Security.
Czech republic	Inveatech	Programmable hardware (FPGA technology)for security and monitoring of high-speed network applications.
Czech Republic	Phonexia	Speech record data mining
Denmark	Guardia A/S	Biometric security technology -3D and infrared face recognition system.
Denmark	Milestone Systems A/S	Video surveillance
Denmark	Napatech	Intelligent Real-time Network Analysis from 1 GbE to 40 GbE and beyond
Denmark	Spectronic Systems A/S	Packet based interception for law enforcement agencies.
Estonia	Cybernetica	Integrated surveillance systems for border security applications and e-customs solution for Customs Authorities/Original equipment manufacturer and solutions provider active in the field of Information and Communication Technologies
Finland	Mirasys Ltd	Video surveillance
France	Alcatel-Lucent	Mobile, fixed, IP and optics technologies
France	Amesys (Bull)	Design and integration of critical high-tech systems, hardened embedded systems, management information systems, signal processing, Automatism, Control command
France	AQSACOM	Lawful interception - IP Interception, Wireless roaming and tracking
France	Eseco Systems	Web3 solutions for wireless security and video surveillance
France	Evitech	Intelligent video surveillance
France	Oberthur Technologies	Smart card technology

France	Qosmos	Deep Packet Inspection and Network Intelligence technology that provides unprecedented real-time visibility into data traffic.
France	SAFRAN Morpho (previously Sagem Securite)	Identification and detection systems - e.g. AFIS (Automated Fingerprint Identification System), smart cards, trace equipment
France	Scan & Target	Real time web and mobile text content analysis for government agencies, service publishers, marketing agencies, e-commerce sites and media & advertising networks.
France	Sogeti (subsidiary of Capgemini Group)	Security solutions
France	Thales	Integrated border security systems, aviation safety devices and identification tools.
France	UVS International	Unmanned vehicle systems
France	Vupen Security	Defensive and offensive cyber security intelligence and advanced vulnerability research.
France	ATOS SA (formerly ATOS Origin)	Homeland security, identity management and border control
Germany	Microdrones	Aerial surveillance
Germany	Cassidian *(defence and security subsidiary of the EADS group)*	Various security solutions - unmanned air systems, coastal surveillance systems, intelligence, mobile data applications.
Germany	Utimaco Safeware AG *(member of the Sophos group)*	Lawful interception and monitoring (LIMS) systems for mobile and fixed network operators and Internet service providers.
Germany	PSI Transcom GmbH	Control systems for public safety, environmental protection and emergency management
Germany	AGT Germany	Critical asset and urban security; urban management and anti-crime intelligence
Germany	AHB Electronic GmbH	Access control, video surveillance
Germany	Alarm	Security and monitoring equipment - keyloggers, screenshot monitoring, CCTV, GPS, audio montioring, mini transmitters, counter surveillance (protection against eavesdropping technology)
Germany	ATIS systems GmbH (ATIS UHER	High-Tech Communications Interception and voice recording

Germany	Bosch Security Systems	Video surveillance systems incl. video over IP and intelligent video analysis, intrusion detection systems, Access control systems
Germany	CanControls	Forward-looking human-machine interfaces, real-time image processing and video-based scene analysis
Germany	Cognitec Systems GmbH	Face recognition technologies (facial database search, video screening, border control, ICAO compliant photo capturing and facial image quality assessment)
Germany	DATAKOM GmbH	Network analysis, security
Germany	EBS Electronic	Assembly of electronic components (SMT, THT) and manual assembly equipment
Germany	ELAMAN GmbH	Governmental security solutions (lawful surveillance) -Audio/Video observation equipment, Geographical Information Systems, Tracking, Counter surveillance, Mobile and strategic Command Control Centers, Intelligence Fusion System
Germany	Ipoque ***(a Rohde & Schwarz company)***	Deep packet inspection solutions for Internet traffic optimization, policy enforcement & network visibility
Germany	MEDAV GmbH	Signal processing, pattern recognition and information technology
Germany	Mobotix AG	Video surveillance
Germany	OHB-System AG (subsidiary of the OHB Group)	Satellite based surveillance
Germany	Rohde & Schwartz	Radio monitoring, signal intelligence, satellite monitoring, spectrum monitoring etc
Germany	Siemens AG	Integrated surveillance system called Siveillance, a security solution integrating different surveillance solutions (like video intelligence analysis and surveillance)
Germany	Syborg	Recording and analysis of voice and data - interception services
Germany	InnoTec DATA GmbH & Co. KG	Video surveillance
Germany	Private Investigator Detektei Stern	Private investigation and surveillance in Germany.

Germany	Trovicor	Communications interception in fixed and mobile networks to next generation networking and Internet. Applications - location tracking, speaker recognition, language identification & link analysis
Greece	Teotec S.A.	RF Communications, Wireless Networks - Sensors, Broadband, IT, Long Range Active RFID, Passive RFID, RFID Middleware, Security, Video Surveillance, MEgapixel Cameras, Video Content Analytics, Training Systems
Hong Kong	Futronic Technology Co. Ltd	Advanced fingerprint recognition hardware and software products
Hungary	Neti Limited	Internet monitoring, mass surveillance [development of systems based on custom designed applications supporting analytic security solutions]
India	Septier Comunications	Lawful interception systems, cellular location determination infrastructure, fraud management applications and network surveillance products.
India	Cleartrail	Consultant and solution provider for Law Enforcement and Intelligence Agencies. ClearTrail solutions enable the LEAs to perform mass, targeted and tactical monitoring and analysis across a variety of communication networks
India	Fusion Biometrics India	Fingerprint technology, biometric technologies
India	Ircon	Signalling/telecoms
India	Shoghi Communications	Electronic Sensor Systems, Communication Intelligence and Information Processing Systems, Jamming Systems for Radio Operated IED, Signal Processing and Data Acquisition Systems, High Resolution Processed Satellite Imagery, Military Grade Encryption, Network Security Systems, Integrated Logistics and Support Services.
India	Private Eye (P) Ltd	Shadowing and Surveillance;Pre and Post Employment Verification;
India	SecureMantra Technologies (P) Ltd	Biometrics - AFIS
India	Bharat Electronics Limited (BEL)	Communications surveillance, radar surveillance, thermal imaging

Ireland	Vigitrust	Cloud based security assessments and learning solutions for organizations namely, PCI DSS, HIPPA, Critical Infrastructure Protection and Data Protection.
Israel	Ability	Satellite and cellular monitoring business
Israel	Agent video intelligence Inc	Open architecture, video analytics software deployed in a variety of security, safety and business intelligence applications worldwide.
Israel	Allot	Intelligent IP service optimization and revenue generation solutions for fixed and mobile service providers and high-end enterprise - IP traffic inspection, classification and policy enforcement
Israel	Amdocs Ltd	Data analytics
Israel	Cellebrite *(fully-owned subsidiary of the Sun Corporation, a listed Japanese company)*	Mobile forensics - extraction and analysis of evidentiary data from mobile phones and GPS devices for military, law enforcement, and government agencies
Israel	Elkat	Intelligence gathering (communications, visual and human); Electronic Protection Against Intelligence Gathering (e.g. jamming, encryption, debugging)
Israel	Elta systems *(subsidiary of Israel Aerospace Industries)*	Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR), Early Warning and Control, Homeland Security (HLS), Self-Protection and Self-Defense, and Fire Control applications - Unmanned air vehicles (UAV), Satellites, ground stations and space launchers Navigation systems, EO payloads, communications and many other technologies, products and services.
Israel	Gita Technologies	Security, encryption and networking
Israel	Nice Systems	NICE solutions capture interactions, transactions and video surveillance from multiple sources, including telephones, CCTV video feed, emergency services radio communications, emails, chat, social media etc.
Israel	Semptian Technologies	Internet Monitoring/Mass surveillance
Israel	TraceSpan	Broadband monitoring solutions; performance analysis and information monitoring
Israel	Elbit Systems	Computer surveillance
Italy	3I Security International SRL	Electronic security products

Italy	A.E.P., SRL	Design and production of equipment and software for Electronic Ticketing System
Italy	Alfacod SRL	Automatic identification and data capture
Italy	BEA (part of Cross Security Group)	Research, production and diffusion of microelectronics products for security
Italy	Expert System Semantic Intelligence	Semantic software, which discovers, classifies and interprets text information.
Italy	Eye-Tech	Automatic video surveillance and computer vision to detect anomalous behaviours, notify suspicious or dangerous events, localize and recognize faces, classify patterns.
Italy	infoFACTORY	Web intelligence, social media monitoring
Italy	Finmeccanica	Aerospace, defence and security
Italy	Hacking team	Remote Control System (RCS) designed to evade encryption
Italy	IMAVIS Srl	Video surveillance - megapixel cameras, License plates reading, Face detection and Video CMS
Italy	Innova	Internet Monitoring/Mass surveillance, SMS Monitoring
Italy	IPS SpA *(subsidiary of the RESI Group)*	Lawful interception, Cyber investigation, Intelligent Analysis, Monitoring centers, Electronic Surveillance (Audio, Video and Data Monitoring, Critical infrastructure security)
Italy	Loquendo S.p.A *(acquired by Nuance Communications, Inc)*	Speech Analysis/Voice Recognition
Italy	RCS S.p.A.	Internet Monitoring/Mass surveillance
Italy	RESI group *(includes five companies RESI, IPS SpA, Smetana, Italia-Mobile and Opto Electronics)*	Internet Monitoring/Mass surveillance, Analytics
Italy	Sympas S.r.l.	Research, development and consulting in the field of radar and surveillance systems
Japan	Aiphone Co. Ltd.	General Intercom Devices, Security Intercom Devices, Video door intercoms, Health Care Intercom Devices, Information Transmission Devices
Japan	Canon Inc	Visual surveillance
Jordan	Silat Solutions (part of Protei Telecommunications of Russia)	Telecommunications -Remote monitoring, intelligent network analysis

Kenya	Absolute Security Ltd.	CCTV, Access Control Systems, I.P Networks, Electric Fences etc.
Lithuania	Neurotechnology	Algorithms and software development products for biometric fingerprint, face, iris, voice and palm print recognition, computer-based vision and object recognition to security companies, system integrators and hardware manufacturers
Mexico	C3 Technology S.A. De C.V.	Video surveillance with biometric facial identification
Netherlands	Fox-IT	Security and intelligence solutions for government bodies and other major organisations
Netherlands	Group 2000	Network forensics (interception solutions, data retention, LIMA platforms, deep packet inspection etc)
Netherlands	Pine Digital Security	Interception of digital traffic
Netherlands	EADS NV	Development, manufacturing, marketing and sale of satellites, orbital infrastructures and launchers; development, manufacturing, marketing and sale of missiles systems, military combat aircraft and training aircraft; provision of defence electronics and of global security market solutions such as integrated systems for global border security and secure communications solutions and logistics etc
Netherlands	Smartrac Technology	Developer, manufacturer and supplier of RFID applications
Netherlands	GenKey	Biometric id system - biometric Identity Cards, Machine Readible Travel Documents, Biometric Registration Systems, Biometric Payment systems, Match-on-Card etc.
New Zealand	Endace	Network monitoring and recording solutions e.g. packet sniffers,
New Zealand	Security Software International	Lawful interception of telecommunications
Poland	Marco system	Intercpetion and analysis of data transmitted across diverse communication channels including voice, video and Internet.
Qatar	Al Kawther Security Systems	Covert surveillance /CCTV

Republic of Ireland	Eirsec	CCTV cameras, DVR Recorders CCTV Accessories, Wireless Surveillance Covert cameras. Tools and Accessories. CCTV Remote access configuration. Distributers of CCTV equipment.
Romania	Seektron S.R.L.	Integrated solutions/systems for surveillance and monitoring of small and medium areas (surfaces) and critical infrastructure objectives
Romania	Amplusnet	Cyclope Employee Monitoring Software
Russia	BioLink	Biometric identification and authentication solutions for civil identification, access control and information security applications
Russia	Oxygen Software	Software development for managing information, data and settings of mobile phones and smartphones; smart forensics
Russia	Protei	Messaging solutions; Intelligent Network & VAS; NGN; Roaming Solutions; Customer Care; AAA & Policy Control;Transport Solutions; Traffic Management
Russia	Speech Technology Center, Ltd.	Audio forensics; voice biometrics; audio recording (covert speech recording)
Singapore	Zycraft	Nanotech coastal surveillance
Slovakia	Innovatrics	Fingerprints software - real-time 1:N identification and 1:1 verification applications running in multi-server, PC or mobile environments in both government and private sector.
Slovenia	Navkom	Biometric devices for access control, logical access
Slovenia	New Order	Computer, internet and networking security
South Africa	Seartech	Design and manufacture of tactical surveillance equipment
South Africa	Vastech Africa (Pty) Limited	Network recording, passive surveillance solutions
Spain	Agnitio	Voice biometrics technology for identification, surveillance and precise ID verification
Spain	INDRA SISTEMAS, S.A.	GIS Software; Airborne intelligence systems;Electronic surveillance measures (ESM) and alert systems ;Intelligence and tactical electronic war systems; radar systems etc

Spain	VICOMTECH	Content monitoring
Spain	Avalon Biometrics Ltd	Biometrics - systems integrator and solution provider - development of Homeland Security solutions, implementation and integration of large and/or complex projects in the international public security sector
Spain	Tecnobit, SLU	Maritime border surveillance/surveillance solutions for critical infrastructure protection
Sweden	ASSA ABLOY AB	Access control - intelligent lock and security
Sweden	Axis communications AB	Network video surveillance
Sweden	Ericsson	Mobile broadband. Security and Surveillance Proof of Concept application - connection of visual recognition and analytical systems in remote locations
Sweden	Speed Identity AB	Data capture and enrolment
Sweden	Securitas AB	Specialised guarding, mobile security services, monitoring and consulting and investigation services.
Sweden	Optimum Biometric Labs	Develops, markets, and sells BioUptime (a monitoring software for supervising infrastructure reliability, availability, maintainability, and performance)
Sweden	Precise Biometrics AB	Smart card technology/fingerprint recognition.
Sweden	Tobii	Eye tracking technology
Sweden	Research In Motion TAT AB *(previously The Astonishing Tribe)*	Facial recognition phone applications
Switzerland	AGT International	Military and national intelligence systems, industrial control systems and high-reliability communication systems.
Switzerland	Dreamlab technologies AG	High-end security test, consulting and education, solutions based on “best-in-class” open standard technologies
Switzerland	Neosoft AG	Social Network Monitoring and Analysis
Taiwan	ACTi	IP surveillance, focusing on multiple security surveillance market segments
Turkey	Inforcept networks	Network monitoring
UK	News Datacom Research Ltd *(subsidiary of News Corp; sought to be acquired by Cisco)*	Encryption technology; Internet Monitoring/Mass surveillance

UK	Audiotel International *(wholly owned subsidiary of PSG Solutions PLC)*	Technical surveillance countermeasures (TSCM) equipment for the effective detection of electronic eavesdropping devices or bugs
UK	Aurora Computer Services Ltd.	Face recognition technology
UK	Autonomy	Meaning-based technology, i.e. pattern matching. Extract meaning in real time from all forms of information, regardless of format, source, or language.
UK	BAE Systems	Global defence, aerospace and security
UK	Cobham	Development, delivery and support of advanced aerospace and defense systems for land, sea and air
UK	ComsTrac Ltd.	Professional surveillance and protection equipment for law enforcement agencies - communication intercept systems, for GSM Interception Systems, Passive GSM Interceptors, Hybrid Active GSM Interceptors, CDMA, Satellite, Computer and Standard Telephone Communications
UK	Creativity software	End-to-End LBS Solutions for Mobile Network Operators - deployer of commercial Location Based Service, “Find Your Child”.
UK	Cybula Ltd.	Pattern matching and data search systems. Diagnostics and Prognostics, based on the Signal Data Explorer technology and in Face Recognition, with the FaceEnforce system.
UK	Data Research Compliance Limited	Covert surveillance (desk, operatives based)
UK	Detica (part of BAE)	Data capture, storage, retrieval, management
UK	dunnhumby	Analysis and sale of online consumer data
UK	Experian	Data and analytical tools
UK	G4S Plc	Security solutions - Electronic tagging
UK	Gamma Group	Advanced technical surveillance, monitoring solutions, and advanced government training, as well as international consultancy for government intelligence departments and Law Enforcement Agencies
UK	Global CCTV Surveillance	Design, supply and installation of electronic security systems services

UK	Hidden Technology Systems International Ltd	Advanced tracking and surveillance equipment for Blue-Chip corporations, law enforcement agencies, governmental and military organizations worldwide - e.g. GPS and RF Tracking, software, audio and visual
UK	IndigoVision Group Plc	Video surveillance
UK	Ipsotek	People and vehicle tracking; crowd management; intrusion detection etc
UK	Irisys	Design and manufacture of intelligent infrared products. Thermal Imaging, People Counting, Queue Management, Security.
UK	Lok8u	GPS/mobile phone triangulation
UK	Northrop Grumman Information Systems Europe	Unmanned systems, cybersecurity, C4ISR, and logistics
UK	OmniPerception Ltd.	Facial biometrics, video analytics and other advanced image processing and recognition applications
UK	Panoptech *(acquired by Bowmer & Kirkland and part of their Soncell Group)*	Network Design and Implementation, Command And Control Systems, Secure Network Monitoring and Maintenance, CCTV and Access Control, Video and Audio Streaming and Recording
UK	Sonic Communications *(part of Bowmer and Kirkland, Soncell Group)*	Design and manufacture of overt and covert communication and security systems for law enforcement, Ministry of Defence and Homeland Defence organisations across the world
UK	Panvista Limited	Software solutions for analysing digital images; video analytics for the surveillance industry
UK	QinetiQ Group plc	Remotely operated robots, unmanned aerial vehicles (UAVs), vehicle armour and sensor networks
UK	Quadnetics Group	Development and design of advanced surveillance technology and security networks
UK	Scyron	Intelligent surveillance and Digital Evidence Management
UK	Sensye (regd TM of BenQ Corp)	Eye tracking software

UK	SESP Group	Radio frequency jammer equipment, RF jammers, bomb jammers, radio jammers and frequency jamming devices. Other tactical observation solutions -medium altitude UAVs, tactical Rotor UAVs and thermal imaging surveillance systems
UK	Smart CCTV Ltd	Intelligent video systems and video analytics
UK	Smiths Detection	Security, notably airport X-ray systems
UK	Sophos	Antivirus, encryption, network, web and email; owns Utimaco LIMS.
UK	Telesoft Technologies	Security and Intelligence, Voice and video IVR, packet capture and analysis etc
UK	ThorpeGlen Ltd	Proactive monitoring, analysis, targeting and response capability for homeland security and organised crime
UK	ThruVision	Visual surveillance (concealed object detection systems)
UK	Global World Check	Finding risk hiding in business relationships and human networks- database screening, customer surveillance, market/trade surevillance, financial irregularity surveillance
UK	BiKal IP CCTV	Developers of IP Cameras to NVR and network surveillance software. IP Surveillance applications and solutions
UK	Flyonthewall	Wireless, infrared, and surveillance cameras and LCD TVs.
UK	Intelligent Protection International	Protective surveillance
UK	IView Cameras	CCTV cameras and equipment plus security systems for the home and small business including a wide range of surveillance equipment, CCTV, baby monitors and spy cameras
UK	Pakatak Security Equipment	Security equipment, surveillance monitoring, and spy cameras from the UK
UK	Remote Asset Management	GPS trackers
UK	RF Concepts	Suppliers of CCTV-Cameras and surveillance security systems.
UK	Blackbox Telematics	GPS vehicle, plant and personal tracking

UK	BlueSkyTracking	Personal and asset tracking devices for individuals, small businesses, private and government corporations
UK	Gap Year Trackers	On-line GPS tracker supplier specifically for gap year travellers, backpackers and adventure holidaymakers.
UK	Mainpage Computing	GIS Systems; GPS Tracking and data logging.
UK	RG Tech	Solar Powered and Wireless CCTV Remote and Rapid Deployment
UK	Xtag	Electronic monitoring systems
UK	UK Evidence	Private and commercial surveillance
UK	Somerdata	Audio surveillance and data communications solutions for police and other public security agencies in the UK and worldwide
UK	Synectics *(part of Quadnetics Group plc)*	Development and design of "e-surveillance" applications software and middleware for control and management of advanced CCTV and networked security systems.
UK	Raytheon UK *(aka Raytheon Systems Limited)*	Radar systems
UK	Cognesia *(formerly Intellitracker)*	Behavioural profiling, customer segmentation and targeted marketing
UK	Movirtu	Mobile Persona Management (MPM) solutions for wireless telecommunication service providers
UK	PredictiveIntent	Behavioural personalisation technology and services for digital businesses
UK	Siraview Imaging Solutions *(part of Sira Defence & Security Ltd- a Volvere Plc Group company)*	CCTV imaging solutions -developing products to help the police use CCTV effectively
UK	Classwatch	Fixed and mobile video systems - school surveillance
UK	Darnbro	RFID (wearable) - schools
UK	BioStore Limited	Secure card and biometric systems for public sector and commercial organisations
UK	CCTV Anywhere	CCTV
UK	MicroLibrarian Systems	Biometric fingerprint recognition
UK	Alterian (acquired by SDL)	Social media monitoring; web analytics
UK	Roke Manor Research Limited *(wholly owned subsidiary of the Chemring Group plc)*	Radar solutions for UAVs and aerial targets; electronic surveillance products for sigbal intercept, analysis and geolocation

Ukraine	Altron	Multichannel digital audio information recording complexes "AMUR"; Multichannel warning systems "ATRIS"; Video surveillance and access control systems; Information protection systems; Complex safety solutions
US	Selling Source	Digital marketing
USA	IP Fabrics	Intelligent network surveillance systems for 1Gbps and 10Gbps networks, designed for use in distributed data retention and lawful intercept solutions
USA	MorphoTrust USA *(previously L-1 Identity Solutions (acquired by SAFRAN Group)*	2D/3D-face recognition, multi-biometrics, video surveillance, border and access control
USA	Access data	Computer forensic technology
USA	Acxiom	Consumer data and analytics, databases, data integration and consulting solutions
USA	ADT Security Services (part of Tyco International)	Home and business security - intrusion detection, fire detection, video surveillance, access control, critical condition monitoring, health and elder care monitoring, electronic article surveillance, RFID and integrated systems.
USA	Arecont Vision LLC	Video surveillance - megapixel IP video
USA	ATCI	End-to-end systems integration and technical services, particularly satellite surveillance
USA	BIO-key International, Inc.	Fingerprint identification solutions
USA	Bivio	Cyber security, continuous monitoring and deep packet inspection handling platforms
USA	Bluecoat	Hardware proxy appliances for corporate networks offering web caching, virus scanning, content filtering, instant messaging control and bandwidth management.
USA	Brightplanet	Harvesting high quality content from inaccessible Deep Web and Surface Web sources
USA	Broadsoft	VoIP communication services
USA	Cernium Corp.	Video analytics
USA	ChoicePoint (purchased by Reed Elsevier)	Unique data and advanced scoring analytics

USA	Comverse	Software and systems enabling value-added services for voice, messaging, mobile Internet and mobile advertising; converged billing and active customer management; and IP communications.
USA	Cubic Corp.	Defense systems, mission support services and transportation systems. Cyber technologies, asset visibility solutions, and defense electronics
USA	DoubleClick *(Google subsidiary)*	Ad management and ad serving; cookie based user tracking
USA	Envysion Inc	Video driven business intelligence through Managed Video as a Service (MVaaS) model
USA	Dow Jones Factiva	Business intelligence
USA	FBI	Biometrics (fingerprint authentication)
USA	FircoSoft	Watch list filtering solutions for financial institutions and corporates
USA	Firetide Inc.	Video surveillance
USA	Fluke	Remote infrared non-contact scanning; thermal imaging
USA	Actimize *(acquired Fortent)*	Statistical-based AML and Know Your Customer (KYC) technology for top-tier financial institutions. Trading surveillance.
Netherlands	Gemalto	Digital security, smart cards, banking cards, ePassports, eID cards, tokens and other devices
USA	Glimmerglass	Cyber Security, Lawful Interception, Intelligence, and Telecom network monitoring
USA	Google	Video surveillance (streetview); online behavioural surveillance (new policy, gaming profiling); marine surveillance.
USA	Guidance Software	E-discovery and digital investigations
USA	Harris	Communications technology, products and networks for both government and commercial markets - e.g. intelligence, surveillance and reconnaisance
USA	Honeywell International Inc	Biometrics, video analytics, UAV's, remote home monitoring, wireless sensing etc.
USA	HP	IP video surveillance

USA	i2 *(acquired by IBM and now called IBM i2)*	Empowering government agencies and private sector businesses to investigate, predict, disrupt and defeat criminal and terrorist activities
USA	IBM	Intelligence network
USA	Lexis-Nexis	Smart screening technology, data analytics solutions
USA	ManTech International Corporation	Technology solutions in information systems, environment, telecommunications, defense, and aeronautics
USA	Meganet	FIPS level security solutions for government, military & corporate organisations to protect data, communications & physical assets (cell phone interception, spy phones, laptops,
USA	Narus *(subsidiary of Boeing)*	Dynamic network traffic intelligence and analytics.
USA	Net optics	Access and Monitoring Architecture - e.g. deep packet inspection
USA	Netezza *(An IBM company)*	Data warehouse appliance leader, combining storage, processing, database and analytics into a single system
USA	NetQuest	Variety of products and services for the collection and processing of online data, also known as online fieldwork.
USA	Ntrepid *(subsidiary of Cubic Corporation)*	Persona Management software
USA	Objectvideo Inc	Video surveillance for security, public safety, business intelligence, process improvement, and other applications
USA	Wildpackets Inc.	Network, application performance, and protocol analysis, VoIP monitoring, and troubleshooting solutions.
USA	Oracle data profiling (Oracle)	Data investigation and quality monitoring tool permitting business users to assess the quality of their data through metrics
USA	Packet Forensics	Network surveillance solutions for Enterprises, Network Operators, Law Enforcement, Defense & Intelligence
USA	Palantir	Analytics platforms for financial and intelligence clients
USA	Panasonic Corp.	Video surveillance
USA	Path Technologies	Mobile phone tracking; information technology services to support federal agencies and commercial clients

USA	Pelco Inc	Design, development and manufacture of video and security systems and equipment ideal for any industry
USA	Pen Link	Data intercept and surveillance equipment
USA	Pivot3 Inc.	High-capacity video surveillance
USA	Polaris Wireless	Software based location systems for wireless operators and LEA's (note its OmniLocate location surveillance product suite)
USA	RainStor	Big Data management and analytics
USA	Rapiscan Systems	Manufacturer of security equipment and systems designed for checkpoints, cargo, vehicle, baggage, parcel, and air cargo security inspection.[Bodyscan technology]
USA	Raytek	Remote infrared non-contact scanning
USA	Smartvue Corp	Video surveillance, Web-based Linux surveillance appliances
USA	Sonus Networks	Session Border Controllers, VOIP based solutions
USA	Surveon Technology Inc	End-to-end network video surveillance solutions
USA	Trapwire Inc	Predictive software system designed to detect patterns indicative of terrorist attacks or criminal operations
USA	United Technologies Corp	Video surveillance
USA	Verint	Intelligence® solutions and services for enterprise and security intelligence
USA	Visual Analytics (VAI)	Software solutions for accessing, sharing, analyzing, and reporting on data across any domain. [visual data mining, analytics and pattern discovery]
USA	Walmart	Data mining
USA	Washington Group International, Inc. (*acquired by URS Corp)*	Integrated homeland security solutions
USA	WatchGuard	Network and content security solutions to provide defense in depth for corporate content, networks and businesses.[Police incar video surveillance]
USA	InterAct Public Safety Systems	Public safety incident response and management software
USA	ContentWatch (Net nanny)	Parental controls software
USA	Academi *(formerly Xe Services LLC, Blackwater USA and Blackwater Worldwide)*	Military intelligence & security [training and security solutions provider serving government and commercial industries worldwide]

USA	DynCorp	US Government services provider delivering support solutions for defense, diplomacy, and international development. Intelligence solutions, Biometric Identification Systems, intelligence Collection and Analysis etc.
USA	United Technologies Corporation (UTC)	Aviation security
USA	Lockheed Martin	U-2 and SR-71 spy planes, F-16, F/A-22 fighter jet, and Javelin missiles. World's leading military contractor and largest arms exporter
USA	Boeing	Commercial jetliners and military aircraft combined, rotorcraft, electronic and defense systems, missiles, satellites, launch vehicles and advanced information and communication systems
USA	Science Applications International Corporation - SAIC	Satelllite, geospatial surveillance, computer surveillance, data mining; etc
USA	Northrop Grumman	Design, build and refuel of nuclear-powered aircraft carriers; jamming devices
USA	Theia Technologies	Visual surveillance
USA	Cisco Systems	Video surveillance software solutions
USA	Owlstone Nanotech	Nanotech surveillance -detection of chemical warfare agents and explosives.
USA	US Investigations Services - USIS *(owned by Altegrity)*	Background screening and risk management solutions
USA	Altegrity	Background investigations for the US government; supplier of on-demand employment background screening for corporates.
USA	Telestrategies	Producer of telecommunications conference (surveillance) events; consulting and specialized education services on the subjects of telecom technologies, billing & OSS, intelligence support systems and product strategy.
USA	T3TECHSYSTEMS	Covert video products
USA	BreakingPoint	Global threat and application intelligence - cyber
USA	Nuance	Voice biometrics

USA	ReTel Technologies	Consumer surveillance - hybrid video auditing solutions. Raw surveillance video into interactive, at-a-glance reports. Surveillance Auditing Solutions for Business Intelligence & Enhanced Security
USA	TRIPwire	Internet surveillance (chat room and website monitoring)
USA	Pictometry	Visual surveillance
USA	Dedicated Micros Inc.	Video surveillance
USA	360 Surveillance, Inc.	IP/analog video surveillance
USA	Anixter	Global supplier of communications and security products, electrical and electronic wire and cable, fasteners and other small components
USA	BrickHouse Security	Security and surveillance solutions - GPS Trackers, Hidden Cameras, PC and Cell Phone Monitoring solutions and Video Surveillance tools
USA	3M Cogent	Biometric identification solutions for governments, law enforcement agencies, and commercial enterprises.
USA	Facebook	Social media application facilitating individual tracking and monitoring; face recognition, integrating forms of surveillance
USA	Textron	Defence, aerospace. Drones technology - sea drones.
USA	Monetate	Targetted advertising
USA	MyBuys	Predictive advertising
USA	BlueCava	User device identification and matching despite cookie erosion, system upgrades, or changes in settings; aggregation of online and offline data
USA	33Across	Technology, tools, and real-time predictive systems. SocialDNA™ Targeting.
USA	Media6Degrees	Marketing technology
USA	SpectorSoft	Employee surveillance solutions
USA	UniView Technologies (owned by Bain Capital)	Infrared antiriot cameras and software that enable police officials in different jurisdictions to share images in real time through the Internet
USA	Sierra Nevada Corporation (SNC)	Systems integration and electronic systems provider (Vigilant Stare, a manned aircraft-based Wide-Area Persistent Surveillance concept demonstrator for commercial use)

USA	ITT Exelis	Aerospace, defense and information solutions company. Collborates with Sierra Nevada Corp to implement the Vigilant Stare.
USA	Datalogix	Purchase-based audience targeting
USA	Jumptap	Targeted mobile advertising
USA	Aggregate Knowledge	Media intelligence and predictive analytics
USA	Commerce Sciences	Behavioural analytics, predictive analysis
USA	MicroPower Technologies Inc.,	Surveillance solutions optimized for rapid, cost-effective deployment;Helios video surveillance system.
USA	L-3 Communications Corp	Visual (imaging scanners)/Command, Control and Communications, Intelligence, Surveillance and Reconnaissance (C^3ISR), Government Services, Aircraft Modernization and Maintenance (AM&M)
USA	Radisys	Embedded wireless infrastructure solutions for telecom, aerospace & defense and public safety applications.
USA	SS8	Communications intercept and regulatory compliant, electronic intercept and surveillance solutions.
USA	Phorm	Global personalisation technology company - online user surveillance
USA	Innovative Security Designs	IP surveillance solutions

ANNEX 2 – SHORTLISTED SAMPLE OF SURVEILLANCE COMPANIES

Organisation	Country - HQ	Focus	Area of operations	Number of employees	Annual turnover (2011 or 2010)	Customers/ clients	Partners	EU research involvement (parti. Security)
3M Cogent Inc.	USA	Biometric identification solutions provider to governments, law enforcement agencies, and commercial enterprises worldwide	Global (65 countries)	3M employed 84,198 people	$3821 million	Governments, law enforcement agencies and commercial enterprises.	Siemens, Lockheed Martin, Fujitsu, HP, Oracle, IBM, Unisys, Sun, Raytheon, EDS, Bull, SAIC, Sierra, Steria, ST Engineering, PCCW, Informix, CSC, Accenture, Validity, Hirsch Identive, Intermec, DataWorks Plus, Northrop Grumman, Simply Biometrics, Intercede, Keyscan, BlackBerry, and Rockwell Automaton.	• Minutiae template interoperability testing (MTIT) -FP6-IST • European Global Border Environment (GLOBE) -FP7-SECURITY
Acxiom Corporation	USA	Consumer data and analytics, databases, data integration and consulting solutions	Global (United States, Europe, Asia and South America)	6,175 employees (associates)	$ 1.131 billion (2012)	Varied - commercial, government, non-profit	Media partners – Yahoo!, PrescisionDemand, AT&T AdWorks, BlueKai, Datalogix, Jumptap, Selling Source and TiVo. Technology partners – HP, IBM, NetApp, Affinity Solutions,	Not found

							Aggregate Knowledge, Alterian, IBM Unica, Zoot, Cisco. Data partners – BigInsight.com, ThinkVine.	
ADT Security Services (part of Tyco International)	Switzerland	Home and business security -intrusion detection, fire detection, video surveillance, access control, critical condition monitoring, health and elder care monitoring, electronic article surveillance, radio frequency identification and integrated systems.	Global - North America, Central America, South America, Europe, Middle East, Asia-Pacific and South Africa	102,000	$8.6 billion (Tyco security services)	Residential, commercial, educational, governmental and industrial customers	Cisco, Motorola, Pelco, Honeywell, American Dynamics.	

AGT Group GmbH	Switzerland	Critical asset and urban security; urban management and anti-crime intelligence	Global	2,300	$ 1 billion	Primarily government	Research institutions such as SAP Research Center Darmstadt/Future Public Security Living Lab, CASED, Seeburger, T-Systems, KIT, Software AG, The Fraunhofer Institute for Secure Information Technology (SIT) and The Fraunhofer Institute for Computer Graphics (IGD).	Not found
Atos SA	France	Homeland security, spanning identity management and border control	Global	74,000	€8.5 billion (2011)	Multi-national groups and organizations and medium and small size companies	SAP; IBM; HP; EMC; Oracle; Microsoft; Siemens; Vmware, Thales; Airbus Military; Lockhead Martin; BAE Systems; Cassidian.	Extensive, including+I2 FI-WARE: Future Internet Core Platform; CASSANDRA, ASTUTE, SMART, TATOO, COOLEMALL, SECOECONOMICS (Socio-Economics meets Security); INTEG-RISK: Early VALUESEC, NESSOS

Audiotel International (wholly owned subsidiary of PSG Solutions PLC)	UK	Technical surveillance countermeasures (TSCM) equipment for the effective detection of electronic eavesdropping devices or bugs	Global (90 countries)	Data not found.	£4,093,905 (2011)	Government, law enforcement, corporate customers, high profile individuals	AudioSoft (data recording and analysis) and CEDAR Audio (R & D and implementation of audio restoration and speech enhancement systems).	Not found
BAE Systems Detica	UK	Data capture, storage, retrieval, management	Global (primary operations in UK, Denmark and Ireland)	2,000	£1,399 million (2011)	Government and commercial customers	BT, Arquiva, McAfee, RuleSpace, Kaspersky Lab, Cloudmark; Amper (sales); organisational partners - Internet Watch Foundation (IWF), Family Online Safety Institute (FOSI), Messaging Anti-Abuse Working Group (MAAWG), Internet Services Providers' Association (ISPA UK).	• Open Architecture for UAV-based Surveillance System (OPARUS) • Total Airport Security System (TASS) • Context-aware data-centric information sharing (CONSEQUENCE) • Automatic Detection of Abnormal Behaviour and Threats in crowded Spaces (ADABTS) • Strategic crime and immigration information management system (SCIIMS) - COORDINATOR

Boeing	USA	Largest manufacturer of commercial jetliners and military aircraft combined. Designs and manufactures rotorcraft, electronic and defense systems, missiles, satellites, launch vehicles and advanced information and communication systems	Global (150 countries)	61,988 (defence, space and security division) - total (171,692)	$68,735 million (2011)	Government and commercial	28,000 suppliers and partners across the world	Extensive, including: Protection of European seas and borders through the intelligent use of surveillance (PERSEUS), Unmanned Aerial Systems in European Airspace (ULTRA)
Bosch Security Systems GmbH	Germany	Video surveillance systems incl. video over IP and	Global (over 50 countries)	12,500	€ 1447 million (2011)	companies, institutions and governments	Construction planners, and major electronic	PANORAMA Project - Ultra Wide Context Aware Imaging;

		intelligent video analysis, intrusion detection systems and access control systems					equipment companies.	
Cassidian (defence and security subsidiary of the EADS group)	Germany	Various security solutions - unmanned air systems, coastal surveillance systems, intelligence, mobile data applications.	Global	28,000	€5.8 billion (2011)	Civil and military customers	Airbus; Astrium; Eurocopter (all integrated in EADS Company). Also shares in MBDA – the world leading missiles company. And Eurofighter GmbH – multinational company that co-ordinates the design, production and upgrade of the Eurofighter Typhoon aircraft. Participates with PERSEUS as technical leader, and with other companies such as AEROLIA, ATR, CILAS, PREMIUM AEROTEC, ROXEL, SODERN, SOGERMA	HELP: Enhanced Communications in Emergencies by Creating and Exploiting Synergies in Composite Radio Systems; DEMCARE: Dementia Ambient Care: Multi-Sensing Monitoring for Intelligent Remote Management and Decision Support; ACRIMAS: Aftermath Crisis Management System-of-systems Demonstration; DARIUS: Deployable SAR Integrated Chain with Unmanned Systems EULER: European software defined radio for wireless in joint security operations; DITSEF: Digital and innovative technologies for security and efficiency of first responders operation; VIRTUOSO: Versatile InfoRmation Toolkit for end-Users oriented Open

								Sources exploitation; PRACTICE: Preparedness and Resilience against CBRN Terrorism using Integrated Concepts and Equipment; EUROSUR: Sea Border Surveillance
Cognitec Systems GmbH	Germany	Face recognition technologies (facial database search, video screening, border control, ICAO compliant photo capturing and facial image quality assessment)	Global	45	Data not available	Government and industry	Industry and government	3D FACE
EADS NV	Netherlands	Development, manufacturing, marketing and sale of satellites, orbital infrastructures and launchers; development, manufacturing, marketing and sale of missiles systems, military combat aircraft and training aircraft; provision of defence electronics and of global security market solutions	Global	133,000	€ 49.128 million (2011)	Government agencies, law enforcement, military forces and major companies.	Large network of global partners.	Management System-of-systems Demonstration; AIRBorne information for Emergency situation Awareness and Monitoring (AIRBEAM);Security of critical infrastructures related to mass transportation (DEMASST);Digital and innovative technologies for security and efficiency of first responders operation (DITSEF); EUropean software defined radio

		such as integrated systems for global border security and secure communications solutions and logistics etc						for wireless in joint security operations(EULER); Open Architecture for UAV-based Surveillance System (OPARUS), Protection of European seas and borders through the intelligent use of surveillance (PERSEUS);Sea Border Surveillance (SeaBILLA); Preparedness and Resilience against CBRN Terrorism using Integrated Concepts and Equipment (PRACTICE)
Ericsson	Sweden	Mobile broadband. Security and Surveillance Proof of Concept application - connection of visual recognition and analytical systems in remote locations	Global	108,000	SEK 226,921 million	Government and commercial	Accenture, Alcatel-Lucent, Atos Origin, Bull, Capgemini, HP, IBM, Knot, Oracle, SAP Business Objects, StreamServe, Tech Mahindra	Converging and conflicting ethical values in the internal/external security continuum in Europe (INEX);

Experian	UK	Data and analytical tools	Global (over than 80 countries)	17,000	$ 4,485 million (year end 31 March 2012)	Public sector and industry	Local businesses and multinational corporations	• Geomarketing internet service for SMEs during Opengis (GISMO) - FP4-ESPRIT 4 (as participant) • Best practice Enhancers for Security in Urban Environments (BESECURE) (Experian Nederland BV – participant) - FP7-SECURITY
Finmeccanica S.p.A.	Italy	Aerospace, defence and security	Global	70,000	EUR 17,318 million	Government, commercial	Alenia North America Inc, BAE Systems, DCNS of France, EADS, L-3 IS (subsidiary of L-3 Communications), NHIndustries, and Thales.	Ten FP7 SECURITY and ICT projects. Also participates as Soluzioni Evolute per la Sistemistica e i Modelli S.c.a.r.l. (SESM) and Selex Elsag.
G4S Plc	UK	Security and safety solutions	Global (125 countries)	657,000	£7.5 billion (2011)	Local companies, governments and global corporations.	Governments, businesses and other organisations	Data not found.

Gemalto	Netherlands	Digital security;UICC and smart cards, banking cards, ePassports, eID cards, tokens and other devices	Global (over 190 countries)	10,000	€2,015 million (2011)	Government and commercial	Resellers, distributors and systems integrators	Various including:RESET (Roadmaps for European research on Smartcard Technologies); SecureChange (Security Engineering for Lifelong Evolvable Systems)

Google	USA	Video surveillance (streetview); online behavioural surveillance (new policy, gaming profiling); marine surveillance…	Global	32,467	$ 37,905 million (2011)	Government, commercial, personal	Unspecified	Google Ireland is/was involved in • Synergetic content creation and communication (SYNC3) - FP7-ICT • A unified framework for multimodal content SEARCH (I-SEARCH) - FP7-ICT+I15 • Policy Gadgets Mashing Underlying Group Knowledge in Web 2.0 Media (PADGETS) – FP7-ICT • Exploiting Social Networks for Building the Future Internet of Services (SOCIOS) – FP7-ICT • Reflecting Knowledge Diversity (RENDER) - FP7-ICT • Policy Formulation and Validation through non moderated crowdsourcing (NOMAD) - FP7-ICT

Honeywell International Inc	USA	Biometrics, video analytics, UAV's, remote home monitoring, wireless sensing etc.	Global (Americas, China, India, Asia Pacific and Europe, the Middle East and Africa.	132,000	$ 36.5 billion (2011)	Government and commercial	Technology and academic	Involved as Honeywell Technology Solutions (HTS) in 18 EU projects.
Indra Sistemas	Spain	Security technology and solutions (i.e border surveillance, protection of physical infrastructures; cybersecurity; Identification and biometrics; Information, investigation and intelligence)	Global (over 118 countries)	40000	EUR 2.688,5 million (2011)	Government and commercial	Various	Extensive e.g. Protection of European seas and borders through the intelligent use of surveillance (PERSEUS), Creation of a secure environment for e-Administration services and applications that enables user access via with an electronic ID card (SECURE ID), Securing the European electricity supply against malicious and accidental threats (SESAME)

Israel Aerospace Industries - IAI (and subsidiary Elta)	Israel	Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR), Early Warning and Control, Homeland Security (HLS), Self-Protection and Self-Defense, and Fire Control applications - Unmanned air vehicles (UAV), Satellites, ground stations and space launchers Upgrading of military aircraft and helicopters, Navigation systems, EO payloads, communications and many other technologies, products and services.	Global	16,000	$ 3.44 billion (2011)	Primarily government	Boeing, Elbit Systems, Aviation Technology Group Tadiran and Technion	Extensively involved in EU research projects with a total public funding amounting to €148.55 million (e.g. 2. Transportable autonomous patrol for land border surveillance (TALOS);3. Open Architecture for UAV-based Surveillance System (OPARUS);18. Smart Intelligent Aircraft Structures (SARISTU) - FP7-TRANSPORT

L-3 Communications Corp.	USA	Visual (imaging scanners)/Command, Control and Communications, Intelligence, Surveillance and Reconnaissance (C^3ISR), Government Services, Aircraft Modernization and Maintenance (AM&M)	Global	61,000	$ 15.2 billion (2011)	Government and commercial	Include: Hummingbird Ltd.,HP Software, iDirect, Imint, Infratherm, Innovative Micro Technology (IMT), Virginia Tech	None
Lok8U	UK	GPS/mobile phone triangulation. GPS locators, designed exclusively to address the adults and children at risk market and to provide personal and family safety.	USA, UK, France, Germany, South Africa, Czech Republic, Romania, Australia	Data not available	Data not available	Adults and children	National Silver Alert Inc, LifePROTEKT, T-Mobile	None

Microdrones GmbH	Germany	Aerial surveillance	Global	125	Data not available	DLR; EADS; ASTRIUM; Chinese Armed Police Forces; Norwegian Defence Research Establishment; Swedish National Police; universities and research institutions, meteorologists, and also military organisations	Industry and academic	None
Neurotechnology	Lithuania	Algorithms and software development products for biometric fingerprint, face, iris, voice and palm print recognition, computer-based vision and object recognition to security companies, system integrators and hardware manufacturers	Global	11 to 50	Data not available	Government and commercial	Various solutions partners.	None

NokiaSiemens Networks B.V. (NSN)	Finland	Mobile networks, government and public security - solutions for technical surveillance (sensors, CCTV), situational awareness (both network-wide and point-to-point), and command and control	Global	73,686	14,041 million euros	Government and commercial	Cisco, Juniper Networks, partners also in partners in Utilities, Transportation, Public Sector markets	Not found
Northrop Grumman Information Systems Europe	UK	Unmanned systems, cybersecurity, C4ISR, and logistics	Global	72,500	$ 26, 412 million	Mainly government. Also commercial.	EU partners include: British Telecommunications (BT), EADS, and Finmeccanica	None
Palantir	USA	Analytics platforms for premier financial and intelligence clients	Global	201-500 (unconfirmed)	$250 million (according to media estimates)	Government agencies, financial institutions and non-profit organisations.	Include Thomson Reuters, SAP, Capgemini, LMN Solutions, Objectivity Solutions, Inc.	None

QinetiQ Group plc	UK	Special areas of expertise include remotely operated robots, unmanned aerial vehicles (UAVs), vehicle armour and sensor networks.	Global (over 40 countries)	11,208	£1,702.6 million (2011)	Government and commercial	Industry and academic	Numerous FP7 projects - Strategic risk assessment and contingency planning in interconnected transport networks (STAR-TRANS) - FP7-SECURITY; Protection of Critical Infrastructures against High Power Microwave Threats (HIPOW) –FP7-SECURITY; Seamless communication for crisis management (SECRICOM) FP7-SECURITY;Semantically enhanced resilient and secure critical infrastructure services (SERSCIS) – FP7 ICT;xiv. Development of Pre-operational Services for Highly Innovative Maritime Surveillance Capabilities (DOLPHIN) - FP7-SPACE
Quadnetics Group plc (including Synetics and Quadrant Security Group)	UK	Development and design of advanced surveillance technology and security networks	North America, Europe, Asia, Middle East	450	£69.1 million. Synetics share was £37.6 million (2011)	Government and commercial	Various	None

Saab AB	Sweden	Commercial aeronautics, defence (air, land, naval), civil security solutions	Global	13,068	SEK 24,434 million (2011)	Government and commercial	Not found	EUropean software defined radio for wireless in joint security operations (EULER), Integrated mobile security kit (IMSK),Localization of threat substances in urban society (LOTUS), Protection of European seas and borders through the intelligent use of surveillance (PERSEUS)
Safran Morpho	France	Identification and detection systems - e.g. AFIS (Automated Fingerprint Identification System), smart cards, trace equipment	Global (over 100 countries)	7,500	Over F361.4 billion (2011)	Governments, national agencies and administrations dedicated to law enforcement and border control, private companies	UAE Ministry of the Interior, SELEX Elsag (framework agreement for cooperation in road enforcement and safety), SIM Dynamics (USSD-based SIM browser).	18 FP7 projects including ASSET, ARENA,CERSCENDO, ETTIS, FIDELITY, ETCETERA, EMPHASIS, EFFISEC, COPRA, HIDE, TACTICS.
Securitas AB	Sweden	Specialized guarding, mobile security services, monitoring and consulting and investigation services.	Global (except Oceania)	300,000	SEK 64,057 million (2011)	Government and commercial	Service partners such as Goingsoft for Internet security; media partners and research partners (universities).	Security UPgrade for PORTs (SUPPORT); MARS (Mobile Authentication using Retina Scanning, 2012-15).

Shoghi Communications	India	Electronic Sensor Systems, Communication Intelligence and Information Processing Systems, Jamming Systems for Radio Operated IED, Signal Processing and Data Acquisition Systems, High Resolution Processed Satellite Imagery, Military Grade Encryption, Network Security Systems, Integrated Logistics and Support Services.	Global	51-100 (unconfirmed)	$2.5 million - $5 million	Primarily, government (Military, defence forces and intelligence agencies of over seventy countries).	Sales partners in Europe, Asia, South Africa and South America	None

Siemens AG	Germany	Integrated surveillance system called Siveillance, a security solution integrating different surveillance solutions (like video intelligence analysis and surveillance)	Global	360,000	€73,515 million	Government and private	Has technology, sales and service delivery partners	Involved in FP7-SECURITY projects: European network for the security of control and real-time systems (ESCORTS), A Framework for electrical power sysTems vulnerability identification, dEfense and Restoration (AFTER), CRitical Infrastructure Security AnaLysIS (CRISALIS)
Smartrac NV	Netherlands	Developer, manufacturer and supplier of RFID applications	Global	4,000	€168 million (2011)	Government and commercial	Variety of industry collaborations and partnerships e.g. semiconductor and communication industry	Not found

Thales	France	Integrated border security systems, aviation safety devices and identification tools. • Airborne, ground and maritime surveillance	Global	Over 67,000	€ 13,214 million (2011)	Governments, intergovernmental organisations, large corporations.	NSN (secure communication), Elbit Israel (tactical systems of the 'Watchkeeper'), Oracle, Microsoft, IBM, Adobe, Airbus, Diehl etc	Security of critical infrastructures related to mass transportation (DEMASST), Efficient integrated security checkpoints(EFFISEC), EUropean software defined radio for wireless in joint security operations (EULER), Sea Border Surveillance (SeaBILLA)
Trovicor GmbH	Germany	Communications interception in fixed and mobile networks to next generation networking and Internet. Applications - location tracking, speaker recognition, language identification & link analysis	Global	170	Data not available	Government clients only	Data not available	Not found

ZTE Corp	China	Telecommunications equipment and network solutions	Global (140 countries)	89, 786	RMB 86.254 billion	International and Chinese clientele. International clients include Vodafone UK, Canadian Telus and Public Mobile, France Telecom.	Hi3G Sweden, Atos, British Telecommunications (BT), Telefonica, Telenor, Vodafone, Telus, France Telecom, Alcatel, Ericsson, France Telecom and Portugal Telecom.	None

ANNEX 3 – INDUSTRY ASSOCIATIONS

Industry association	Country	Area of operation	Focus/specialisation	Objectives, mission, values	Membership type/number of members	Code of conduct	Source of funding	Activities	Website
ADS Security Innovation and Technology Consortium (ADS SITC)	UK	Global	Innovative and technologically sophisticated security solutions	To promote security industry growth through greater exploitation of innovation and technology in security solutions.	Organisations (companies, institutions, partnerships, sole traders) operating in the information security, homeland security or related technology sector; those with a legitimate interest (as buyers, end users or experts) in developing innovative technology solutions in these sectors.	SITC Members' Obligations	Membership fees	Provide information about and for SITC members; business promotions; networking; sharing of market knowledge & experience; partnerships and collaborations.	http://www.securityintech.com/
Aerospace and Defence Industries Association of Europe (ASD)	Belgium	Global	Aeronautics, space, defence and security industries in Europe	To enhance the competitive development of the Aeronautics, Space, Defence and Security Industry in Europe in partnership with European Institutions and Member associations.	The ASD Council includes 19 companies and 28 member associations in 20 countries across Europe. Council companies include: BAE Systems, Cobham, EADS, Cassidian, Finmeccanica, Saab, Safran, Thales and Morpho.	Not found	Not found	Joint industry actions; Raising awareness; Advocacy; Cooperation projects	www.asd-europe.org/
Association for Geographic Information (AGI) (UK)	UK	UK	UK's geographic information (GI) industry	To maximise the use of GI for the benefit of the citizen, good governance and commerce	Public and private sector organisations, suppliers of GI software, hardware, data and services, consultants, academics and interested individuals	Its Constitution	Membership fees and 9 sponsor members who contribute a substantial proportion of the AGI annual revenues.	Lobbying, Networking, Events organisation (annual conference and trade exhibition etc)	www.agi.org.uk

Association of Security Consultants (ASC)	UK	UK	Independent security consultants	To represent and promote the interests of independent security consultants.	Independent consultants with no allegiance to specific suppliers of goods or services (e.g. company heads, senior representatives in consultancy practices)	ASC Code of conduct	Not found	ASC website, Register of Members, Access to individual/joint business opportunities, networking and events, member services, contribution to standards	http://www.securityconsultants.org.uk/
Bundesverband der Deutschen Luft- und Raumfahrtindustrie e.V./The German Aerospace Industries Association - BDLI (BDLI)	Germany	Europe	Aerospace	To be the voice of the sector	200 members -all segments and company sizes in the German aerospace industry.	Not clear	Not found	Networking; News updates to members; Public relations; joint trade fair stands; international platform, ILA; Legal regulation campaigns; civil and military research and technology programmes advocacy;	www.bdli.de/en/
Bundesverband der Hersteller- und Errichterfirmen von Sicherheitssystemen (BHE) (Germany)	Germany	Europe	Preventive security	To represent its members' interests and cooperation with other institutions (such as public authorities, insurance companies, police stations), national, international and European standardization committees.	650 member companies related to preventive security (77% builder, 20% of manufacturers and 3% of planners).	BHE practice guides & directives	Not found	Support of security companies; Advocacy; Standardisation; BHE-QM group certification; Membership directory and online database; Training; Public relations	http://www.bhe.de/

Central Eastern European Smart Card Association (CEESCA)	Croatia	Central Eastern European region	Smart card industry	To provide members with an unparalleled opportunity to solve problems, facilitate smart card initiatives and generate increased business development.	Companies and individuals, from public and private sectors (i.e. suppliers, potential/existing scheme operators or consultants, government agencies, banks, national banking organisations, card payments associations, telecommunications companies, transport operators, systems integrators and solutions providers) in Central Eastern Europe	Rules of Membership CEESCA Club	Not found	Information, consultancy, guidance and networking	http://ceesca.org/
Confederation of European Security Services (CoESS)	Belgium	Europe/global	Private security services sector	To represent and defend the joint interests of its national member federations and of their member companies in turn, at European and international level.	Active members are National bodies (associations or federations or other institutions) representing security companies (in particular, guarding, transport of valuables, airport security, maritime security, monitoring and remote surveillance etc) in European countries. Associated members are members from out with the EU. It also has company members and supporting members from out with the EU.	CoESS Statutes	Annual membership fees	The CoESS General Assemblies; liaison with private security federations and partners; Professional and vocational training; partnerships with the relevant Directorates-General within the European Commission; partnerships with European and international organisations and bodies	http://www.coess.org/

Danish Biometrics (Denmark)	Denmark	Denmark, Scandinavia, Europe, International (in that order)	Biometrics	To promote the sustainable use of biometrics as ID technology	54 members from consultancies, engineering companies, IT integrators, technology providers, government agencies, universities, research and technology institutions, professional bodies, public and private end-user organisations and corporations. 160 Member organisations (and over 1,500 Member contacts)	Not found	Not found	• Networking meetings and conferences on biometrics. • Policy influence actions – responses to draft bills • Stakeholder education	http://danishbiometrics.org/
Direct Marketing Association	UK	UK	Direct marketing	To help the direct marketing industry do better business	800 members in the UK, including agencies, list brokers, mailing houses, blue-chip corporations such as BT, M&S, Lloyds TSB and the AA.	DMA's Memorandum and Articles of Association, DMA Direct Marketing Code of Practice, UK Code of Advertising, Sales Promotion and Direct Marketing (CAP Code), The UK Code of Broadcast Advertising (BCAP Code)	Membership fees	Legal advice; lobbying; compliance service; research and events	http://www.dma.org.uk/content/who-we-are

European Association for e-identity and Security – EEMA	UK	Global	E-identity, security	To promote collaboration in the technical and business aspects of ICT	IT professionals, businesses and governments providing business and technical networking opportunities at both local and regional levels in digital identity and its applications, including security.	Not found	Membership subscriptions and sponsorship revenue.	Conferences, meetings, industry papers, working groups, reports, white papers, networking, project collaborations	www.eema.org/
European Corporate Security Association – ECSA	Belgium	Europe	Corporate security	To provide its members with a trusted forum for: o Sharing common issues & experiences o Information & education o Networking with co-members and third parties.	Professionals, active in corporate security, public security, security risk management, security auditing & resilience & continuity.	The ECSA spirit	Not found	Information & Education; Networking; Professional Training	http://www.ecsa-eu.org/
European NanoBusiness Association (ENA))	Belgium	Europe	Nanotechnology	To promote a strong and competitive European nanotechnology industry	European nanotechnology companies	Not found	Not found	Nanotechnology centre; Creation of national local nanotechnology hubs in Oslo, Helsinki, Copenhagen, Newcastle, Cambridge, London, Dublin, Munich, Eindhoven, Madrid, Budapest and Sofia; Events organisation; Publications	Not found

European Organisation for Security (EOS)	Belgium	European Economic Area	Security	To develop a consistent European Security Market in close cooperation with users from the public and private sector, while satisfying political, social and economic needs, through the efficient use of budgets and the implementation of available security solutions and services in priority areas.	Private bodies or associations active in the security domain. 39 Members involved in Security providing technology Solutions and Services from 13 different countries of the European Economic Area, representing more than 65% of the European Security Market and 2 million employees in Europe.	EOS Statues, Internal Governance Rules and Code of Conduct	Not found	Public – private dialogue with European and Member States Institutions on security issues through working groups, task forces, SME services and project collaborations, Events, Publications (position papers, white papers, press releases, brochures, news letters).	www.eos-eu.com/
European Telecommunications Standards Institute – Technical Committee on Lawful Interception	Belgium	Global	Lawful interception	To develop standards supporting the requirements of national/international law for the Lawful Interception of electronic communications where those communications services are built using ETSI or other open standards.	ETSI is a not-for-profit organisation with more than 700 ETSI member organisations from 62 countries across 5 continents.	ETSI Statutes and Rules of Procedure	•Member contributions •Grants •Revenue from assets •Services provided by ETSI •Any other legal source	Development of Lawful Interception and LI standards, Lawful Interception and Data Retention suite of deliverables, Technical Specifications (TS), technical reports, Participation in EC's Expert Group,' Platform for Electronic Data Retention for the Investigation, Detection and Prosecution of Serious Crime'; other collaborations.	http://portal.etsi.org/li/Summary.asp

Eurosmart	Belgium	Europe/global	Smart Security Industry	To promote Smart Secure Devices and Smart Secure Devices systems	Manufacturers of smart cards and smart secure devices, universities, educational institutions, government bodies, public labs, not-for-profit organisations, independent and industry experts. Members work within dedicated working groups on security, market analysis, new form factors, electronic identity and communication issues.	Not found	Not found	Promoting Smart Secure Devices and Smart Secure Devices; Standardisation activities; Information provision and exchange; Lobbying; Defining test standards; Expert networks; Events	http://www.eurosmart.com/
Federation of European Direct and Interactive Marketing (FEDMA)	Belgium	Europe	Direct and interactive marketing	To promote and protect the European direct and interactive marketing industry by creating greater acceptance and usage of, and confidence in direct and interactive marketing by European consumers and business communities.	Represents most of the European Direct Marketing Associations and companies with multinational business. Around hundred company members.	FEDMA European Code of Practice for the Use of Personal Data in Direct Marketing; Best Practice Recommendation on Online Behavioural Advertising	Not found	Committees, councils; Events; Position papers; Publications (reports); Educational activities	www.fedma.org/
GSMA Europe	Belgium	Europe	Mobile industry	To support our members' efforts to advance their collective public policy interests at the European Union (EU) level by effectively informing the public policy debate on mobile issues.	Over 100 mobile network operators	Codes of conduct – e.g. GSM Europe Code of Conduct for Information on International Roaming Retails Prices	Not found	Inform European public policy impacting the mobile industry; Monitor relevant policy and legislative developments; Identify priorities for the mobile industry; Develop and communicate	http://www.gsma.com/gsmaeurope/

								consensus positions on priorities; Adopt public positions; Issue publications; Respond to public consultations; Form strategic partnerships; Organise events - awards	
Intellect - Information Technology Telecommunications and Electronics Association	UK	UK	Information Technology Telecommunications and Electronics	To use its expertise and knowledge to provide the highest quality of service and intelligence to its members	800 SME and multinational member companies from ICT, electronics manufacturing and design and consumer electronics (CE) sectors, including defence and space-related IT.	Intellect's Code of Conduct	Not found	Publication of guidelines, codes of practice, regulatory developments, frequent discussions with regulatory bodies, group discussion forums/meetings, industry lunches and awards evenings	http://www.intellectuk.org/
Internet Advertising Bureau Europe (IAB)	Belgium	Europe	Digital and interactive marketing industry	To protect, prove, promote and professionalise the digital and interactive advertising industry in Europe.	27 National IABs and Partners across Europe and over 5,500 companies.	IAB Code of Conduct	Not found	Public affairs activities; Research activities; Events; Standards Committees and taskforces; Lobbying. Publications (reports); Information for members.	http://www.iabeurope.eu/

Irish Security Industry Association (ISIA)	Ireland	Ireland	Full spectrum of security services of all sizes in Ireland	To represent its members across the spectrum of the private security industry, promote, develop and maintain the highest professional standards for its members.	Companies involved in guarding services, transport, security systems (CCTV, intruder & fire alarms), alarm receiving centres, physical security, security consultants, private investigation.	Code of Ethical Conduct	Not found	Representation and lobbying; Quality and Standards through QualSec programme; Training; Free recruitment facility, Advertising jobs; Member insurance discounts and Annual Awards.	www.isia.ie
Nordic Biometrics Forum	Denmark	Nordic countries	Biometrics	To help Nordic parliaments, governments, policy makers, businesses, academics, and the wider Nordic community look beyond immediate horizons, to some of the future challenges and opportunities in biometrics ID technology; To provide a vibrant and prospering community for biometrics recognition technology that attracts new talent and industry to the Nordic region.	Key members are Danish Biometrics, the Swedish National Biometric Association and ITS Norway	Not found	Not found	Cooperation in research, innovation, knowledge dealing, standardization and awareness.	http://www.nordicbiometrics.org/
RFIDLab Finland	Finland	Finland	RFID and NFC technologies	To improve the operational efficiency of companies with identification technology.	Any RFID organisation involved in manufacture, whole sales, retail, logistics, and service provider sector.	The purposes and rules of the Association.	It is owned by its member companies.	Business leads; News letters; Networking; Projects participation; Demo room; Events – seminars; Discounts.	http://www.rfidlab.fi/

SIMalliance	UK	Global	Mobile industry	To create a secure, open and interoperable environment where mobile services thrive	Manufacturers, technology providers and application developers with a stake in identity, security and mobility. Members include Datang, Eastcompeace, Gemalto, Giesecke & Devrient, Incard, Inkript, Kebt, Oberthur Technologies, Morpho, Valid, Watchdata & Wuhan Tianyu. SIMalliance Strategic Partners are Comprion, FCI and Movenda	The SIMalliance Code of Ethics	Not found	Workgroup Programme; Consultations with other industry associations; Events; Development of expert resource materials.	www.simalliance.org/
Smartex	UK	Global	Smart card, RFID and biometric technologies	To serve the smart card and RFID tag communities	Membership of Smartex UK forums is open to any company or individual interested in smart technology, biometrics, smart payments, prepaid, RFID tags, M2M and NFC. 400 members worldwide and 138 UK members.	Not evident from website	Membership fees	Expert sessions; networking; news updates; advertising; Smartex-organised and led annual group visit to CARTES & IDentification in Paris; Regular educative forums; Workshops	www.smartex.com/
Swedish National Biometric Association (SNBA)	Sweden	Sweden	Biometrics	To develop into the Swedish focal point for biometrics	Suppliers/vendors (such as Optimum Biometrics Labs, Precise Biometrics AB, Speed Identity, Oberthur, TRP Teknik, Logica), Academia (Blekinge Tekniska Högskola), end user companies and organisations (Blekinge Business Incubator, Karlskrona kommun).	SNBA Statute	Not found	Arrival and usage of international standards; free, online, and mobile-friendly BiometricProducts.info	http://biometricassociation.org/

The ADS Group	UK	Global	AeroSpace, Defence and Security industries	To advance the UK Aerospace, Defence, Security and Space industries	Businesses and organisations (manufacturers, manufacturing suppliers, equipment providers, service companies and operators) in Civil Aviation, Defence, Security and Space. Together with its regional partners, ADS represents over 2,600 companies	Regulations outlined in the organisation's Memorandum and Articles of Association	Not found	• Access to the latest tender and business opportunities • Business meetings services • Assistance for SMEs with Government funding and business development • Specialist business advice to SMEs, support to prime contractors • Events programme • Exhibition service • UK and EU lobbying • Publications • Assistance with personal security clearance • Member directories • Boards, Committees and Special Interest Groups (SIGs) • International business support in key growth economies • Advice and guidance on exports	www.adsgroup.org.uk

The British Security Industry Association (BSIA)	UK	UK	Private security industry	To support members and encourage excellence; educate the marketplace on the value of quality and professional security; and create an atmosphere for members to flourish.	Open only to companies with a significant proportion of their business within the security industry and in business for two years.	BSIA criteria	Not found	Lobbying; information dissemination; standards; skills	www.bsia.co.uk
The Fingerprint Society	UK	UK/Global	Fingerprint evidence	To advance the study and application of fingerprint evidence and to facilitate the co-operation among persons interested in this field of personal identification.	Anybody can join The Fingerprint Society (on acceptance via the application process), though the level of membership is dependent on occupation and experience.	The Society's Codes of Professional Conduct and Practice	Not found	• Annual conference • Publication of professional journal • Research (e.g. aspects of fingerprint identification and analysis) • Annual awards namely, The Lewis Minshall Award and The Henry Medal	http://www.fpsociety.org.uk/
The International Imaging Industry Association (I3A) Europe	Italy	Europe/Global	Imaging	To enable the use of imaging to simplify and enrich people's lives through visual experiences that connect generations, communities, information and services	Major imaging solutions companies - 18 Strategic and regular members and 9 Associate members	I3A By-Laws	Not found	VISION 2020 Imaging Innovation Awards; Advocacy; Information dissemination; Creating standards and metrics	http://www.i3a.org

The Internet Telephony Services Providers' Association (ITSPA) (UK)	UK	UK/EU	VoIP services	• To promote competition and self-regulation in order to encourage the development of a flourishing and innovative VoIP industry. • To act as the representative voice of the industry to UK Government bodies; • To encourage the innovation and development	Large and small suppliers of VoIP services. UK-based network operators, service providers and other businesses involved in VoIP services	ITSPA Code of practice	Not found	• Regular contact with Ofcom, Government and the European Commission to help promote VoIP and the Unified Communications industry; • Accreditation through the ITSPA Quality Mark • Representation on industry bodies • Dispute resolution • Members events • Participation in key events involving Government Ministers, parliamentarians, regulators and the media • Involvement in Technical Forums • Peering network • Investigate solutions for industry including fraud black lists, interoperability etc. • Weekly newsletter and Intelligence Reports.	http://www.itspa.org.uk/

The Ligue Internationale des Sociétés de Surveillance	Switzerland	Global	Private security industry	To establish a supranational organisation to initiate and broaden contacts and exchanges of experience and opinion, and deepen reciprocal understanding among its members and the countries they represent	Established private security organisations satisfying the Ligue's requirements	Constitution and the lawful decisions of the General Assembly and the Board	Not found	Information and idea exchange between member organisations; Events organisation; publication of the Ligazette.	http://www.security-ligue.org/
The Security Alliance	UK	UK	Security Industry	To provide strong secure business partnerships that place it as the No 1 Security Solution provider, and ensure delivery of margin improvement to all parts of the Alliance	Alliance between Loomis, Niscayah, Pinkerton, Securitas Services, Securitas Mobile, Securitas Alert Services, SPS Doorguard, Gunnebo, CamEra, County Parking Enforcement Agency, Russell Richardson, Detechnology, Omni Security, and Solaglas Windowcare & Betafence.	Not found	Not clear	Offering customers various solutions such as manned security solutions, electronic systems, cash handling, monitoring, mobile services, physical security solutions, IT security, business continuity or crisis management, data destruction, consulting & investigation services etc.	http://www.thesecurityalliance.info/

The Unmanned Aerial Vehicle Systems Association (UAVS)	UK	UK/Global	Unmanned aircraft systems (UAS)	To promote the safe, integrated, and effective use of UAVs in military and civilian airspace environments	Companies, academic institutions, related organisations and individuals.	Not found	Funded solely by membership subscriptions	Networking; Access to information on best practice, accredited suppliers and services, certified aircraft, pilot competence and the latest regulatory requirements; Lobbying; Members Directory; Events	www.uavs.org
UK Security & Resilience Industry Suppliers Community (RISC)	UK	UK	Critical National Infrastructure	To bring together the UK industrial community to support the Government in creating a more secure and safe environment for UK citizens.	Alliance of industry, trade associations and think tanks. Membership of RISC is through the British Security Industry Association (BSIA), the ADS and Intellect.	RISC constitution	Not found	Governing council; meetings with government; Industrial Advisory Groups; Information dissemination	http://www.riscuk.org/
Unmanned Vehicle Systems International – UVS International	Netherlands	Global	Unmanned vehicle systems	Primarily to promote UVS (air, ground, naval & space) of all sizes & classes and their current & future applications; provide the UVS community with a voice on a global level	Manufacturers of unmanned vehicle systems (UVS), sub-systems and critical components for UVS and associated equipment, companies supplying services with or for UVS, research organizations and academia.	UVS Constitution	Not found	Promotional activities; Co-ordinate relations with existing national, pan-European & international organizations; Keep members informed on international UVS developments; Promote awareness of unmanned aircraft systems with the relevant stakeholders and the general public	www.uvs-international.org/