Policing, surveillance and law in a pre-crime society: Understanding the consequences of technology based strategies.

Rosamunde van Brakel¹ & Paul De Hert²

The last decades have seen several trends emerging in policing, the policing landscape has become fragmented, (surveillance) technology is starting to play an increasingly important role in policing practices and recently new police models are more and more geared to predicting what will happen in the future. A first goal of this article is to explore new developments in policing and more specifically the focus will be on the huge expansion of the use of surveillance technologies by police, and the growing belief amongst both policy makers and police that it is possible, to a certain extent, by using surveillance technology to predict crime before it happens. A second goal is to explore a number of important unintended consequences that arise as a result of what we will call ‘preemptive policing’.

For our exploration Garland’s much cited theory of the ‘culture of control’ is used as a theoretical backdrop to contextualize the trends in policing that have led to the emergence of pre-emptive policing. The article shows the fundamental importance of taking into account social and legal issues arising when deciding upon the deployment of new surveillance technologies by police and that proportionality, transparency, non-discrimination and due process need to take centre stage in the development of new police models.

1. Introduction

“I feel that the faith in technological solutions may actually lead to, in a sense, a shift from one of the fundamental principles of British policing” (Norris & Murakami Wood, 2009: 24).

¹ Drs. Rosamunde Van Brakel is Phd-student at Law, Science, Technology & Society (LSTS), Vrije Universiteit Brussel, Belgium.
² Prof. dr. Paul De Hert Professor of Criminal Law at Law, Science, Technology & Society (LSTS), Vrije Universiteit Brussel, Belgium
Government officials are human. Their imagination can be stirred and they can be captured by vendor of all kind. Philip K. Dick’s * Minority Report* cinematized by Steven Spielberg has contributed to an almost enlightened belief in technology, dominating government and public discourse, where everything is considered possible. Several commentators observe in this respect that science fiction does have a distinct influence, not only on public beliefs and discourse, but also upon government policy and technological development (Haraway, 1997; Clough, 2002). This message is rubbed in further by technology companies to make governments and police believe that technology makes anything possible (see for an example British Security Industry Association, 2009). Wood, labelling this phenomenon the ‘political economics driver’ or ‘driver of industry,’ highlights how industries produce more and more highly advanced technologies that seem to come as a complete package and solution to social problems in a nice, neat technological bundle attractive to policy makers. “Easy solutions are very attractive” (Norris & Murakami Wood, 2009:33).

This belief in technology and quest for easy solutions has led to an increased often indiscriminate implementation of technology in all domains of governance. Exemplary has been the ubiquitous use of surveillance technologies, by police and law enforcement, such as CCTV, databases, data mining, biometrics, body scanners etc. Sophie in’t Veld, Rapporteur of the Civil Liberties Committee of the European Parliament, speaking on the issue of counter-terrorism formulates this in following terms: “whereas mass surveillance has become a key feature of counter-terrorism policies, and whereas the large-scale collection of personal data, detection and identification technologies, tracking and tracing, data mining and profiling, risk assessment and behavioural analysis are all used for the purpose of preventing terrorism; whereas public authorities are making more and more use of data collected for commercial or private purposes” (Committee on Civil Liberties, Justice and Home Affairs, 2011, p.5).

Dick’s story raises several social and ethical issues from the use of drug babies who as a result of genetic experiments turned into pre-cogs, who can see future murders happening to the punishment of people who have not (yet) done anything wrong. Another issue raised concerns accountability for actions and thoughts, motivations and emotions. Finally the issue that police officers are completely dependent on technology is raised, whereby they stop thinking critically, and technology is the culpable agent, not the police officer, who merely identifies the person, the pre-cog shows in the visions in order to arrest them. Illustrative is the fact that minority reports, drafted on the rare occasion when one of the three pre-cogs will disagree with the other two, are always destroyed, making it seem that the predictions are 100% reliable.

*Minority Report* is still very much science fiction and does not seem to resemble at all how police work nowadays. Or does it? Although the possibility that through genetic experiments pre-cogs will look into the future is almost unthinkable, the idea of predicting who will commit crime in the future is tempting and already being tried out as will be shown in this article. Furthermore the issues raised in the story are extremely relevant for developments in the use of surveillance technologies by the police, as well as how both policy makers and police perceive these new technologies. Just as in the broader society technology is becoming increasingly important in policing not just in the sense that new crimes are emerging (cybercrime) but also as a tool for police investigation.
and crime prevention, the police is relying increasingly on (information) technology to take over certain parts of their tasks. This is why this special issue is very timely.

The main purpose of this article is to explore new developments in policing. More specifically the focus will be on the huge expansion of the use of surveillance technologies by police, and the growing belief amongst both policy makers and police that it is possible, to a certain extent, by using surveillance technology to predict crime before it happens. For this exploration the article draws from several disciplines; it reviews literature on policing, but will also venture into surveillance studies and science and technology studies. Up till now there have not been many authors within police studies who have undertaken this. Opening-up to these other academic fields allows for a better understanding of the role of technology and surveillance in contemporary policing practices.

The goal of this contribution is not to present empirical data to test the literature but to discuss certain social consequences that are raised by pre-emptive policing and to analyze how European law deals with these consequences through a discussion of several judgments of the European Court of Human Rights. For our exploration Garland’s much cited theory of the ‘culture of control’ is used as a theoretical backdrop to contextualize the trends in policing that have led to the emergence of pre-emptive policing. Finally it should be noted that although it was not our intention in this contribution to focus on the United Kingdom (UK) this was inevitable as the UK, together with the United States (US), has been on the forefront of the development of surveillance technologies and the implementation of them. Illustrative of this is the abundance of publications by North American authors on police use of surveillance or information technologies (Manning, 1992/2008; Marx, 1989/2002; Ericson & Haggerty, 1997; Leman-Langlois, 2008 to name a few) and by British authors on CCTV and policing (Norris & Armstrong, 1999a; Newburn & Hayman, 2001; Goold, 2007; Welsh & Farrington, 2009). As a result most literature dealing with surveillance technology cited3 and also most important case law and illustrations taken from the European context focus on the UK, although we have tried to refer to other countries where possible.

When looking at relevant literature from policing, criminology and surveillance studies, two recent trends catch the eye: (1) a shift to more proactive, predictive and pre-crime methods; and (2) surveillance technologies and more specifically, databases and profiling/data mining methods becoming more and more ubiquitous in policing practices. In what follows we will discuss these trends more elaborately and will explore how these new developments fit into Garland’s theory of crime control presented in his book *The Culture of Control* (2001).

Part one of this paper will present an exploration in how pre-emptive policing emerged (section 2.1), and its use of adaptive (section 2.1.1) and non-adaptive strategies (section 2.1.2) and its increased reliance on surveillance technology in policing (section 2.2). In the risk and pre-crime society, policing is not just about crime control, but is also more and more a matter of surveillance made possible by technology. After defining technology-based surveillance (section 2.2.1), we pay attention to the perceived neutrality

---

3 For example when one looks at Belgium there is hardly any research conducted or articles published on the topic of surveillance within criminology and policing studies. However, with the increased use of these technologies in Belgian policing, here and there this is slowly changing as this issue illustrates.
of technology (section 2.2.2). A third part tries bring the two trends discussed in section 1 and 2 together: pre-emptive policing and surveillance policing together by discussing the surveillance technology pre-emptive profiling (section 2.3.1) and this will be expanded by discussing the case of the Dutch Border Controls Framework (section 2.3.2).

The first section of the second part of the paper (section 3.1) discusses some of the most important, often unintended social consequences of these trends: discrimination and loss of social cohesion. In addition, the use of surveillance also has consequences for trust and for accountability issues when something goes wrong. Finally we will shortly touch on the function creep phenomenon. In the last section (section 3.2) the crucial but ambiguous role of law is critically discussed. On the positive side we note some very relevant recent case law by the European Courts addressing in a straightforward way some of the main issues raised by developments towards pre-emption and unlimited surveillance.

2. Part 1. Emerging trends in policing: pre-emption and technology based surveillance

2.1.1. The emergence of pre-emptive policing

Several authors within criminology have observed a shift in society away from Foucauldian disciplinarity. Illustrative of this has been the introduction of the term ‘risk society’ (Beck, 1992; Giddens, 1990) and the paradigm shift suggested by Feeley and Simon from ‘old penology’ to the ‘new penology’. (Simon, 1988; Feeley & Simon, 1992). Simon (1988) argues that, rather than working to normalize individuals by identifying their pathological propensities, placing them in reformatory institutions, and attempting to move each pathological person towards uniformity, an actuarial regime seeks to “manage them in place … . While the disciplinary regime attempts to alter individual behaviour and motivation, the actuarial regime alters the physical and social structures within which individuals behave.” (Simon, 1988: 771-73). The old penology was concerned with the identification of the individual criminal for the purpose of ascribing guilt and blame, and the imposition of punishment and treatment. The new penology, on the other hand, is “concerned with techniques for identifying, classifying and managing groups assorted by levels of dangerousness” (Simon, 1994: 180). A clear shift can be observed in society from a post-crime to a pre-crime society “characterised by calculation, risk and uncertainty, surveillance, precaution, prudentialism, moral hazard, prevention and which has the overarching goal of the pursuit of security” (Zedner, 2007: 262). The shift is not only temporal it is also sectorial: In a pre-crime society the responsibility for security against risk is not just the responsibility of the State but extends to a larger group of individual, communal and private actors. Criminal justice techniques are not based on individualized suspicion, but on the probability that an individual may be an offender (Norris & McCahill, 2006). In this new paradigm prediction of criminality is no longer seen as mere convenience but rather as a necessity (Harcourt, 2007).

These observations about the emergence of the risk society and shift to pre-crime society are echoed in policing literature in which there is a consensus that there have been profound changes in the delivery, practice and orientation of policing in Western societies at the end of the 20th Century (Ericson and Haggerty, 1997; Garland, 1996/2001; Jones
These changes respond to the observed failure of the police to deter by their presence, as well as the competition they face from private security companies, whose strategies overwhelmingly favour prevention (Bailey & Shearing 1996). As a result of the high crime rates and the growing problem of organised crime, police and policy makers started to question their role, operating strategies, organization and management (Garland, 2001). The response to these problems by policy makers has been “deeply contradictory” (Garland, 2001): on the one hand the response was to face up to the problem and develop pragmatic new strategies that are adapted to it (adaptive strategies); but on the other hand, there also has been a recurring tendency towards a kind of “hysterical denial” of the problems (non-adaptive strategies).

2.1.2. New police models as adaptive strategies

Illustrative of the adaptive strategies has been the introduction of more proactive police models such as community and problem-oriented policing, which became very popular in the 1990s. Both models tried to address the observed problems mentioned above and developed in a large part in response to the more traditional, reactive, remote policing styles (Garland, 2001). We will briefly discuss both models and then turn to new models that have been embraced in recent times.

In order to improve the quality of life in the community or to solve the existing neighbourhood problems, community policing strongly emphasises the need for pro-activity (Ponsaers, 2001). The idea behind this form of policing is that “the police cannot successfully prevent or, investigate crime without the willing participation of the public, therefore police should transform communities from being passive consumers of police protection to active co-producers of public safety” (Bailey & Shearing 1996, 717-18). As a result several initiatives were launched of which the most famous was Neighbourhood Watch, widely implemented in North America and the UK (Bailey & Shearing, 1996; Garland, 2001), and in several other European countries including Belgium (Eliaerts, Enhus & van den Broeck, 1993). Other similar initiatives, emerging at the end of the century, are publicity campaigns, informers and citizen patrols. These community-led crime prevention initiatives can be understood as ‘responsibilisation strategies’: “A new mode of governing crime whereby individuals and organizations outside of the state apparatus are encouraged to take responsibility for crime prevention and security” (Garland, 2001). A fine recent example of this approach is the call on the public to be vigilant and help police at the occasion of the royal wedding of Kate and William in April 2011 (McGinty, 2011) but also the anti-terrorism campaigns that have been launched in several countries since 9/11 which call on the public to report anything or anyone suspicious.

Problem-oriented policing is considered as a variant of community (oriented) policing and should be seen as a reaction against the dominant ‘means over ends’ syndrome of

---

community policing. (Ponsaers, 2001). It is an approach to policing in which “each discrete piece of police business that the public expects the police to handle (referred to as a “problem”) is subject to careful, in-depth study in hope that what is learned about each problem will lead to discovering a new and more effective strategy for dealing with it” (Goldstein, 2003: 14). Characteristic of this type of policing is the emphasis on prevention, effectiveness and the involvement of other public agencies and the private sector in order to make it work.

The emphasis on pro-activeness or better pre-emption increased after 9/11 gave birth to new policing concepts. Illustrative is the emergence of intelligence-led policing, which can be defined as “a strategic, future-oriented and targeted approach to crime control, focussing upon the identification, analysis and ‘management’ of persisting and developing ‘problems’ or ‘risks’ (which may be particular people, activities or areas), rather than on the reactive investigation and detection of individual crimes” (Maguire, 2000: 315). Although intelligence-led policing is also an adaptive strategy and as proactive as the other police models discussed above there are some significant differences. The difference with community oriented policing is pretty clear: the two policing models emerged out of different needs. Where community oriented policing was a reaction to several more petty crime problems at local level (Garland, 2001), intelligence-led policing emerged from a need for new methods in the fight against organised crime. However in recent years net widening has taken place and the intelligence-led policing model is now applied to a much broader area (De Hert, Huisman & Vis, 2005). The difference with problem solving policing is less clear; and there is much discussion in what way these two models differ from each other. The models mainly differ at the conceptual level, whereby ‘intelligence-led policing’ is geared to finding (potential) individual offenders, while ‘problem-solving policing’ focuses on preventing crime opportunities (Tilley, 2003), however in practice both aspects may be present, but to varying degrees depending on parameters such as organised/individual crimes.

Characteristic for intelligence-led policing is its insistence to build up intelligence through all kinds of data collection strategies. Illustrative for these strategies is the UK Regulation of Investigatory Powers Act (RIPA) 2000, which regulates the powers of public bodies to carry out surveillance, investigation, and the interception of communications. These powers should be understood as part of an adaptive strategy in the sense that they were introduced to take account of technological change such as the growth of the Internet and strong encryption. Similar regulations were drafted in other countries. Also illustrative are the specific Acts in member states of Europe making possible and regulating the use of CCTV camera for the purpose of crime prevention and investigation.7

2.1.3. Non-adaptive strategies

Adaptive strategies postpone but do not eradicate the unconscious desire for aggressive and exclusionary punishments (Matravers & Maruna 2004: 126). Garland therefore argues that governments who are confronted with pressures, such as public outrage, media criticism and electoral challenges also turn to so-called non-adaptive responses to crime. The essential and enduring attractiveness of this response to crime is that it can be represented as an immediate, authoritative intervention. It gives the impression that something is being done: “Instead of acknowledging the limits of the sovereign state

---

7 See for example the camera law which is in effect in Belgium from 2007: http://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=nl&la=N&cn=2007032139&table_name=wet.
and adapting to them, the political agenda governing high profile policies was to ‘restore public confidence’ in criminal justice while asserting the values of moral discipline, individual responsibility and respect for authority. In penal policy as in welfare policy, the imperative was the re-imposition of control, usually by punitive means. In both cases the population singled out as being the most in need of control was composed of the welfare poor, urban blacks, and marginalized working-class youth” (Garland, 2001: 132).

Talking about several laws passed in the UK and US in the 1990s, Garland argues that non-adaptive measures are “passed amidst great public outrage in the wake of sensationalist crimes of violence, often involving a disturbingly archetypal confrontation between a poorly controlled dangerous criminal and an innocent, defenceless middle class victim” (Garland, 2001: 133).

Non-adaptive responses can be both reactive and proactive in nature and they can involve technology or be limited to physical police actions. Garland’s book predates the 9/11 attacks. Fine examples of non-adaptive reactions abound in the post 9/11 era; legislation at the European level and in member states was changed hastily to be able, for example, to give police more powers in keeping terrorist suspects in remand custody for a longer time, to stop-and-search people without reasonable suspicion, to use increasingly invasive surveillance techniques to try and identify potential terrorists, and to introduce a whole range of invasive airport security measures. Examples of more punitive forms of pre-emptive policing can be found in looking at how for example protestors are being policed in the context of mega-events such as the Winter Olympics in Vancouver and the G20 summits in Toronto and London. In all cases one of the police strategies was to arrest protestors that had a record of being ‘trouble-makers’ before they did anything wrong as a preventative measure. Similarly legislation that was passed in 2000 in the UK: the Terrorism Act gave police the power to stop and search anyone without reasonable suspicion. Similarly in 2002 a change of the local regulations in Amsterdam made it possible for police to stop and search persons within the city without any suspicion.
To conclude the discussion of the first trend is that the policing landscape is constantly trying to invent itself. There is a development to what has been called a pre-crime society where pre-emptive and proactive methods are becoming more and more the dominant mode of policing be it adaptive or non-adaptive. However there is no singular development. The landscape of police models is fragmented. More old-fashioned punitive policing methods exist in tandem with the more recent adaptive methods, such as community (oriented) policing and intelligence-led policing.

2.2. Surveillance policing

Next to the move to pre-emptive policing there is a second development that we would like to highlight in this contribution: the increased use of technology by the police. We hinted at this phenomenon while discussing intelligence-led policing. Recourse to technology is however not limited to strategies falling under this model. Take vehicle inspection security systems that inspect vehicles by taking pictures of the underside of vehicle checking for suspicious modifications. Implementation of this anti car bomb technology could very well fit strategies of problem oriented policing. In the press coverage the anti car bomb system was described as “a guardian that is never distracted, sleeps or tires” (Blackmore, 2011). These observations bring us to the issue of surveillance.

2.2.1. Surveillance

Surveillance is considered as one of the main institutional components of late modernity (Giddens, 1990; Haggerty & Ericson, 2000; Lyon, 2003). It is far from a completely new phenomenon in society; it is part of a broad continuing process of rationalisation, professionalisation and specialisation, which are characteristic of modernization (Marx, 2001). Denominating some practice as surveillance is not necessary rejecting it. More and more the use of the term has gained general acceptance. It is done by private and public actors and can be done overtly, covertly, directed or routinely (House of Lords, 2009: 12). It has always been an integral part of policing, but in recent decades surveillance technologies have been digitized and proliferated taking over more and more policing tasks, thereby changing the responsibilities of the police. The ability to easily and efficiently store, sort, classify, retrieve and match information in digital systems becomes increasingly significant within police work (Norris & Armstrong, 1999a). While surveillance used to be restricted to spying and undercover policing, now surveillance technologies are being used in all fields of policing. The result of these changes is that the main task of the police has now become to ‘front load’ the system with relevant knowledge that can later be sorted and distributed to interested institutional audiences (Ericson & Haggerty, 1997).

There are many definitions around, even legal ones such as the very precise (and not representative definition in the UK Regulation of Investigatory Powers Act. In section 48(2) of the Act, surveillance is described as the “monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications; recording anything monitored, observed or listened to in the course of surveillance; and surveillance by or with the assistance of a surveillance device.” (House of Lords, 2009: 37). Lyon’s much cited definition – “any collection and processing of personal data, whether identifiable or not, for

15 From the 16th century onwards the use by nation states of undercover surveillance techniques can be recognised (Marx & Fijnaut, 1995).
the purposes of influencing or managing those whose data have been garnered” (Lyon, 2001: 2) – is more useful for our purposes as we are mainly interested in contemporary or new digital surveillance. With digitisation comes information that is more amenable to storage, transmission and computation, as well as algorithmic surveillance (Introna and Wood 2004). Digital surveillance can be characterized on a technological level by the use of latest technologies and by features such as pervasiveness, greater intensity, greater speed, action at a distance, interconnection, social sorting (aimed at categorizing and profiling based on risk or probability, automation (driven by computer systems and using algorithms to analyse collected data; simulation and pre-emption (tending towards anticipation of possible actions, risks), data doubles (Ball, 2009: 22). The changes brought about by the digitisation of surveillance technologies are not merely quantitative (in terms of size, coverage, speed, intensity, etc), but also qualitative.

‘New’ surveillance technologies such as CCTV, databases and predictive software allow the police to increase their fields of vision and to simultaneously collect evidence. The main motivations that are given for the implementation of surveillance technologies by policy makers and policing, are that technologies increase the crime fighting capacities of the police and provide better services to the community, so make policing more effective and efficient. In addition it is contended by some that there is a cost-benefit in the long run, in the sense that the deployment of these technologies would be cheaper than the equivalent in staff (Dupont, 1999; Norris & McCahill, 2003). Vendors never defend surveillance as such but propagate use and further development on an ad hoc basis. CCTV, for instance, is presented as "a vital weapon in the prevention and detection of crime and in reducing fear of crime, used comprehensively as a tool by the police and contributing significantly to the evidence produced in thousands of investigations obtained from publicly and privately operated systems” (British Security Industry Association, 2009). Its ‘proven record’ contains the identification of the London bombers (2005) and the Jamie Bulger case (1993) and one can expect only ‘real rewards’ from further developments such as facial recognition and behavioural analysis (British Security Industry Association, 2009: 394). The House of Lords’ report Surveillance: Citizen and the State critically reviews both the enthusiastic and the more critical views on CCTV and concludes with the recommendation for more independent appraisal of the existing evidence (House of Lords, 2009: 22). Interesting is the subsequent section on the advantages of all kinds of surveillance activities in the context of e-government allowing the government to provide better and faster public services. “Through the intensive analysis of large collections of personal data, it is now possible for government to be more ‘citizen-focused’ and for services to be better tailored to individual needs and circumstances” (House of Lords, 2009: 24).

2.2.2. The role of technology: neutral?

In the sociological and criminological literature on new policing models the role of technology has often been neglected and is seen as not having such a great influence on police practice. Ponsaers (2001), for instance, observes, referring to amongst others, Manning (1992), that new technologies are a tool to aid police work and can be fit into almost any police model. Furthermore, they do not essentially change the underlying code of police work and the ways in which the police use technologies is in a reactive way. In similar vein there is little attention to the role of technology in Garland’s The Culture of Control. A technology respectful analysis, taking into account insights from science and technology studies research, which is also gaining more and more attention
in surveillance studies literature (Lyon, 2003; Monahan, 2006; Sætnan 2007; Martin et al 2009; to name a few) could enrich these analyses of contemporary criminal justice policies. In between technological determinism and technological disregard or instrumentalism, there is a growing body of literature (Ihde, 1990; Jonas, 1979; Winner, 1986; Latour, 2002/2005) in which a complex but interactive relation between technologies and human behaviour is underlined; it provides views on how technologies themselves transcend the inanimate and can become agents in social processes. Technology is seen to have agency in much the same ways as human elements of the organization. “Those who believe that tools are simple utensils have never held a hammer in their hand, have never allowed themselves to recognize the flux of possibilities that they are suddenly able to envisage” (Latour, 2002: 250).

Technology is important, no matter how its role is presented. Everybody agrees that the 9/11 terrorist attacks led to an intensification and acceleration of the development of surveillance technologies (Lyon, 2004; Ball & Webster, 2003). Equally there is agreement that these technologies in combination with the significant developments in storage capacity of computers and new software possibilities, have allowed a fundamental new criminal justice policy. Hence, one can safely conclude that the distinctive technologies seem to be one of the defining characteristics of modern policing. But is it really that daring to go one step further and suggest that modern policing is partly shaped by the technologies at hand, as partly ‘enabling’ factors, rather than passive, desired tools?

The fact remains that we are trying out new ideas today, ideas that would have sounded unsound only some time ago. Ball and others point at obsession with risk, militarisation, economics and the information society as “reasons for the spread and intensification of surveillance”, thus avoiding to take an explicit stand on the proper role of technology, but they state nevertheless that the “characteristics and systems lead to increases both in targeted and mass surveillance” in contemporary society (Ball and others, 2009: 23). Targeted surveillance is understood as surveillance of distinct individuals or groups, for a particular purpose, whereas mass surveillance refers to the undifferentiated and general surveillance of the population as a whole. Ball and others make the following breath taking observation: “Both of these take place, but the re-emergence of mass surveillance (which had been a key part of the authoritarian regimes of the mid-Twentieth Century) and the much greater use of intensive targeted and pre-emptive surveillance poses particular problems for constitutional rights in democracies” (Ball and others, 2009: 23). We like to believe that not all this is the result of a malicious plan of some. Although we do not find any reference to Latour in the final report of the House of Lords, there are important paragraphs on ‘the role of technology’ and ‘the availability of technology’ next to other explanatory features (House of Lords, 2009: 15-17).

The foregoing does not want to downplay human agency, but leave the door open for an understanding of complex interrelations. Prudence with big explanatory schemes is warranted, as are generalisations about ‘technologies’. To see what (police) men do with technology, and what technology does with (police) men, a sustained effort to understand specific technologies, produced by industry but subsequently used for a variety of anticipated and non-anticipated purposes needs to be the starting point. CCTV remains a fascinating technology and an example of how the implementation of
surveillance technologies not only conveys features from old and new penology, but also from the adaptive and non-adaptive strategies. Norris & McCahill (2006) have shown that although CCTV operators are using ‘post-modern’ technology, they interpret the images on the screen through a mind’s eye that is steeped in a modernist conception of crime. The ‘surveillance gaze’ is mediated by the selective concerns of the operators and as studies of the routine operation of control rooms have shown, the targeted gaze of CCTV cameras does not fall equally on all sections of the population and categories: for instance age, ethnicity and gender have a big influence. The authors conclude that “rather than representing a radical break with the past, the operation of CCTV merely gives an electronically mediated twist to that very old-fashioned mantra of ‘round up the usual suspects’” (Norris & McCahill, 2006: 114).

2.3. Profiling

Profiling brings our two trends (pre-emptive policing and surveillance policing) together. The idea of profiling is not new, different types of offender profiling have been around since the 1960s, whereby two main types can be distinguished: inductive and deductive. Inductive profiling draws on the known characteristics of a general criminal population to ascribe characteristics to a specific offender. It often makes use of any available statistical analysis of quantitative data gathered from convicted offenders to make generalisations on behavioural patterns (Ainsworth, 2004). Deductive profiling, on the other hand, focuses on the case-at-hand, and attempts to develop a set of characteristics that are incident specific. It does not rely on generalities from sample groups. It is a, “forensic evidence based, process–orientated, method of investigative reasoning about the behaviour patterns of a particular offender” (Turvey, 1999).

2.3.1. Pre-emptive profiling

New digitised pre-emptive profiling techniques that are characteristic of the new pre-emptive surveillance techniques being used by the police are based on inductive profiling. The main purpose then is to cluster data in such a way that information is inferred and predictions or expectations can be proposed. The profiles obtained are patterns that are the result of a probabilistic processing of data. They do not describe reality, but are detected in databases by the aggregation, mining and cleansing of data. The profiles are based on correlations and therefore cannot be considered as causal relations (Gutwirth & Hildebrandt, 2010). In contrast with traditional criminal profiling, the decision-making is done by machines and not humans, becoming difficult to trace back where certain motivations behind the decisions come from (Lessig, 1999).17

Inductive profiling is a key element to the predictive policing model described above. Exemplary are the pre-crime databases. Although several types can be distinguished, they all have one thing in common namely trying to prevent crime before it happens by using digitalized profiling techniques. A first example of this type is predictive software, which is already used by police in Baltimore and Philadelphia and was developed by

17 “When the system seems to know what you want better and earlier than you do, how can you know where these desires really come from? (...) profiles will begin to normalize the population from which the norm is drawn. The observing will affect the observed. The system watches what you do; it fits you into a pattern; the pattern is then fed back to you in the form of options set by the pattern; the options reinforce the patterns; the cycle begins again” (Lessig 1999: 154).
Richard Berk, a professor at the University of Pennsylvania. It predicts which individuals on probation or parole are most likely to murder or to be murdered. In his latest version, which is being implemented in Washington D.C., the software goes even further, identifying the individuals most likely to commit crimes other than murder (Bland, 2011). Berk et al (2009) assembled a dataset of more than 60,000 various crimes, including homicides. Using an algorithm they had developed, they found a subset of people much more likely to commit homicide when paroled or probated. Instead of finding one murderer in 100, the researchers could identify eight future murderers out of 100.

A second type of pre-crime databases is the E-CAF system, which was introduced by the former Labour government in England. This is a web-based IT system designed for use by practitioners and managers who use the Common Assessment Framework as part of their work with children. Originally it was developed within the crime prevention framework (the Ryogens database); but after criticism, it was reframed within the child protection framework. Characteristic of this policy initiative, in combination with a new Children’s act in 2004, and developments in criminal justice policy was the recommendation that to increase the efficiency in crime prevention and child protection initiatives, public services needed to be joined up to improve communication. In line with this, several public services have access to the ECAF database, including police, social services, housing services, schools to name a few. The idea behind the database is to have a way of predicting which children will commit crime in the future and to intervene before it is too late. The system works on the basis of profiling and risk factors for delinquency that have been suggested in crime prevention research. The database makes a decision about the need for further intervention on the basis of the risk score that is assigned to a certain child (van Brakel, 2010).

Modern surveillance based on inductive profiling, in a benevolent perspective (hoping that it works), fits Garland’s definition of an adaptive strategy; creating new strategies to deal with perceived problems. Crime can be everywhere and needs to be detected everywhere. Would-be bombers and would-be dangerous children are amongst us, thus everybody needs to be watched and processed in databases. The two examples of existing pre-crime databases discussed above allow us to explain more in-depth what kind of surveillance technologies are being used by police nowadays. They give a flavour of the type of surveillance technologies that are being developed.

2.3.2. Bringing the trends together: the Dutch Border Controls Framework

Perhaps the most complete example, rich in ingredients, which we came across is the initiative of the Dutch Minister of Justice Ballin to coordinate border controls as an instrument against terrorism, presented in the Framework document Border Controls (Ballin, 2009a and 2009b). The initiative saw the light after a very critical report by the Court Of Audit of the Netherlands (2005). This independent body (‘Algemene

---

18 More information about the ECAF can be found here: http://www.education.gov.uk/childrenandyoungpeople/strategy/integratedworking/caf/a0072820/national-ecaf
22 See for example project INDECT, http://www.indect-project.eu/.
Rekenkamer’) is empowered to audit the spending of the Dutch government on its efficiency and legitimacy. In its 2005 report ‘The Use of Border Controls to Combat Terrorism’ the Court found that Dutch border controls were an inadequate means to combat terrorism. Checks of goods and persons are not integrated; many travellers and goods were not checked and information on incoming ships and aircrafts was often inadequate or not available on time. The report did not come by accident. The Minister of Justice, responsible for combating terrorism, after September 11, 2001, had announced his intent to use borders as anti-terrorism instruments and was going to develop policy in this area. In the 2009 Framework document ‘Border controls’ the responsible minister looks back at the analysis of the Court of Audit and first sketches the policy context. Of course border controls cannot be complete since a balance has to be found ‘between the control and security interest and other economic interests of the Netherlands in a smooth and customized handling of passengers and goods’. So not deterring people and traders to choose the Netherlands as a hub is a prime objective.

The solution is technology and integrated risk assessments and analysis. This will be the cement of a solid, future-oriented system of border control.

All services involved in border control, such as the Royal Military Police, Customs, Seaport Police and intelligence agencies need to share their information together, together with private partners involved in border traffic. On this basis, a comprehensive profile of a passenger and his luggage will be drawn, to assess whether the person needs extra controls (Ballin, 2009a and 2009b). Profiling makes differentiation in passenger flows possible. Through this differentiation, the focus will be on those passengers with an increased risk in the context of illegal immigration and organized crime, and less on ‘bona fide passengers.’ Hence, differentiation will positively effect on the attractiveness of the Netherlands as a business and tourist destination. Is there any better proof of profiling and pre-emptive policing becoming part of the mainstream policy language?

Although the introduction of (pre-emptive) surveillance technologies can seem to have changed the whole idea of crime control as Marx observed in 1988: “Control is now better symbolized by manipulation than coercion, by computer chips than prison bars, and by remote and invisible filters than by handcuffs and straitjacket” (220), when taking into account Garland’s culture of control it is clear that the old-fashioned punitive strategies have not gone at all and are used in tandem with the adaptive strategies. Exemplary are the UK Anti-Terrorism Crime and Security Act 2001 and Prevention of Terrorism Act 2005 that give wide powers to stop and search to police. Guilt need not be proved to the reasonable doubt standard, suspicions as the nature of certain associations and activities that would not support a conviction can nevertheless support the imposition of such measures. Where no criminal offence appears to apply, intervention can nevertheless disrupt a budding terrorist conspiracy. The decision to impose the measures can be retained in executive hands, meaning that a rapid response to information obtained can occur. Security service material does not have to be presented in the form of evidence: thus sources can be protected, and use of certain methods, such as employing intercepts, can remain secret (Fenwick 2010).

Let us now turn to our second part discussing some of the consequences of these technologies and the trends outlined above. In this second part we will focus on the intended and unintended social consequences and legal challenges of these trends, which should be seen as intertwined with each other. What follows is a selective account...
of some of the possible consequences, one that builds further upon the trends that we chose to discuss in the foregoing.

3. Part 2. Critical Assessment

In the House of Lords’ report *Surveillance: Citizen and the State* at least four ‘disadvantages’ of surveillance are identified: the threat to privacy and social relationships, declining trust in the state that acts on categories and from a distance, discrimination and threats to security due to large scale storing of more data (House of Lords, 2009: 26-29). A significant amount of literature has been published about privacy consequences of new surveillance technologies, however a lot less attention has been paid to other unintended consequences that arise as a result of the use of surveillance technologies and more specifically use of the technologies by the police. In this second part of the paper we will start by a critical exploration of some of the most important consequences of the use of surveillance technologies by police followed by a critical assessment on how legal institutions and actors deal with and react to the implementation of these new technologies and what significant issues arise.

3.1. Unintended (social) consequences

3.1.1. Suspicion, identity and discrimination

One of the consequences of the use of surveillance techniques and technologies, which are used in pre-emptive policing, is social sorting: they sort people into categories assigning worth or risk; this is done on the assumption of a certain idea of what is the norm (Lyon, 2003). Non-confirmation of this norm is seen as suspicious. Often this social sorting mechanism translates into the filtering of people’s identities into categories of inclusion and exclusion based on informational data by which relevant authorities enforce and naturalize social inequalities (Monahan, 2006). Passenger profiling practices, which were discussed above are an excellent example of this process, whereby certain marginalized and already discriminated groups in society who carry distinct characteristics (for example Muslim community) are targeted even more by having to undergo a series of tedious security investigations before they can board a plane as they are considered more suspicious than other groups who conform to the current norm and on the other hand people such as business travellers who already enjoy a lot of advantages in society are able to get preferential treatment trough positive profiling mechanisms such as fast track boarding.

Discriminatory effects reveal themselves very clearly in non-adaptive police strategies. According to Garland, many non-adaptive responses are rooted in a “criminology of the ‘alien other’, which represents criminals as dangerous members of distinct racial and social groups which bear little resemblance to ‘us’.” The clearest example of this can be found in the case of stop and search practices by the police, especially in the United Kingdom (Norris, 1992; Dodd, 2010). However from our discussion above it can be inferred that this “criminology of the ‘alien other’” is not just present in non-adaptive strategies but also raises its ugly head in adaptive or more mixed strategies as was clearly demonstrated
by the case of CCTV (Norris & Armstrong, 1999b) discussed in section 2 in part 1. And is also clearly present in the case of passenger profiling.23

However, more recently adaptive strategies have been implemented, which extend the category of the ‘the other’ to people that do not look obviously different or do not carry plain signs of belonging to a different group than ‘ourselves.’ These strategies have been introduced to deal with the problem of racial profiling practices and pride themselves of not being discriminating. Potentially dangerous individuals are now identified on the basis of their behaviour instead. Their ‘otherness’ comes from the strangeness of their hidden motives, leading them to commit deviant acts that can be rendered visible through behaviour that will generally be considered normal, or at least, not deemed suspicious before. Exemplary of these ‘responsibilisation’ strategies (see above) have been the anti-terrorist campaigns that have been launched by the London Metropolitan Police in recent years and several similar ones in other European countries and North America, where different variations of the slogan “if you suspect it report it”24 address normal citizens to be responsible for their own security and report anything that might seem suspicious behaviour.25 Questions need to be addressed about what is ‘normal’ and ‘abnormal’ behaviour;26 furthermore, the judgements of the police or security officers involved might still be based – be it unconsciously or consciously – on racial stereotypes (see our discussion of CCTV in part 1).

By shifting definitions of suspicion or otherness from an ‘orientalist’ discourse to behavioural patterns has implications for social cohesion. Whilst it is argued that before social cohesion was sustained by ‘threatening others’ that were easily recognisable, now everyone becomes suspicious. This development is not just a result of anti-terrorist policy but should be seen as part of a much larger development within policing and government policy. More and more police officers are using this same discourse in relation to petty crime and in defence of installing more and more CCTV, as recent declarations from an interview on Belgian television with a Flemish police commissioner illustrate in relation to the instalment of more CCTV.27 Evidence from the House of Lords report on surveillance shows that the increased emphasis on record-keeping and centralized databases by the government undermines the presumption of innocence by making anyone who is not willing to provide requested information to government a target of suspicion. In the words of Norris “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

---


25 So for example after the July bombings in London in 2005 David Mery was arrested because the police thought he was suspicious. Some of the reasons they gave him to warrant his arrest included: “he went into the station without looking at the police officers at the entrance or by the gates, i.e. he was ‘avoiding them’; two other men entered the station at about the same time as him; he’s wearing a jacket ‘too warm for the season’; he’s carrying a bulky rucksack; he kept his rucksack with him at all times; he looked at people coming on the platform; he played with his mobile phone and then took a paper from inside his jacket.” David Mery, http://gizmonaut.net/bits/suspect.html#action.

26 For example are police officers to be trained in recognising when someone who is acting abnormal actually has a psychiatric disorder and how will for example a smart CCTV system be able to recognise this?

do something wrong. this is promoting a view that as citizens we cannot be trusted” (House of Lords, 2009: 27).

3.1.2. Accountability, trust and function creep

Part of the development towards pre-emptive policing consists in engaging a plurality of actors other than the police and bringing data together regardless of the (public or private) source. Everybody needs to cooperate to prevent risks from happening. Sound as the idea may look, it can have had certain undesired consequences with regard to expectations concerning accountability. The more actors involved, the more likely people will assume that someone else is responsible if something goes wrong. Also, when hierarchy has not been clearly defined, people will not know who is responsible (see Maes et al 2010). Take the example of public-private partnerships. A private company has a contract with the government or police to monitor the offenders who are electronically monitored, but it has not been clearly stated in the contract when the private company should notify the police. When an offender decides to abscond, this can result in a situation where it is not clear who should be held accountable, a situation that might worsen when the offender commits another crime (Maes et al, 2010).

With the increased use and ‘responsibilisation’ of surveillance technology, it becomes tempting to blame the technology when the risk effectuates itself with the result that no one will be held or feels accountable. A problem of accountability might rise when somewhere in a chain data is enriched through data mining and profiling. Who is responsible for the new data thus conceived? Can the source still be held responsible? Or is it the user of the profiled data? Finally there is the problem of the interface between facts and interpretation. Decisions that are made by the technology are less flexible, less open for interpretation and are de-contextual compared to their human counterparts. The main difference between deciding on whether someone is suspicious or not by a human actor (the police officer) or the technological artefact (the software/computer) is that the police officer can take into account unexpected factors and the context in which something happens, while the computer can only make a decision on the basis of the information that is entered into the system.

In the previous section we saw that by laying an increasing emphasis on surveillance and the collection of data, governments are sending a clear message of distrust to members of the public. Accountability gaps as discussed here might cause loss of trust in the state. The House of Lords’ report goes one step further by suggesting that the sheer act of surveillance might cause this effect and create feelings of insecurity, unwillingness to co-operate and has the potential to generate resistance (House of Lords, 2009: 27). A bit of distrust towards the state is proper to all modern constitutional state. The lesson of history suggests that states can and do fall prey to malign regimes. A line is crossed when infrastructures are created that would greatly enhance the capacity of the government to collect data and to do harm (Ball, 2009: 24). Too much trust accorded to government is a reason for distrust. Similarly, wide powers given to police to stop and search can trigger distrust and resistance. Fenwick discussing the Anti-Terrorism Crime and Security Act 2001 and the Prevention of Terrorism Act 2005 warns for loss of human rights credibility, handing a propaganda tool to radical groups, and the possible alienation of certain communities, leading to the fomenting of radicalism. Recruitment to radical
groups linked to terrorism may be aided, and within certain communities information as to planned attacks may not be passed to police (Fenwick 2010).

The general recommendation speaking to us from the evidence collected by the House of Lords is that governments should shy away from those forms of surveillance that reduce trust, in particular secret surveillance, unnecessary mass surveillance and consent-less surveillance. Norris, one of the academics giving evidence, particularly stresses the relevance of this for policing. Pre-emptive surveillance promotes the view that everybody is untrustworthy and will never respect initial self-constraint because these kinds of ‘surveillance solutions’ are expansionary to a huge degree: “If you see that information is what you need to solve a problem but you do not quite know what that problem is and you do not know what future events you are going to be responding to, the temptation is to collect all information about all people, and that is in a sense partly the way that things have gone” (Norris & Murakami Wood, 2009: 24). Surveillance for pre-emptive purposes does not only thwart with checks and brakes, it also distances the police from its public. “The best way for police to solve crime is if the public gives them information freely. It is if the public trust the police that there is that flow. That is about a reciprocal relationship” (Norris & Murakami Wood, 2009: 24). An unreflective turn of policing towards pre-emptive surveillance can lead ‘official’ policies of community policing astray and create a police that actually see themselves as standing outside the community and coming down in a sense from the mountain to impose order rather than a police that are an integral part of that community who have to negotiate, sometimes with discretion and toleration, with various communities and individuals but, in that process of trade-off, what one does is build up trust and consent and consent is at the heart (Norris & Murakami Wood, 2009).

A final important consequence that should be mentioned is function creep. The faith in technological solutions and the inherent expansionary tendency of surveillance solutions explains this phenomenon: the use of surveillance technologies in areas or for a purpose for which it was not originally intended. The world got used to the police massively using Google Earth for exploratory purposes. Also many countries made possible an extension of DNA sampling for ‘ordinary’ crimes (Prinsen, 2008). Other examples are less known, but hardly less breathtaking. The House of Lords’ report contains an in-depth analysis of UK local policing using the Regulation of Investigatory Powers Act 2000 for detecting petty crimes such as littering and also for example in April 2008 a council in Dorset used the Act to spy on a family for nearly three weeks to find out if they were lying about living in a school catchment area (Schlesinger, 2008), a situation that the UK legislator acknowledged by amending the said Act in 2003 (House of Lords, 2009: 31, 40).

3.2. Law as a framework for surveillance solutions?

Some surveillance practices are too benign for regulation. Think for instance about the police using open sources and Google Streetview. The more extensive or important practices are often introduced via specific regulations. We already discussed the stop and search powers in the Anti-Terrorism Crime and Security Act 2001 and Prevention of Terrorism Act 2005. The UK Regulation of Investigatory Powers Act 2000, also touched upon above, is another fine example. On the one hand it criminalizes the intercepting of a communication over a public network without consent or a warrant authorized by the Secretary of State. On the other hand it offers a legal definition of surveillance and
establishes a framework for the use of surveillance and data collection techniques by the police, the security services, and other law enforcement agencies. The second feature is predominant. The bulk of the Act concentrates on setting out the circumstances under which public authorities – most notably the police – can engage in various types of surveillance activities with authorization and review of those activities by the Office of Surveillance Commissioners (OSC) and the Intelligence Services Commissioner (House of Lords, 2009: 36-37). Our example shows that regulating certain practices and enabling practices are often one and the same. What frames regulation? In his oral evidence to the House of Lords Norris explains the growth in surveillance in the UK by pointing at the poor constitutional safeguards (“because there has been little to stop it”), compared to countries such as Germany with more protective elements in their constitutional regimes (Norris & Murakami Wood, 2009), a statement that has been confirmed by a recent comparative study. In particular constitutions with provisions on privacy and human dignity are recognized critical backgrounds for discussion of surveillance technology (Leenes, 2008).

The existence of general data protection laws in most Western States covering all new technologies and aiming to protect subjects whose data is being processed, do not seem to provide sufficient safeguards for the issues arising from surveillance, and this for many reasons. We name only a few. First there is the benevolence of these laws for processing done by governments that can easily create statutory gateways that override the need for consent in the Data Protection Act, which can be seen as one of the major protections. This happens repeatedly and especially in cases where the general data protection acts would not allow the sharing of information. By use of statutory duties to process and share data that bypass the consent requirements, the general acts lose all meaning (Dowty & Munro, 2009: 277). Secondly, there is the frequent use in these statutory gateways of broad discretionary powers to allow the processing and sharing of the information, a situation that the general data protection acts seemingly do not appear to limit. Dowty gives the example of information shared on the basis of a general duty on a local authority to prevent crime in their area or to reduce youth offending. “That is then used to justify specific instances of information sharing about an individual. Suddenly the line becomes very blurred. How far do we go to stop crime occurring in an area? Does this broad power allow the police to enter your house and search for stolen goods? Presumably not. Why does it allow information to be shared, but it seems the Data Protection Act does not stop that?” (Dowty & Munro, 2009: 277-278).

National and general data protection laws therefore need to be strictly enforced and complemented with specific legislation. In the latter case, it is however observed that legislators either create solely enabling legislation that refers essential elements of the regulation to secondary, often unchecked legislation, or create abstract legislation with few concrete provisions on the rights of the citizens, remedy and compensation. An example of the former is the Identity Cards Act 2006 (Hosein, 2009). An example of the latter is the Regulation of Investigatory Powers Act 2000 fuzzy about judicial control and close to silent about redress, compensation and informing the subject of surveillance of that surveillance, when completed, where no investigation might be prejudiced as a result (House of Lords, 2009: 39). The EU does not better. In general most EU legal Instruments such as the proposed regulation for a European processing of passenger data include the ‘usual data protection rights’ such as the right of access, rectification, and erasure. However they seldom include strict deadlines within which these requests must
be met or fulfilled. Equally, these regulations mention as a rule a right to compensation and a right to judicial remedies for any breaches, but the scope of these rights is left to the scrutiny of the national legislators. In practice the added value is very limited, since the absence of strict rules on the liability of the different authorities involved does not allow the competent judicial or administrative authorities to impose sanctions when necessary (Brouwer, 2009).

Political weight is used to introduce new surveillance and pre-emptive friendly features. The pressure of the United States to accept technologies such as PNR and Swift is well known. Fenwick highlights Labour pressure to pass UK legislation abandoning of the requirement that police can only intervene on suspicion. Public and the judges were ‘asked’ to understand and accept (Fenwick 2010). The laws were passed, but in general the political strategy was and remains not wholly successful due to resistance by the English and the European Court on Human Rights. This brings us to the theme of legal resistance that will be dealt with in our next section.

3.2.1. Legal resistance against aggressive pre-emptive surveillance solutions

Recently there has been quite a lot of attention from both the European courts and legal academics to what extent existing rules on human rights can already offer protection for aggressive pre-emptive strategies and against emerging technologies, pending more specific legislation. A lot of this attention has focussed on data protection and privacy issues. The House of Lords’ 2009 report Surveillance: Citizen and the State makes no less than 44 recommendations to protect individuals from invasions of their privacy related to surveillance and data collection. One recommendation targets the use of the RIPA powers by local authorities and local police. This should either be prohibited or tied to the investigation of serious criminal offences, which would attract a custodial sentence of at least two years (House of Lords, 2009: 43). In June 2010 the Council of Europe elaborated a (first) Recommendation on the regulation of profiling by European member states (Council of Europe, 2010).

At the academic level, there is a growing body of legal scholars for surveillance practices (see the many contributions in Hildebrandt & Gutwirth, 2008). Scholars, such as Solove, question current legal understandings of privacy in the light of new technologies and elaborate new conceptions for use in courts to better balance privacy concerns against perceived benefits from the use of technologies such as profiling and data mining (Solove 2001 & 2007). Ideas about the ban on automatic profiling or decision-making processes that has been laid down in article 15 of the Data Protection Directive,28 for instance, seem valid starting points, but in practice appear to be insufficient to guarantee efficient legal protection (De Hert & Gutwirth, 2008). Absolutely promising is the research by Brouwer taking stock of the many existing regulations on anti-discrimination and protection of minorities and investigating their relevance for profiling practices (Brouwer, 2009).

---

28 Art 15: The processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal of the European Union, L 281, 23/11/1995 P. 0031 – 0050.
A very important line of principle developed by the Court on Human Rights has to insist on the transparency of the pre-emptive and surveillance solutions when these touch upon human rights. If the legislator decides to implement these solutions then it needs to be done on the basis of a clear legal basis describing the modalities, the limits and the checks and balances. The legality requirement is incorporated throughout the European Convention on Human Rights. European human rights are seldom absolute, but limitations can only be created on the basis of a ‘law’. The definition of what is a law is a matter for the European Court not the national authorities. Although national authorities may declare that they have a law that is adequate for the purpose of justifying an interference with a specific right, it is for the European Court to decide whether the legislation that the state puts forward fulfills the requirements of law according to the court’s definition (Guild, 2009: 8-9). The key feature is that it must be formulated with sufficient precision indicating with sufficient clarity the scope of discretion of the authorities to enable the individual to regulate his or her conduct (foreseeability) and must afford adequate legal protection against arbitrariness (adequacy). One understands immediately that a strict application of this requirement of a legal foreseeable and adequate legal basis can be of a nature to stop all non-adequate pre-emptive or surveillance solutions and even to hinder adequate solutions (adequate in Garland’s terms) that are imposed without due attention to transparency and checks and balances.

In Gillan and Quinton v. United Kingdom29 the European Court held that stop and search powers by law enforcement in the UK violate privacy, because they are “not in accordance with law.” Under sections 44-47 of the Terrorism Act 200030, police in the UK gained power to stop and search people without any requirement to first form a reasonable suspicion of unlawful behavior. The Court held that the extraordinary breadth of power given to police under the Act lacked appropriate legal safeguards capable of protecting individuals against arbitrary interference. Finally also the risks of the discriminatory use of the powers against black and Asian persons was acknowledged. Statistics accepted by the Court showed that black and Asian persons were disproportionately affected by the UK police powers.

The same strict line was also followed in a case concerning digital surveillance, a case that led to the judgement Liberty v. United Kingdom.31 In this case the European Court of Human Rights held that a system of mass surveillance operated by the UK government to spy on all telephone calls, faxes and emails to and from Ireland, was in breach of the right to privacy under Article 8 of the European Convention on Human Rights, since relevant domestic law did not indicate with sufficient clarity, the scope or manner to intercept and examine external communications and did not foresee adequate legal protection against abuse of power.

3.2.2. Checking on transparent pre-emptive surveillance solutions

Of course one can rightly wonder what would happen when member states start imposing pre-emptive and surveillance solutions fully abiding to the requirement of

29 Gillan and Quinton v. the United Kingdom, Application no. 4158/05, European Court of Human Rights, Judgement of 12 January 2010.
31 Liberty and others v. the United Kingdom, Application no. 58243/00, European Court of Human Rights, Judgement of 1 July 2008.
a clear legal basis? What in human rights law can hamper the official and transparent surveillance state? The answer to that is twofold. Firstly, one should understand that transparency is already more than half of the answer: it allows parliamentary, democratic and individual scrutiny. It allows debate and revision. Second, and this is the other side of the story, there is the requirement in human rights law that a rights limiting initiative should not only have a legal basis, but should also respect the proportionality requirement. Article 8 of the Convention requires the European Court to reject any interference with privacy that is not justified as “necessary in a democratic society”. An interference will be considered “necessary in a democratic society” for a legitimate aim if it answers a “pressing social need” and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are “relevant and sufficient” (Guild, 2009: 8).

This “quite a shopping list of elements to assess” (Guild, 2009: 8) was at the core of the discussion in the seminal S. and Marper v. United Kingdom case32, which addresses the need for proportionality in a context very close to this of the pre-crime databases discussed above. The case concerned two non-convicted individuals who wanted to have their records removed from the DNA database used for criminal identification in the UK. In its ruling the Court concluded that the blanket and indiscriminate nature of the powers granted to UK authorities, constituted a disproportionate interference with the applicants’ right to respect for private life, and could not be considered as necessary in a democratic society, amounting therefore to a violation of Article 8 of the ECHR.

The storage and retention of the data in question raised several issues. First the mere storage of such information conveys in itself a risk of stigmatization. A second issue raised, is that even though the Court acknowledged that two separate logics are in place in this kind of system: the original collection of information aims at linking a particular person to a particular crime of which he or she is suspected, whereas the retention of such data aims at another, different, purpose, i.e. assisting in the identification of offenders of future crimes. The question arises here if it is proportionate and necessary in a democratic society, to store the personal data of innocent individuals for the sake of preventing the committal of future, and perhaps never to be committed crimes, even when there is no particular indication that such future possible crimes will be committed, and there is no relation whatsoever between the individuals whose data is processed and the yet uncommitted crimes? (Gonzales Fuster et al, 2010).

In the House of Lords’ report the use of DNA as a tool to treat people as suspects for any future crimes was singled out (House of Lords, 2009: 45). The Lords equally received testimony of police men and policy makers denying any stigmatization of being processed in the DNA database: “By contrast, the NPIA argued that “inclusion on the DNA Database does not signify a criminal record and there is no personal cost or material disadvantage to the individual simply by being on it.” McNulty insisted that “there are no guilty people on [the NDNAD] in the sense of guilty of future charges” and that “it is not an information source for all the naughty and potentially nasty people in the country ... It is purely an informational and investigatory device for the police.” He dismissed the suggestion that the Government was saying that “we have all these people on the database, they all must be guilty, now let us find a crime to attach to them” and he went on that “I

---

32 S. and Marper v. the United Kingdom, Applications nos. 30562/04 and 30566/04, European Court of Human Rights, Judgement of 4 December 2008.
do not think there is a matter of principle here; I do not think there is any stigma attached at all with being on the database” (House of Lords, 2009: 45-46). Although the European Court did not express itself clearly on the disproportionality of the pre-emptive logic of DNA sampling, it clearly saw the risk of stigmatization. The importance of Marper is that it puts an end to misleading presentations about DNA-sampling, as it is “purely an informational and investigatory device for the police”.

The insistence of the Court in Marper on the issue of discrimination also needs to be welcomed. Interesting in this respect is a judgement by the Court of Justice (the EU Court that is vested in Luxemburg). The Heinz Huber v. Germany case33 dealt with the existence in Germany of a centralised, nationwide database containing information on non-German EU citizens, for the sake of applying the law relating to the right of residence, and its use by German authorities to fight crime. In its assessment, the European Court of Justice took the view that, as the fight against crime necessarily involves the prosecution of crimes and offences committed irrespective of the nationality of their perpetrators, it follows that, as regards a member state, the situation of its nationals cannot be different in relation to this objective from that of non-national EU citizens resident on its territory (Gonzales Fuster et al, 2010).

More interesting European cases can be singled out, but we think we have provided the reader with enough material to make our point. Our highest European Courts are progressively speaking to us on the issue of pre-emptive policing and surveillance and their message is clear: proportionality, non-discrimination and law-guaranteed transparency of police powers need to be mandatory starting points for the regulation of it. It remains to be seen whether this message will be picked up and whether the European Courts maintain their strict approach. Also, it is wise to assume that law cannot deal with all unintended consequences discussed above. Other mechanisms need to come into play (think about ethics and culture). However, as law is an instrument of power in Western society it is absolutely necessary that it is involved in discussions about unintended consequences of the use of surveillance technologies by police.

Again it should be underlined that law also plays an enabling role: it is the instrument by excellence that explains consent-less based governmental surveillance. Some acknowledge the safeguarding due process role of law, but tend to think of it as an instrument that in general broadens the legal foundations of surveillance practices (see Marx, 1988). Increasingly, then as developments in science and technology enhance police surveillance “due process” is gaining less and less relevance to contemporary police actions and the law as an agency of surveillance and legitimization changes in tandem (Ericson & Haggerty, 1997).

4. Concluding remarks and discussion

In our analysis we made use of Garland’s theory of adaptive and non-adaptive strategies as a way of understanding changed and unchanged policing patterns. Probably the distinction between and adaptive and non-adaptive strategies should be understood in a non-dualistic way. Responses to new public order and crime challenges should be seen as more fluid, with new police models incorporating both adaptive and non-adaptive

33 Huber v. Germany, European Court of Justice, Case C-524/06, Judgement of 16 December 2008.
strategies as was illustrated in section 2.2.1. In our feeling, although writing before 9/11, Garland in his analysis, neglects the increased use of surveillance technologies and technology more in general, in shaping the latest police strategies and crime control policy. Surveillance technologies are an integral part of both intelligence-led policing and of pre-emptive policing. They do not only characterize these police strategies in a substantial way, but also raise important social and legal issues.

In the second part of the article we discussed several social and legal consequences as a result of the changing policing landscape that was discussed in part 1. We started this part with highlighting that several social issues that were already an issue within policing, referred to by Garland as the ‘criminology of the alien other’ are not solved by using surveillance technologies and that in fact technology often only strengthens these social sorting processes. Both strategies geared to identification of groups and of individual offenders can be recognised in recent strategies of crime control. It can be concluded that the importance of identification has been a longstanding goal of policing and the consequences of social sorting are ingrained in this type of technique. Although the increased use of surveillance technologies is giving police and law enforcement more and more possibilities and is changing the way they work often the unintended social consequences stay the same. Finally issues of accountability and trust were discussed. As was shown both the increased ‘responsibilisation’ of people and technology have had significant consequences for issues of accountability. Research is urgently needed which addresses these problems and examines what regulatory measures can be put in place to deal with the issue.

In the second part of our critical assessment we discussed some of the legal challenges that come to the fore with the increased use of surveillance technologies. Legal academics but also national and European courts are busy looking for ways to react to these changes. As was shown when judges from the European Court of Justice and the European Court of Human Rights are confronted with related cases, which so far is rare they put forward values such as transparency, proportionality, non-discrimination and due process. As was pointed out law is only part of the solution in dealing with the challenges of pre-emptive policing and the increased use of surveillance technologies, such as databases and data mining; political will and policy change play a huge part in this too.

Finally it should be noted that as said in the introduction as the UK is on the forefront of technological innovation and the use of surveillance technologies in policing, therefore it has a special responsibility in showing the right example for other countries. However as the Marper case shows the will to do this seems to be lacking as now three years later the police in the UK are still storing DNA from suspects and have not undertaken any initiative to remove DNA from innocents from the database.34

In sum the main conclusions of this article that can be drawn are:

• The policing landscape has become fragmented as a result of ever changing police models and shifting responsibilities to other agents than just the traditional police.

---

The police seem to be driven by the need to keep reinventing themselves by suggesting ‘new’ models, although when looked at more closely these models are not always so new.

It is important to recognise that policing decisions are influenced by many extraneous factors, including political motivations and/or community concerns.

Confirmation of Garland’s theory that both adaptive and non-adaptive strategies co-exist in tandem and there has not been a radical break from the past, however, the article does show when looking at new developments that the distinction should not be considered as dualistic, but more fluid, with some new strategies showing both adaptive and non-adaptive characteristics.

Where one can see a radical shift, is in the increased role of surveillance technologies in policing, and more specifically, the use of databases and (predictive) data mining and profiling techniques.

Although surveillance technologies are often introduced as being a more objective and efficient alternative to old-fashioned methods, we have shown that they raise similar, but also other social and legal issues.

Shifting responsibilities, the increased use of surveillance technologies and new ideas about policing all have social and legal consequences that should be taken into account when implementing new models.

Proportionality, transparency, non-discrimination and due process need to be central in the development of new police models.

The article has tried to show how other disciplines such as surveillance studies, science and technology studies but also legal studies can enrich the debate on talking about the use of surveillance technology by police.

Future research into policing needs to address more seriously the unintended social consequences and legal challenges of the use of surveillance technologies in policing in addition to more detailed studies into the effectiveness of the use of surveillance technologies in policing.

**Bibliography**


