Surveillance assemblages: preventing crime and terrorism through data monitoring

den Boer, M.G.W.; van Buuren, G.M.

published in
Governing Security Through the Rule of Law, Amsterdam, Boom.
2010

document version
Publisher's PDF, also known as Version of record

12. European Surveillance Assemblages: Preventing Crime and Terrorism through Data Monitoring

Monica den Boer & Jelle van Buuren

1. Introduction

The concept of the 'surveillance assemblage' can be applied to the governance of practices of data-exchange, both at the level of the European Union as well as that within the individual Member States. In line with the argument of Johnston and Shearing (2003) that plural security practices have emerged widely, data can be interlinked and shared at a variety of levels by a substantial number of different actors, who may function in the context of a highly differentiated governance system. At the same time, it can be argued that criminal justice governance is transforming into a remote crime control mechanism, where gradually – instead of territorial patrol and physical encounters between police and citizens – law enforcement organizations compose collages of deviant (future) conduct. The popularization of the precautionary logic – in internal as well as external security environments – has encouraged wide acceptance of surveillance and mass-data gathering for the purpose of preventing crime, terrorism or military conflict. Through preventive monitoring, social ordering and mental disciplining (Foucault 1995; Haggerty and Ericson 2000; Zedner 2006; Elden 2003: 242; Lyon 2003), law enforcement can seek to deliver and distribute safety in a more efficient manner, as the sector can seek to limit its focus on serious criminal offences and public order issues. At the same time, however, the legitimacy of this managerially driven focus may come under pressure when viewed from the perspective of equal justice distribution (Van Buuren 2009).

From a criminal justice governance perspective, a few observations can be made about the emergence of a surveillance complex in Europe: 1) at the national and European level, a range of surveillance instruments has been coined which enable the law enforcement arena to gather, store and analyze data about citizens in order to control crime and terrorism; 2) these organizational surveillance 'nodes' are aggregated, concatenated and even fused into a larger surveillance complex which is jointly operated within the European Union; 3) the interoperability of surveillance nodes in the Member States allows for a large-scale sharing of information about European citizens which in turn flexes the margins for storage, use and interpretation of high volumes of data; 4) the rise of technological means and the interface with the military world have enlarged the surveillance potential; 5) the encouragement of multi-disciplinary co-operation within these agencies has nourished the erosion of fire-walls

between the different agencies, gradually loosening the hitherto applicable information regimes; and 6) the enlargement of the mandate of existing agencies such as Europol and the creation of new agencies has expanded the counter-terrorism and intelligence potential, furthering the application of the precautionary surveillance of terrorism, crime and deviance.

Our main contention is that the European Union, which is in a position to initiate, facilitate, finance and implement surveillance instruments, is in the process of developing itself into a supernode, which is tentacled by smaller but powerful nodes that interlink public and private actors throughout the Member States through surveillance systems. Instead of drawing a sharp distinction between 'surveillance nodes' (assemblages, networks) on the one hand, and a Panopticon that is centrally operated by one powerful actor, we prefer to define surveillance as a continually changing theatre of activity, spurred on by the sheer Utopian dream of making societies maximally controllable. Neither will we dwell on the distinction between mass surveillance and targeted surveillance. Our emphasis is more descriptive than theoretical, and also more focused on the evolution of several smaller and larger surveillance practices, that sometimes compete and at other times seem to neatly fold into each other. Also, we seek to accentuate that surveillance has gone adrift, like a larger technocratic instrument which can no longer be controlled by one single actor. Finally, our emphasis is on analyzing how the European Union as a security actor has been caught by the logic of prevention and seeks to expand its recently adopted role of security actor through surveillance measures.

In the course of this chapter, we seek to further unpeel the role of surveillance systems in preventive security governance, and we will transpose it to shifting patterns in security governance as well as to the European policy-making level. Moreover, we will seek to clarify how vocabularies and conceptualizations in national and international discourses on security influence – or even bedevil – each other.

2. Preventive Security Governance through Surveillance

The concept of 'surveillant assemblage' was introduced by Deleuze and Guattari (1987) and further developed by Haggerty and Ericson (2000). In the context of our analysis, it provides a conceptual tool for the analysis of data-gathering and information across Europe. 'Surveillance' is understood by us as watching over, i.e. monitoring the behaviour and movement of persons, goods and systems. Surveillance includes a range of measures, exercised by public and private authorities, and is considered to enhance objective and subjective security. As such, surveillance has become closely intertwined with security. Gill (2006: 28) writes – comparably but more extensively – that global surveillance is argued to be an intrinsic part of the general economic restructuring of capitalism, and that 'security intelligence processes' are 'essentially a sub-set of the more general surveillance that constitutes contemporary governance. Thus, since intelligence

is one of the two defining components of surveillance, and, in turn governance, then security intelligence is one of the defining components of security governance.'

Our discussion does not merely focus on data-systems which are widely used in European states and at the level of the European Union itself, but also on the adjacent (and interrelated) practices of de-centralized, networked, transnational data-processing and surveillance, which may not fall within the delineated lines of accountability (Gill 2006: 45). Ericson (2007: 1) observed an 'intensification of security measures' through an incremental series of legal transformations, as well as through 'innovative surveillance technologies and networks'. Below, we seek to illustrate this development by giving some examples. Closed-circuit television (CCTV), for instance, has been introduced in several environments (European Parliament 2009: 7; Hempel and Topfer 2009: 27-34). Face recognition has been proposed, for instance by Interpol, and in some instances has been introduced at local and international levels of security governance; fingerprint controls and facial recognition are and will be introduced at border entry points, allowing for the matching of personal biometric information with travel watch lists.[1]

Except for the growing acceptance of methods of surveillance such as data matching,[2] data mining,[3] and profiling, there has been a widespread introduction of smart cards, body scans, body-cams, storage and interception of telecommunication, the use of GPS for detection purposes, and environmental designs. Radio Frequency Identification (RFID) tags and electronic chips implanted in goods and vehicles are used as instruments of surveillance, often for the purpose of security governance (Ericson 2007: 2; House of Lords 2009: 17; Rathenau Instituut 2007; Van 't Hof, 2007). Although not (yet) widely used by law enforcement authorities because the information is too fragmented, RFID chips can and are used for guiding and monitoring processes such as luggage-handling. The European Commission announced recommendations and a citizens' summary for the implementation of privacy and data protection safeguards for RFID applications. The guidance directs organizations to perform privacy impact assessments, apply risk minimization techniques, and inform individuals about RFID.[4]

---

1 Electronic Privacy Information Centre, <http://epic.org/privacy/facerecognition/>. In the meantime, automated face-recognition systems have also been introduced in local public transport environments.

2 According to the American Civil Liberties Union ACLU (2004), data-matching is a loosely coupled set of techniques to tap into a wide number of data-bases containing details on the individual's behaviour, aggregate the data and scrutinize them en masse for criminal or terrorist intentions. See also House of Lords (2009: 14).

3 Data mining involves the use of mathematically based analytical tools to detect patterns in large sets of data with the purpose of predicting certain kinds of behaviour, such as the propensity to engage in criminal activity or to purchase particular consumer goods (House of Lords 2009: 14).

4 <http://epic.org>.

National surveillance assemblages as well as international data-exchange practices gradually evolve into 'horizontal' strategies, whereby de-central i.e. local law enforcement authorities can exchange information and intelligence with their foreign counterparts in other EU Member States.[5] This can be illustrated by referring to vehicle registration, a practice which gradually gains popularity within law enforcement organizations.

Vehicle recognition is extensively discussed in the European Parliament report on CCTV (2009: 14):

> 'In the UK, one of the first major applications of ANPR was launched in 1996, as part of the city of London's defences against the IRA terrorist threat: all vehicles entering the City of London had their license plates checked against police databases. In 2003 the Home Office drew up plans to extend this for more routine crime prevention purposes, and launched a national pilot scheme which involved 300 officers operating as part of 50 intercept teams across 23 police forces (…) in the first nine months 22.8 million vehicle registration marks were read (…) of which 900,000 (4%) were of immediate interest to the police. Within the resources available, the intercept teams stopped 136,857 vehicles (PA Consulting 2004). These stops led to the arrest of 10,546 people for offences ranging from burglary to drug related offence, and 2611 persons for driving offences. In other words, *seventy-five percent of the arrests were neither for traffic nor for driving related offences* (our emphasis). The significance of ANPR is that it integrates a surveillance device, the camera, with the police national computer and all of its associated databases. Like open street CCTV it targets all under its gaze but greatly enhances its surveillance capacity as it creates a major investigative resource of a vehicle's movements and locations, regardless of the status of the driver. As Watson and Walsh, in their Australian review of ANPR argue, the British Police have exploited the system's potential for: data mining as a means of building a picture of a person's (i.e. offender's) habits and lifestyle. The risk in this approach, however, is that profiles of non-offenders can also be derived from ANPR databases using data mining techniques (2008:8). The Australian Privacy Commissioner noted the British system would soon be collecting and storing around 35 million images per day and stated that they planned to keep this data for two years. Further, the ANPR data that is collected is not only mined and matched with a number of databases, but also then stored for future use. The Australian Privacy Commissioner regards this as an expansive and invasive practice.'

In short, for law enforcement organizations that seek to co-operate across the national borders of EU Member States, a wide range of surveillance possibilities has become available for the active monitoring of individuals and commodities. Ericson and Haggerty have labeled this the 'surveillant assemblage' (see also Sheptycki, 2007). Increasingly, a vast volume of data is available to government in general and to law enforcement and security agencies in particular, to the extent that the physical movement, the decisions, and even the mental state of

[5] See e.g. the application of the Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union in the form of guidelines (Council doc. 16870/08, Brussels, 7 January 2009).

each individual is subject to continuous observation. Over a decade ago, Marx (1998) referred to this development by arguing that:

> 'New technologies for collecting personal information which transcend the physical, liberty enhancing limitations of the old means are constantly appearing. They probe more deeply, widely and softly than traditional methods, transcending barriers (whether walls, distance, darkness, skin or time) that historically made personal information inaccessible. The boundaries which have defined and given integrity to social systems, groups and the self are increasingly permeable. The power of governmental and private organizations to compel disclosure (whether based on law or circumstance) and to aggregate, analyze and distribute personal information is growing rapidly.'

Whether or not international data-gathering practices are subject to 'horizontal' or 'vertical' governance, warning shots have been given that we may be 'sleepwalking into a surveillance society'.[6] Data which have been gathered by different public authorities can be concatenated in a powerful manner, such that new knowledge or intelligence may arise from it. The justification for these practices is the elevation of security for those individuals and society as a whole, mainly through the minimization of risk and uncertainty. The interlinkage between surveillance practices and the prevention of terrorism and crime is a relatively new one within the realm of European policing. Never before did European or intergovernmental security actors such as Europol or SitCen have the possibility to gather and analyze information proactively with a view to early intervention in illegal markets or radicalization contexts; never before was the European Union in such a powerful position to stimulate the interoperability between security-enhancing databases, or to finance research on technologically advanced surveillance systems.

Preventive security governance is an area of activity where the European Union can act potently, without upsetting the sovereign Member States that hold the monopoly of violence, and thus of coercive powers which are used in the context of reactive or repressive security governance. With its encouragement of crime and radicalization prevention programmes, the European Union reinforces national developments rather than competes with national arenas which cultivate preventive security governance through surveillance. According to Ericson, 'risk is the way organizations make sense of their environment and act upon it. External sources of harm are converted into organizational risks through technologies such as early warning systems, risk profiling, and red flag indicators. Internal sources of harm are converted into operational risks through technologies such as inspections, audits, reporting procedures, and electronic surveillance. Risk management has become engrained in the social imaginary of organizations.' (Ericson 2007: 11).

[6] UK Information Commissioner Richard Thomas in 2004, quoted in House of Lords Select Committee on the Constitution report, Surveillance: Citizens and the State, 2009, HL Paper 18-I, p. 5.

More than ever before, today's risk societies are preoccupied by a need to predict. Unpredictability, uncontrollability and invisibility are gradually defined as undesirable practices and thus ruled out from late modern governance (Trommel 2009; Sackers 2010). Longing for a safety utopia (Boutellier 2002), we have landed in a so-called *non-permissive society*.[7] The tendency to prevent disasters, calamities, crises, accidents, crimes and terrorist attacks has influenced the transition from reactive to proactive intervention (Den Boer 2010).

This preventive logic (also referred to as the 'precautionary principle') is not new as it has been apparent in 'high policing' strategies (Borgers and Van Sliedregt 2009), which can be characterized as the gathering of intelligence which may lead to a proactive intervention, often without an explicit criminal procedure. Scenario's, risk assessments and intelligence models have become part and parcel of accepted working methods for police and military, allowing for the prediction of patterns of uncertainty, crimes and security gaps, and allowing for a smart and timely intervention. The preventive logic involves a transition from accusation to an orientation; a transition from individual risk citizens to their environments (social network analysis; money transfers; virtual communication); from penal to administrative intervention; and from repression to the mental disciplining of citizens.

A law enforcement image that presents itself is that of '*policing by the velvet glove*', where physical encounters with the citizens are substituted by electronic data-collection (Den Boer and Van Buuren, forthcoming). The gathering of data, the conditioning, and the restyling of citizens have become part of a larger complex of '*datawars*'. Several police forces have welcomed the introduction of (smart) camera's in public spaces (Sackers 2010: 14), allowing law enforcement authorities to keep a constant watch on mobility and flows of traffic, people, goods, finances and information. This fits in a new strategy of intelligence-led policing which is labeled 'nodal policing' and which has – in a rather technocratic fashion (Den Boer, forthcoming) – become an accepted modus operandi within several law enforcement agencies'.[8]

3. Evolving Surveillance Systems

Surveillance – particularly exercised through electronic i.e. technological means – has become an inescapable reality, primarily because governments seek to reduce risk by means of preventative control (Zureik and Salter 2005: 1), culminating in a 'risk aversive Panopticon' (Whitaker 1999: 44). In a few decades, spurred on by security crises such as 9/11, the surveillance climate has altered dramatically. Below, we seek to illustrate this development by highlighting different dimensions of surveillance: its potential, its depth (pervasiveness), its application, its finality, its interaction and its effect.

[7] Quotation from Chief Constable Bernard Welten, 11 March 2010, Public Lecture, VU University Amsterdam.

[8] Rapport 'Politie in Ontwikkeling', Raad van Hoofdcommissarissen, 2005.

Function Creep

Governments and law enforcement authorities have principally sought to justify the introduction of new surveillance measures by arguing that the scrutiny of millions of data helps in identifying would-be terrorists. But gradually, anti-terrorism surveillance measures can also be used for the monitoring and registration of minor crimes or public nuisance. Or, '(W)hat is developed as an anti-crime surveillance device can be redirected against refugees, political dissidents, or striking trade unionists. Such technologies are also moving into the hands of private, corporate security, which stands outside whatever regulation and democratic accountability may constrain state agencies' (Whitaker 1999: 85).[9] Moreover, large amounts of data can now cross national borders either formally or informally, between public as well as private users (Adviescommissie Informatiestromen Veiligheid 2007; Gill 2006: 33).

Penetration of Social and Private Life

As mentioned previously, practices like data-matching, data-mining and text-mining have become widely introduced. Whitaker (2006) for instance refers to the FBI's CARNIVOR, which is a super search engine capable of trolling through e-mail traffic and flagging communications of interest, e.g. on the basis of key word recognition. In Europe, there has been discussion about the well-known ECHELON system (Whitaker 1999: 93, 105), which, allows SIGINT (signals intelligence collection) and operates on behalf of the five signatory states (Australia, United States, Canada, United Kingdom and New Zealand). ECHELON is capable of (mass) interception and content inspection of telephone calls, fax, e-mail and other data-traffic communicated across a range of media (radio, microwave, cyber-optic, cellular or satellite).[10]

More pervasive surveillance methods include data-profiling practices, which can be based on the collection and sharing of DNA-material and fingerprints.[11] Biometric information systems are thus increasingly woven into existing practices and procedures of international police co-operation (Lewis 2005: 97). According to the House of Lords (2009: 14), data-profiling is used in the public sector 'to predict a variety of risk patterns in the population, thereby enabling public services and law enforcement resources to be appropriately focused. Although this process may enable benefits and social services to be targeted more accurately and effectively, it may arguably lead to discrimination by singling out individuals or social groups for adverse treatment on the basis of incorrect or misleading assumptions.' Profiling is done on the basis of a variety of criteria, e.g. race or ethnic group, and used in security settings.

---

[9] On the issue of democratic accountability, see *Parliamentary Oversight of the Security Sector.*

[10] For the European Parliament Report on intelligence in general and Echelon in particular (11 July 2001), see: http://www.au.af.mil/au/awc/awcgate/echelon/echelon_eur_parliament.pdf.

[11] For a discussion, see European Parliament Working Document on problem of profiling (2008).

From Evidence to Intelligence

As has been noted above, if there is one dimension of information-gathering that has changed considerably, it is the moment at which information is collected about an individual's behaviour: the last few decades have seen a steady increase of pro-active intelligence gathering (instead of reactive information-gathering in response to a concrete suspicion concerning the role of an individual in a reported crime). Hence, there has been a move from tagging real suspicions to possible suspicions. An emergent 'precautionary logic' (Ericson 2007: 25) combined with administrative anxiety about accountability has paved the path for more pro-active data-gathering and risk management: 'While other approaches to government seem to yield more uncertainty, governing through crime sends a strong signal of certainty. When there is a persistent threat that is said to affect the quality of life, or a catastrophic failure in a risk management system for which the government is held responsible, criminalization through counter-law provides an ending to the political narrative of uncertainty in the short term, and perpetuates the myth of governability in the long term.' (Ericson 2007: 207). The evolving finality can also be demonstrated in the new application potential of the Schengen Information System (SIS), which functions in the context of the Schengen Implementing Convention (1990): it allows the submission of data which are defined as indicators of future criminal action; these data will also be used for counter-terrorism purposes by virtue of the Prüm Treaty (2005).

Multiple Users, Shared Information Spaces

The House of Lords (2009: 15) reminds us that: 'The role of technology in surveillance is pre-eminent and poses formidable regulatory problems. The Information Commissioner told us that individuals 'leave electronic footprints behind with the click of mouse, making a phone call, paying with a payment card, using 'joined up' government services or just walking down a street where CCTV is in operation. Our transactions are tracked, our interactions identified and our preferences profiled – all with potential to build up an increasingly detailed and intrusive picture of how each of us lives our life. This has increased the capability for surveillance of the citizen through data collection.' New technology allows for ambient intelligence and ubiquitous computing, enabling a total information awareness on the side of government and law enforcement authorities, exercised by means of Real Time Intelligence Rooms. A condition for this practice is the cultivation of multi-disciplinary co-operation, primarily between security agents, but increasingly also between public and private agents. It is contended that public authorities organize a co-production (or 'conscription') with private business to enable the construction of a surveillance society (ACLU 2004). Air carriers have been included in this public-private security co-operation, for instance as a consequence of the Air Carrier Sanctions in the Schengen Implementing Agreement or in the context of PNR (see below): 'Multiple airlines have admitted turning over the records of their customers' travels to the government. In each case, the information was turned over not to

help the government solve a particular crime or track a particular suspect, but in order to examine each traveler's records in the hopes of identifying terrorists by detecting 'suspicious' patterns in his or her travels – in effect, turning every traveler into a suspect (…)' (ACLU 2004: 10). Private vigilantism thus becomes part of the surveillance complex, and it becomes more difficult for customers or citizens to distinguish the roles and responsibilities of the surveillance agents.

Meanwhile, technology becomes smarter and more sophisticated, for instance due to the introduction of swift and massive hard drives and content analysis (ACLU 2004: 9). A new generation smart cameras has been introduced in several (semi) public spaces, such as shopping malls and railway stations, which can register a concentration of people, irregular behaviour (such as shouting, pushing), allowing for a direct notification to security agents. Within the law enforcement field, netcentric 'warfare' as well as rapid automatic intervention by means of intelligent technology are close to being applied on a vast scale.[12]

Hybrid Interaction and 'Interoperability'

At the level of the European Union, several instruments have been adopted and good practices shared in law enforcement circles which enable the connection between public order policing and overt ('forward intelligence') as well as covert surveillance of audiences, to enable a prognosis of the behaviour of political dissidents, football hooligans, mentally deranged people etc., in order to prevent riots, or in the worst case, attacks. In the UK, this is called 'forward intelligence'. Moreover, as indicated above, there is an increasing development towards authorized access to large national and international databases for police and law enforcement authorities, which increases the possibilities for multi-disciplinary usage of data and data-fusion and which enhances the interaction between intelligence-led policing and public order policing. 'Interoperability' has become the magic wand in European and transnational security arrangements.

Internalization of the Gazing Eye

The effect of total surveillance or total information awareness is that individuals are conscious of being continuously watched by state and private authorities, to the extent that they discipline themselves mentally. This 'panopticism' has become a core element of the modernist project. In this regard, Ericson (2007: 29) noted that 'The police power is perfected when it results in self-policing among members of the population. The liberal social imaginary of the 'house of certainty' is a house of discipline as self-policing. The individual who knows that she is seen through by the surveillant assemblage, who recognizes her visibility, will internalize the gaze. That is, she will not only assume responsibility for the constraints of power, but will have that power inscribed in

[12] See 'Neoconopticon', Report of the Transnational Institute, 2009 (this report can be accessed through http://tni.org/report/neoconopticon).

her to the point where she polices others as well as herself.' The Leviathan-like surveillance net is incrementally enlarged through new legislation (not always passed by parliament but de-centrally widened by municipal authorities who then 'export' their new surveillance practice to other cities) to include ever new groups of the population, who for reasons of safety, education, health, housing or social benefit are made subject of more active monitoring.

4. Surveillance in the EU

Security has become one of the essential pillars in the EU polity, particularly through the construction and promotion of an 'Area of Freedom, Security and Justice'. This policy domain, previously known as the field of justice and home affairs co-operation or the 'Third Pillar', has gradually matured since the adoption of the Maastricht Treaty in 1991, and now encompasses hundreds of legal instruments, as well as several action and financing programmes.

The development of the EU Area of Freedom, Security and Justice has been flanked by wider and more general developments. On the one hand, globalization and informatization have reinforced networked (security) governance and the commodification of public security (Van Buuren 2009), whilst on the other hand, a merging process between internal and external security has facilitated the criminalization and 'securitization' of migratory flows (Bigo 1994). Furthermore, terrorist attacks have sent accelerating shockwaves through EU decision-making machinery and has culminated in the adoption of several legal instruments which entail deep consequences for information-gathering, such as the Passenger Name Record agreement and the EU Retention Directive on Telecommunication.

Particularly noticeable is the reliance of law enforcement authorities – both at the European and the national level – on information, principally gathered and dispersed through large data-bases (Van Linde 2002). Examples of European, cross-border data-bases that are used by law enforcement authorities (including customs and border control authorities) are the VIS (visa information system),[13] SIS I and II[14] (Schengen Information System), the CIS (Customs Information

[13] Access to VIS by law enforcement authorities and Europol is based on Regulation (EG) No 767/2008 of 9 July 2008 (OJ L 218/60, 13.8.2008) and Council Decision 2008/633/JHA of 23 June 2008 (OJ L 218/129, 13.8.2008), for the purpose(s) of prevention, detection and investigation of terrorist offences and of other serious crime. This can only be done when it is deemed necessary, when there are reasonable grounds and when the request is expected to substantially contribute to solving the crime, and should be performed by means of an electronic request via central access points. Source: Lecture Kurt Hager, ERA, 23 April 2009.

[14] Legal basis of SIS II: Regulation (EC) No 1987/2006 of 20 December 2006 (OJ L 318/4, 28.12.2006) and Council Decision 2007/533/JHA of 12 June 2007 (OJ L 205/63, 7.8.2007) on the establishment, operation and use of the second generation Schengen Information System.

System), and Eurodac[15] (fingerprint system for asylum-seekers) and the EIS (Europol Information System). Meanwhile, the creation of new data-bases has been announced, such as the (interlinking of) national DNA-databases (flowing from the Prüm Treaty which was signed in 2005), the creation of a European Border Surveillance System (Eurosur)[16] and the creation of an entry-exit system that registers the entry and exit of all visitors to Europe.[17]

These large data-systems are geared around the principle of verticality, i.e. data-input organized inside the Member States and mediated by a central (law enforcement) authority. The reason for this is the stronghold of national sovereignty: the prime locus of control on law enforcement activity still resides with national authorities. A vertical, central, hierarchical system of data-gathering and exchange suggests that information practices are correctly, intelligibly and transparently subjected to national and international data protection systems.

Retention of Telecommunications Directive

A core element of the EU counter-terrorism strategy is the facilitation of electronic surveillance (Akdeniz and Walker 2003), which has been formalized by means of the EU Directive on the Retention of Telecommunications, which was adopted on 15 March 2006.[18] Data retention or data preservation generally refers to the (temporary) storage of internet traffic, electronic message exchange and mobile telephony. This allows governments traffic analysis as well as mass surveillance.

The Directive requires Member States to ensure that communications providers must retain, for a period of between 6 months and 2 years, necessary

---

[15] Council Regulation (EC) No 2725/2000/EC of 11 December 2000 (OJ L 316, 15.12.2000). Eurodac became operational on 15 January 2003 and is used by all EU Member States, Iceland, Norway and Switzerland. The EU Council Conclusions (11004/07) under the German Presidency recommended access to Eurodac by police and law enforcement authorities for the purpose of prevention, detection and investigation of terrorist offences and serious criminal offences. It was suggested by Kurt Hager at the ERA Conference on 23 April 2009 that around 1100 criminals could be detected by this system.

[16] For a report of the European Parliament's Policy Department C on Citizen's Rights and Constitutional Affairs on Eurosur, see PE 408.295 Briefing Paper 'An Analysis of the Commission Communications on Future Development of Frontex and the Creation of a European Border Surveillance System (Eurosur)', June 2008. The briefing paper opines that the evaluation of Frontex falls short of 'critically assessing the consistence of Frontex activities with the fundamental values upheld by the EU.'

[17] Commission of the European Communities (2008) Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions. Preparing the next steps in border management in the European Union. COM (2008) 69 final, Brussels, 13 February 2008.

[18] 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 provisions of publicly available electronic communications services or of public communications networks (OJ 2006 L 105, p. 54).

data as specified in the Directive to trace and identify the source of a communication; to trace and identify the destination of a communication; to identify the date, time and duration of a communication; to identify the type of communication; to identify the communication device; to identify the location of mobile communication equipment. The data are required to be available to competent national authorities in specific cases, 'for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law'.

In its verdict on the 10th of February 2009, the European Court of Justice ruled that the Data Retention Directive is founded on an appropriate legal basis, correctly adopted on the basis of the EC Treaty and predominantly relating to the functioning of the internal market.[19] Prior to the adoption of the Directive, EU Member States had already introduced measures to oblige service providers to retain data. These measures differed substantially however, in view of the data to be retained as well as with regard to the data retention periods. This may have been the result of the EU Framework Decision, which had been proposed in 2004 by France, Ireland, Sweden, and the United Kingdom. In its ruling, the ECJ also established that the provisions of the directive are essentially limited to the activities of service providers and do not govern access to data or use thereof by the police and judicial authorities of the Member States: 'The measures provided for by the directive do not, in themselves, involve intervention by the police or law-enforcement authorities of the Member States. Those issues, which fall in principle within the domain covered by police and judicial cooperation in criminal matters, have been excluded from the provisions of the directive.'[20] It has however been claimed that access to these data is provided to law enforcement authorities without a warrant and for crimes that are not necessarily serious in nature.[21] For the access of law enforcement authorities to e.g. mobile phone records, additional measures are mostly to be found within the realms of the individual Member States.

Guild (2010: p. 3) explains that the EU Directive on Data Retention ran 'into serious trouble in the national courts in the EU', also because since the ruling of the ECJ, the Romanian Supreme Court ruled against the national implementing legislation in October 2009, and the German Constitutional Court struck down its national implementing legislation on 2 March 2010; in both cases the intrusive nature in combination with the individual right to privacy was at the heart of the argument. Guild (2010, p. 3):

> 'The German court was particularly concerned about the purpose of the collection and the storage of the data, which was precautionary in nature, that is to say not directed at events that had already taken place but at some future possible action or

[19] Judgement of the Court of Justice in Case C-301/06, Ireland v. Parliament and Council.

[20] Judgement of the Court of Justice in Case C-301/06, Ireland v. Parliament and Council, par. 82.

[21] <http://en.wikipedia.org/wiki/Mass_surveillance#Mobile_phone_tracking>.

event. It found that retention of such data must not lead to the possibility to virtually reconstruct any activities of citizens'.

PNR agreement

Since 2003, USA authorities have demanded on-line access to the Passenger Name Records which are kept by European flight carriers on flights to the USA. By screening the data, the American and Canadian authorities[22] seek to decrease the possibility that (would-be) terrorists enter their territories from Europe. The PNR's comprise several data, such as name, date of birth and telephone numbers, as well as credit card numbers, seat numbers and meals. The USA authorities may also demand information from the Advanced Passenger Information System, including gender, passport number and nationality of the passengers (Rathenau Instituut 2007).

The screening method raises several questions however as to how the PNR's help to identify risks, what the substance of the precise procedure actually is, and whether the data are run against existing criminal data (Kuipers, 2008). There are several bilateral agreements which have shaped the basis for the exchange of PNR-data by airlines. These comprise the 2004 EU-US PNR agreement, in 2006 ruled by the European Court of Justice to be founded on the wrong legal basis (Balzacq 2008: 91); the 2005 EU-Canada agreement on API (Advanced Passenger Information) and PNR data; the 2006 EU-US interim PNR agreement (replaced by the 2007 definitive EU-US agreement on the submission of PNR-data), and the PNR agreement between the EU and Australia from June 2008 (Kuipers 2008: 17f).

Foreign authorities can use these data of individuals travelling from Europe for the purpose of data-matching, data-mining and profiling. In the meantime, it has been ventured that these data have also been used to detect criminals and to control land borders. Hence, vast numbers of data are put on stock by American,[23] Canadian and Australian authorities which demonstrates the increasingly dense information web and the way in which the EU has actively developed an external security link in its counter-terrorism policy.

Members of the European Parliament, privacy organizations, airlines and data protection authorities are increasingly concerned about the transmission of personal files without the approval of the relevant individual (Kuipers 2008: 3). One of the concerns is the potential function creep, i.e. the use of data for other

[22] United States' Customs and Border Protection (US-CBP) and the Canada Border Services Agency (CBSA).

[23] On 14 July 2008, the American Civil Liberties Union ACLU announced that the US authorities had tagged the names of 400.000 individuals on the terrorist suspects list, 95% of whom are foreign or not a resident of the United States. 50.000 people were tagged as potentially suspicious with regard to (terrorist attacks on) air transport, while only 16 names were known to the authorities when the 9/11 attacks took place (ANP Press, 14 July 2008).

than counter-terrorism purposes, as well as the lack of reciprocity in the obligation to transfer data on passengers.[24]

Europol

Although Europol had been established before 9/11, its competences were extended considerably thereafter, partly as the consequence of a long-term programme for the Area of Freedom, Security and Justice, partly as an *ad hoc* response to large-scale terrorist attacks (Madrid 11 March 2004, London 7 July 2005 in addition to the September 2001 attacks in the USA). After 9/11, Europol established a team of counter-terrorist specialists, later transferred to the entity SC 5 (Serious Crime), with – in principle – two Liaison Officers from each EU Member State, one from the police and one from the intelligence service. The team was requested to collaborate directly with American counterparts.

Furthermore, the Director of Europol was instructed to conclude an 'informal agreement' with the USA, which provided for the exchange of liaison officers between Europol and US law enforcement agencies: at present, the FBI, the US Secret Service, the DEA and the US Postal Inspection have Liaison Officers at Europol, while Europol has seconded two Liaison Officers to a bureau in Washington DC (Ratzel 2007: 289). In addition, on 6 December 2001 Europol and the US signed an agreement on the exchange of strategic and technical information, and negotiations were started on a supplemental agreement concerning the exchange of personal data.[25] Hence, Europol has played its part in the post 9/11 tendency to blur the distinction between police and secret service intelligence, mainly by managing to overcome hitherto existing firewalls, the one being the gulf between police and intelligence agencies (MacVean 2008: 67), the other being the transatlantic gap. The question whether this has eroded restrictions to information-gathering and intelligence-exchange should be regarded as a prime subject for research.

The most important issue in the light of this paper is however the role which the agency plays in (electronic) surveillance. Europol bases itself on information which is made available by the Member States. Hence, the agency has the capacity for electronic data-storage and data-warehousing,[26] and does so by means of its information system EIS. The analytical capacity of Europol implies systematizing and assessing the data, mainly through the European Crime Intelligence Model (ECIM), as well as in OCTA (Organized Crime Threat Assessment), TE-SAT (Trends and Situations Report on Terrorism), and

[24] The European Parliament rejected a former SWIFT-agreement (Terrorist Finance Tracking Programme) as it was of the opinion that the agreement was not in line with European data protection standards, represented an disproportionate invasion in people's private lives, and was asymmetric in the sense that the EU does not require private financial data of American citizens to be analyzed for counter terrorism investigation purposes. In the meantime however, the European Parliament adopted a minor revised version of the agreement (8 July 2010).

[25] <http://www.europol.europa.eu/legal/agreements>.

[26] See Article 7 Europol Convention.

selected Analytical Work Files (AWF's).[27] Moreover, there is frequent interaction between the Europol database and other international data bases which contain information on criminals and their activities, such as the Schengen Information System, Interpol data systems and data held by Eurojust. The most salient aspect is the strong emphasis on (pro-active) intelligence gathering in combination with risk assessment strategies. Europol has a rather elaborate data protection system and is subjected to the control of the Joint Supervisory Board. In the new SWIFT-agreement which facilitates USA authorities to track terrorist financing, Europol shall even be entrusted with the task of controlling the data requests from the USA.

The European Internal Security Strategy

In the beginning of 2010 the EU launched its Internal Security Strategy, which aims at the development of a 'larger consensus of the vision, values and objectives' which underpin European internal security.[28] As main objectives of the strategy a proactive, intelligence led approach is advocated that focuses on the prevention of criminal and terrorist acts before they can take place. Prevention and anticipation are emphasized, structured around analytical tools and early-warning systems. 'A comprehensive approach must be taken that is geared to constant detection and prevention of the threats and risks facing the EU in the various areas of internal security.' Further, the EU advocates a strategy of 'responsibilization': security policies must take a broad approach, involving not only law-enforcement agencies, but also 'institutions and professionals at both national and local levels', like schools, universities, the private sector and civil society organizations. One of the corner stones of the Internal Security Strategy is an accompanying Information Exchange Strategy, aimed at the timely access to 'as much data as possible'. The model will include all the different EU databases relevant for ensuring security in the EU so that there can be 'interaction between them' for the purpose of providing effective information exchange across the whole of the EU and 'maximizing the opportunities' presented by biometric and other technologies.

---

[27] For Rules applicable to Europol Analysis Files, see: <http://www.europol.europa.eu/legal/other/files/Rules_applicable_to_Europol_Analysis_Files_en.pdf>.

[28] Council of the European Union (2010) Note from Presidency to delegations. Draft Internal Security Strategy for the European Union: 'Towards a European Security Model', 5842/10 JAI 90, Brussels, 2 February 2010.

5. Conclusion: A Europe That Interlinks Polycentric Surveillance Practices

The expansion of the European surveillance society is intimately connected with the growing popularity of the precautionary principle (crime prevention, preventive intervention in fragile environments). While emphasizing that our sketch may be far from complete, we have looked into some European strategies in the area of internal security co-operation and we have identified these as indicative of the rapid introduction of new surveillance measures in the field of EU homeland security. Despite the fact that 'Big Brother' critiques have not managed to obtain much cultural and political purchase in the fact of the 'obvious' benefits of surveillance technology' (Loader 2007: 32), several concerns have been voiced about the all-encompassing surveillance society. A few years ago, Privacy International conducted a comparative international survey in 47 countries and found there had been an increase in surveillance and an erosion of privacy safeguards. Of the EU Member States that were included in the survey, the United Kingdom scored lowest (primarily because of its massive presence of CCTV cameras, the number of which in 2002 was estimated to be 4,2 million, and the sizeable police databases containing 5,5 million fingerprint records and 3,4 million DNA records).

Within the EU, the accumulation of surveillance measures is formidable, the speed with which measures have been adopted is impressive given their intrusive effect, the relative absence of controversy (public silence) is surprising, and the number of technological advances is hard to match with new data protection standards. Generally, however, one may argue that there has been a tidal shift in public opinion and checks and balances: governments have aggregated vast volumes of power and knowledge vis-à-vis their citizens. This process has been bolstered by the tidal concerns of the anxiety society in which organized crime and terrorism have been transformed into fluid and ungraspable demons. New legislation – in particular anti-terrorism legislation but also the development of administrative powers at local level[29] – has restricted (the access to) rights in the fields of due process and data protection.

So is large-scale surveillance, coupled with transnational security governance (Johnston 2006), effective in what it seeks to achieve? The answers provided by the law enforcement community are mostly positive, to the extent that e.g. the electronic identification of vehicle license plates amounts to stops, searches, successful 'hits' and arrests. The collection of electronic data may also assist in reconstructing the movements of criminals and illegal transports or money flows. For the time being, although there is a strong pragmatic and technocratic aspiration to interlink surveillance practices for the purpose of crime control, there are several political, organizational, cultural and technological obstacles which obscure the realization of a panopticon from our view. According to David Lyon (2006: 4), the more soft and subtle 'panoptic strategies', the more it produces the desired docile bodies, or worse, perhaps, the absence of social

[29] For a discussion in the British context, see House of Lords (2009: p. 41).

reflection on the emergence of surveillance practices. Future research will have to generate empirical data on whether surveillance contributes to early detection of deviance, marginalization or radicalization, and whether this proactive information stops future criminals and terrorists in their tracks in an effective, efficient and legitimate manner. Alternatively, crime control and surveillance measures can be regarded as colonizing speech acts, meant to expand the regulatory power of governmental authorities over 'deviant' minds.

References

Adviescommissie Informatiestromen Veiligheid (2007). *Data voor daadkracht. Gegevensbestanden voor veiligheid: observaties en analyse*. Den Haag.

American Civil Liberties Union (2004). *The Surveillance-Industrial Complex: How the American Government is Conscripting Business and Individuals in the Construction of a Surveillance Society*. Jay Stanley (author), New York. <http://www.aclu.org/FilesPDFs/surveillance_report.pdf>.

Akdeniz, Y., & Walker, C. (2003). Anti-Terrorism Laws and Data Retention: War is Over? *Northern Ireland Legal Quarterly, 54 (2)*, 159-182.

Balzacq, T, (2008). The Policy Tools of Securitization: Information Exchange, EU Foreign and Interior Policies. *Journal of Common Market Studies, 46 (1)*, 75-100.

Bendiek, A. (2006). *EU Strategy on Counter Terrorism: Steps towards a Coherent Network Policy*. SWP Research Paper 2006/RP 12.

Bigo, D. (1994). The European Internal Security Field: Stakes and Rivalries in a Newly Developing Area of Police Intervention. In M. Anderson, & M. den Boer (Eds.), *Policing Across National Boundaries*. London: Pinter Publications.

Borgers, M., & Van Sliedregt, E. (2009). The Meaning of the Precautionary Principle for the Assessment of Criminal Measures in the Fight Against Terrorism. *Erasmus Law Review, 2 (2)*, 171-195.

Born, H. (Ed.) (2003). *Parliamentary Oversight of the Security Sector. Principles, Mechanisms and Practices.* Geneva: Geneva Centre for the Democratic Control of Armed Forces.

Boutellier, H. (2002). *De Veiligheidsutopie*. Den Haag: Boom Juridische uitgevers.

Brodeur, J.P. (1983/1996). High and Low Policing: Remarks about The Policing of Political Activities. *Social Problems* (1983/1996) 30/5:507–521. (reprinted in R. Reiner (Ed.) (1996). *Police Discretion and Accountability, Policing Vol. II*. Aldershot (UK): Dartmouth Pub, 261–274).

Deleuze, G., & Guattari, F. (1987). *A Thousand Plateaus: Capitalism and Schizophrenia*. Minneapolis, University of Minnesota Press.

Den Boer, M. (2010). Revolving Doors: Ethics in a Shifting Security Paradigm. In M. den Boer, & E. Kolthoff (Eds.) (2010), *Ethics & Security*. The Hague: Boom Juridische uitgevers.

Den Boer, M. (forthcoming). Go with the Flow and Undo the Knots: Policing Strategies in an Interconnected World. In F. Allum (Ed.), *Handbook on Transnational Organized Crime.* London: Routledge.

Den Boer, M., & Van Buuren, J. (forthcoming). *Door het oog van de staat.* Amsterdam: Boom.

Elden, S. (2003). Plague, Panopticon, Police. *Surveillance & Society 1 (3)*, 240-253.

Ericson, R. (2007). *Crime in an Insecure World*. Cambridge: Polity Press.

European Parliament (2008). *Working Document on Profiling, Notably on the Basis of Ethnicity and Race, in Counter-Terrorism, Law Enforcement, Immigration, Customs and Border Control*. Committee on Civil Liberties, Justice and Home Affairs, Sarah Ludford (rapporteur), 30 September 2008, DT\745085EN.doc.

European Parliament (2009). *A Review of the Increased Use of CCTV and Video-Surveillance for Crime Prevention Purposes in Europe*. Clive Norris (author), note for the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, PE 419.588.

Foucault, M. (1995). *Discipline and Punish*. New York: Random House.

Gill, P. (2006). Not Just Joining the Dots But Crossing the Borders and Bridging the Voids: Constructing Security Networks after 11 September 2001. *Policing & Society, 16 (1)*, 27-49.

Guild, E. (2010). *Global Data Transfers: The Human Rights Implications*. Brussels: Centre for European Policy Studies. INEX Policy Brief No. 9 (www.inexproject.eu).

Haggerty, K.D., & Ericson, R.V. (2000). The Surveillant Assemblage. *British Journal of Sociology, 51 (4)*, 605-622.

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

House of Lords (2009). *Surveillance: Citizens and the State*. House of Lords Select Committee on the Constitution, Volume I, HL Report 18-I.

Johnston, L. (2006). Transnational Security Governance. In J. Wood, & B. Dupont (Eds.), *Democracy, Society and the Governance of Security*. Cambridge: Cambridge University Press.

Johnston, L., & Shearing, C. (2003). *Governing Security, Explorations in Policing and Justice*. London: Routledge.

Koffijberg, J., Dekkers, S., Homburg, G., & Van den Berg, B. (2009). *Niets te verbergen en toch bang. Nederlandse burgers over het gebruik van hun gegevens in de glazen samenleving*. Regioplan, see: www.cpbweb.nl.

Kuipers, F. (2008). *No Dream Ticket to Security. PNR Data & Terrorism*. Clingendael Security Paper No. 5, The Hague.

Lewis, N. (2005). Expanding Surveillance: Connecting Biometric Information Systems to International Police Cooperation. In E. Zureik, & M. Salter (Eds.), *Global Surveillance and Policing: Borders, Security, Identity* (pp. 97-112). Devon: Willan Publishing.

Loader, I. (2007). The Cultural Lives of Security and Rights. In B. J. Goold, & L. Lazarus (Eds.), *Security and Human Rights*. Oxford and Portland: Hart Publishing.

Lyon, D. (2003). *Surveillance after September 11th*. Cambridge: Polity Press.

Lyon, D. (2006). The Search for Surveillance Theories. In D. Lyon (Ed.), *Theorizing Surveillance. The Panopticon and Beyond* (pp. 3-20). Collumpton: Willan Publishing.

MacVean, A. (2008). The Governance of Intelligence. In C. Harfield, A. MacVean, J. Grieve, & D. Phillips (Eds.), *The Handbook of Intelligent Policing. Consilience, Crime Control and Community Safety*. Oxford: Oxford University Press, 63-73.

Marx, G.T. (1998). An Ethics for the New Surveillance. *The Information Society, 14 (3)*, 171-186.

Rathenau Instituut (2007). *Van privacyparadijs tot controlestaat? Misdaad- en terreurbestrijding in Nederland aan het begin van de 21ste eeuw*. Studie 49, February, The Hague.

Ratzel, M.-P. (2007). Europol – das Europäische Polizeiamt, Teil 1: Geschichte, Organisation, Aufgaben, Zuständigkeiten und Rechtsgrundlage. *Kriminalistik 5/2007*, 284-291.

Sackers, H. (2010). *Herder, hoeder en handhaver. De burgemeester en het bestuurlijk sanctierecht*. Inaugural Speech, 15 januari, Radboud University Nijmegen.

Sheptycki, J. (2007). High Policing in the Security Control Society. *Policing, 1 (1)*, 70-79.

Trommel, W. (2009). *Gulzig Bestuur*. Inaugural Speech. VU University Amsterdam, 17 September 2009.

Van Linde, E. (2002). *Quick Scan of Post 9/11 National Counter-Terrorism Policymaking and Implementation in Selected European Countries*. RAND, Europe.

Van Buuren, J. (2009). *Security as a Commodity. Ethical Dilemmas of Private Security*. Brussels: INEX.

Van 't Hof, C. (2007). *RFID & Identity Management in Everyday Life. Striking the Balance between Convenience, Choice and Control*. The Hague: The Rathenau Institute.

Whitaker, R. (1999). *The End of Privacy. How Total Surveillance is Becoming a Reality*. New York: The New Press.

Whitaker, R. (2006). A Faustian Bargain? America and the Dream of Total Information Awareness. In R.V. Ericson, & K.D. Haggerty (Eds.), *The New Politics of Surveillance and Visibility* (pp. 141-171). Toronto: University of Toronto Press.

Zedner, L. (2006). The Concept of Security: An Agenda for Comparative Analysis. *Legal Studies, 23(1)*, 153-176.

Zureik, E., & Salter, M. (2005). Global Surveillance and Policing: Borders, Security, Identity – Introduction. In E. Zureik, & M. Salter (Eds.), *Global Surveillance and Policing: Borders, Security, Identity* (pp. 1-10). Devon: Willan Publishing.