Metadata	
Title	Technologies of Control
Description	
Keywords	
Objectives	
Author	Criminology
Organisation	University of Leicester
Version	V1.0
Date	08 Feb 2010
Copyright	

8.1 Aims and objectives of the Unit

The aim of this unit is to provide an overview of recent technology developments in the field of security, with particular emphasis on how the use of the technologies impacts on the lives of individuals. The objectives are:

- Consider the main research techniques that have been used to evaluate the impact of security technologies.
- Identify the main drivers that have led to the growth of technological fixes to modern security risks.
- Examine how the technologies are impacting or could potentially impact on offending behaviour and their effect on society.
- Review research findings related to the effectiveness of the technologies

8.2 Introduction

> *Contemporary security policies are characterised by a dramatic focus on high technology like biometrics as a security enabler. The process of technoligization of security i.e. the making of technology the centrepiece of security systems and its perception as an absolute security provider started in the US in the Eighties and has since been expanded to the European Union (EU) and to almost all developed countries.*
> *(Ceyham, 2007: 102)*

> *Basically all technology is made for ordering the world and reproducing it. Modernity has applied these ordering techniques to humans, under the general category of discipline.*
> *(Lianos and Douglas, 2000: 263)*

Modern society is characterised by increasing levels of global social mobility and uncertainty relating to levels of risk posed by internal and external security threats. Within this climate security driven by technology is increasingly being used by governments, corporate bodies and individuals to monitor and reduce

risk (Lyon, 2004). There has been an acceptance that the criminal justice system is limited in its capacity to control crime which has led to the exploration of other avenues for tackling crime (Zedner, 2003) and this has provided a market for private companies to push forward the growth of technological security innovations. Security technologies are primarily a type of surveillance tool that takes a number of forms and is used to check identity, prevent and deter crimes, intercept communications and they address the 'demand for knowledge and support, coming from the public and private sectors' (Savona and Mignone, 2004: 23). The technological developments that have infiltrated security and crime prevention strategies have allowed increased surveillance and recording of the movement and behaviour of people 'without the need for constant direct observation or containment of those monitored in particular spaces' (Graham and Wood, 2003).

This unit considers three forms of technologies that have been utilised for the purpose of security namely CCTV, biometrics and RFID (Radio, Frequency, Identification Devices). These technologies have been implemented for the purpose of security across a range of different contexts. CCTV has been widely implemented in the UK as a crime prevention measure in public spaces whilst the major use of biometrics is controlling flows of individuals across borders. RFID has been used extensively to electronically tag and monitor offenders within the criminal justice system (so represents another realm that has been infiltrated by technological solutions). Technologies are used often in conjunction to allow for more effective surveillance and this issue is considered at the end of the unit. A theme running through the unit is how research has investigated the real or potential impact of security technologies and a number of research models are initially outlined in the unit. Academic research has certainly raised concerns regarding how well security technologies work, the levels of discrimination contained with the technologies and the extent that the technologies are infiltrating different aspects of society (Ball and Haggerty, 2005), and these themes form the foundation of the unit.

8.3 Researching the Impact of Security Technologies

Within the field of research that investigates and theorises about the impact of security technologies, a wealth of research methodologies have been applied which reflects the diverse nature of the individual technologies and the huge disparities in where and how they are implemented and operated. The discussion below considers some of the methodologies used to study security technologies but only scratches the surface of this complex field of investigation and is intended to introduce the reader to the main forms of evaluation used within the research field.

The expansion of security technologies across many areas of society has lead to intensification of surveillance practices and this in turn has 'prompted rich empirical and theoretical inquiry' (Ball and Haggerty, 2005: 129). The empirical techniques that have been adopted by academic researchers are varied and there has been a great deal of debate regarding the most suitable methods of identifying whether interventions are effective (Tilley, 1998; Farrington, 2002)

which is covered below. Academics have also tried to examine the potential impact that expanding security technologies, such as biometrics, may have on society by using various theoretical frameworks and some of the main characteristics of this type of research are examined below.

8.3.1 Empirical Research

Empirical research develops findings through the collection of data gathered through observation that is usually used to test research hypotheses. Across a number of security technologies evaluation research has been conducted to examine the effectiveness of programmes by applying scientific procedures to the research design. Evaluation is concerned with ascertaining the 'merit or worth or value' of an intervention and developing 'practical knowledge to aid the decision making process' used to inform the operation of interventions (Clarke and Dawson, 1999: 3). Evaluations will not just try and establish whether an intervention has worked but also looks at what factors account for the success or failure of the intervention, and this information can be fed back into the project to improve its operation and outcomes.

Researchers can be under pressure to find whether interventions are successful. Clarke and Dawson (1999: 16) highlight that any research takes place within a particular social context and there are often stakeholders who have a vested interest in the evaluation findings. In the context of security technologies they are often expensive to implement and stakeholders may want evidence of success to verify the benefits of their financial commitment.

When evaluating any intervention it is important to establish the aims and objectives of the project which are the desired outcomes. Part of an evaluation process will often entail collecting outputs and these are what are produced by the project. The outputs are things that need to be achieved before an intervention can meet its objectives (Home Office, 2002). For example, a CCTV project will need to install cameras and establish monitoring operations as outputs before any crime reductions can be realised. A process evaluation will often be undertaken to ascertain whether a project is working properly which seeks to establish whether a project has been fully implemented and how it operates (Home Office, 2002: 104). The outcomes from a project are the overall results from the project and often relate to reductions in crime or fear of crime levels. The actual form an evaluation takes varies depending on the objectives of the research and a number of models are considered below.

8.3.1.1 Quasi-Experimental Evaluation

The basic structure of a quasi-experimental evaluation involves examining the impact of an intervention by taking measurements before and after it is implemented. An evaluation may examine the impact of an intervention on crime levels or whether an intervention has changed the perception of individuals. The actual process of conducting a quasi-experimental evaluation is often complex as inferring cause and effect is often difficult (Sherman et al, 1997). Evidence should be collected to ascertain whether any change that has occurred is due to

the intervention being researched or other causes, known as confounding variables. Sherman et al (1997) developed a 5-point scale called the Maryland Scientific Method Scale (SMS) to evaluate the methodological quality of studies and the authors indicate that confidence in the results is highest at level 5 and level 3 should be the minimum level required to achieve reasonably accurate results. The criteria for each level of the scale are:

> *Level 1: Correlation between a prevention programme and a measure of crime at one point in time (e.g. areas with CCTV have lower crime rates than areas without CCTV)*
>
> *Level 2: Measures of crime before and after the programme, with no comparable control conditions (e.g. crime decreased after CCTV was installed)*
>
> *Level 3: Measures of crime before and after the programme in experimental and control conditions (e.g. crime decreased after CCTV was installed in an experimental area, but there was no decrease in crime in a comparable area)*
>
> *Level 4: Measures of crime before and after in multiple experimental and control units, controlling for the variables that influence crime (e.g. victimisation of premises under CCTV surveillance decreased compared to victimisation of control premises, after controlling for features of premises that influenced their victimisation)*
>
> *Level 5: Random assignment of program and control conditions to units (e.g. victimisation of premises randomly assigned to have CCTV surveillance decreased compared to victimisation of control premises)*
> *(Farrington, 2002)*

When researching the impact of security technologies it is very difficult to achieve level 5 on the SMS because interventions are often implemented across areas and groups without any scope for random assignment. Research within real world settings has to take account of ethical issues. For example, a researcher cannot dictate whether certain groups experience one technological security sanction (e.g. electronic monitoring) and another group are deprived of the sanction (Finn and Muirhead-Steves, 2002: 309; Bonta et al, 2000a: 324). A range of independent variables have been used to measure the impact of security technologies including recorded crime levels across target areas (e.g. Welsh and Farrington, 2002, 2008), recidivism rates of offenders (Finn and Muirhead-Steves, 2002) and public attitudes (e.g. Gill et Spriggs, 2005d).

One of the main difficulties in conducting real world research is identifying suitable control units. Ideally control and experimental units are identical and then when an intervention is introduced into the experimental unit any difference between the two units can be attributed to the intervention. Problems can occur matching control and experimental conditions especially when

examining the impact of interventions within real world settings such as cities and towns. Over an evaluation period inconsistent changes may occur across the two conditions that mean it is no longer valid to compare the two conditions. Security technologies are rarely implemented as an isolated measure and therefore it is often difficult to unpick their impact from quantitative measures taken from experimental and control areas. For example, levels of detected crimes are often used to evaluate CCTV but a range of activities can impact on crime levels, therefore the impact of the cameras can be difficult to isolate.

An important issue that needs to be factored into any evaluation is displacement. An intervention may simply displace a problem to another area or make the offenders change the type of crime they commit, how they commit crimes and/or the times when they commit crimes (Repetto, 1976). Advocates of situational techniques have acknowledged that it is nearly impossible to find evidence showing that displacement has not occurred and this is an inherent weakness of research on displacement (Barr and Pease, 1990; Clarke, 2004). A fuller understanding of displacement effects can be gained by integrating research methodologies. For example, some forms of geographical displacement can be measured by examining crime trends in buffer zones around intervention areas (Gill and Spriggs, 2005) or by looking in detail at offending patterns within intervention areas. Interviewing offenders can provide evidence related to whether interventions cause them to change their offending behaviour either temporally or how they committed crimes.

The Campbell Collaboration (www.campbellcollaboration.org) advocate conducting systematic evaluations on a range of research studies to 'estimate the average effect size in evaluations' (Welsh and Farrington, 2008: 12). This type of research does not produce new empirical data but draws together the findings from a range of studies and is referred to as a meta-analysis.

8.3.1.2 Realistic Evaluation

Tilley and Pawson (1997) developed a model of theory driven evaluation called 'realistic evaluation' that was centred on finding not only what outcomes were produced from interventions but also 'how they are produced, and what is significant about the varying conditions in the which the interventions take place' (Tilley, 2000). Tilley has been critical of quasi-experimental models of evaluation and suggests they fail to effectively identify why interventions work differently across different contexts. Realistic evaluation seeks to find the contextual conditions that make interventions effective therefore developing lessons about how they produce outcomes to inform policy decisions. Tilley outlined three investigative areas that need to be addressed when evaluating the impact of an intervention within any given context.

Mechanism: what is it about a measure which may lead it to have a particular outcome in a given context?

Context: what conditions are needed for a measure to trigger mechanisms to produce particular outcomes patterns?

> *Outcomes pattern: what are the practical effects produced by causal mechanisms being triggered in a given context?*
> *(Tilley, 1998: 145)*

The model involves developing a 'context mechanism, outcome pattern configurations' (CMOCs) that allow a researcher to understand 'what works for whom in what circumstances' (Tilley, 2000). The generation of CMOCs occurs through consultation with relevant stakeholders responsible for implementing, operating and participating in interventions. The model of evaluation allows the researcher to understand what aspects of an intervention make it effective or ineffective and what contextual factors are needed to replicate the intervention in other areas. Interventions can work in a number of ways within one area and realistic evaluation provides a model to understand the effect being produced by the intervention and crucially for policy development how it can be consistently replicated. Tilley suggested that models need to be developed for replication of interventions and realistic evaluation provides the framework to develop appropriate models:

> *Realism provided the necessary ingredients for such a model: specification of the crucial contextual conditions for the intervention, the change-inducing mechanisms that will be triggered by the intervention, and the anticipated outcomes pattern that will be generated by triggering these mechanisms. This compromises a 'context mechanism outcome pattern configuration*
> *(Tilley, 2000: 104)*

One of the key strengths of realistic evaluation is the ability to take the lessons learnt from one evaluation and apply them across a range of different contexts. Once the CMOCs are developed they need to be tested and they produce very specific data requirements across the context, mechanisms and outcomes and collecting all the relevant data can be very resource intensive (Gill and Turbin, 1999).

8.3.2 Qualitative Evaluation

Evaluation research often focuses on the outcomes of projects as defined by quantitative data that allows the impact of a project to be measured but to really understand the impact of a project and to discover why a project may have an effect qualitative research is also required. Qualitative research attempts to undercover the 'subjective realities' of an intervention by examining how it affects different groups and individuals. Quantitative research looks for 'a single objective reality' but qualitative research acknowledges that individuals may experience an intervention differently and the multiple realities need to be documented (Clarke and Dawson, 1999: 39). The role of the researcher is fundamentally different within the context of qualitative research where they get closer to the data often through data collection that involves interaction with subject whilst quantitative research can involve analysis data whilst being removed from the social world that produced the information.

A number of evaluations have investigated the impact of CCTV on crime levels (e.g. Farrington and Walsh, 2002; Gill and Spriggs, 2005) but to fully understand the actual impact of the cameras on offenders their views must be obtained (Gill and Loveday, 2002). Padgett, Bales and Blomberg (2006) investigated how offenders experienced electronically monitored curfews and the qualitative methodology adopted allowed them to develop a better understanding of whether the sanction was more punitive for one group than another and this has implications for criminal justice policy and theory. Security technologies may impact at different levels across areas and have differential impacts across social groups, and these differences can be understood through qualitative data sources. Useful information about the effectiveness and impact of security technologies can be accessed through talking to the subjects of their surveillance.

8.3.3 Theorising on the Impact of Security Technologies

Theory can play a role in evaluation by helping the researcher decide on their methodology and directing them to certain issues and problems (Clarke and Dawson, 1999). It is important to understand the theoretical basis of an intervention so that during an evaluation the theories can be tested. A theoretical framework helps to unpick the relationship between the intervention and its impact.

Within the field of research in security technologies theory has been used as a framework to examine the real and potential impact of interventions. Many of the technologies have the potential to impact on large sections of society and, rather than waiting to evaluate the impact of these interventions once they have been implemented, academics have sought to theorise about their potential effects. General social theories have been used as a framework to examine the potential effects of security technologies 'either with whole societies and the processes involved in their development, or with very general aspects of social reality such as the relationship between agency and structure or macro and micro level of analysis' (Layder, 1998: 14 quoted in Bottoms, 2000). Academics examining the impact of surveillance technologies, such as CCTV and biometrics, have turned to Foucault's general social theory and used the themes of power and the increase of disciplinary mechanism throughout society as a framework to discuss the influence of the technologies (Koskela, 2003; Yar, 2003). Ball and Haggerty (2005: 134) suggest that:

> *... surveillance based research highlights the power relations inherent in surveillance practices: power relationships that concern an organisation's ability to watch in an unproblematic and unchallenged way.*

Many of the global security technologies used to monitor individuals, are comparatively secret and individuals may not be aware of the impact upon their lives, therefore academic research utilises theoretical material to document some of the potential consequences of the technologies. Research

into the impact of security technologies is transdisciplinary and theoretical models have been utilised from a number of research fields. For example, Ackleson (2005) explored the social, economic and political impact of deploying security technologies across the United States borders and used Birkland's "focussing event" framework to examine the 'postcrisis policy formulation process' that drove the growth of the technologies. Theorising about the actual and potential impact of security technologies has allowed academics to engage in debate about how security technologies impact on issues such as 'equity, fairness, justice, and respect for a person in a digitally mediated world' (Ball and Haggerty, 2005:131) which moves the debate about security technologies beyond whether they are effective or not.

A number of different methods of examining the real and potential impact of security technologies have been outlined above. Academic debate will continue around the various merits of different research methodologies but it is essential that research methodologies meet the specific objectives of research projects. The types of issues being investigated should define the research design adopted and often different models of evaluation have been integrated to provide a full picture of an intervention's impact (e.g. Gill and Spriggs, 2005). Some of the research issues examined above are revisited in the context of the security technologies discussed below.

8.4 Surveillance and CCTV

8.4.1 Growth of CCTV

Across the developed countries of the world today surveillance is part of everyday life and this has led to the acknowledgement that the UK is part of a surveillance society (Ball et al, 2006). The UK has experienced a massive growth in CCTV since the 1980s and this was initially based on the assumption that CCTV was a panacea for crime and disorder (Norris and Armstrong, 1999). The discussion below explores some of the key debates that have emerged regarding the growth of CCTV and then moves onto explore the effectiveness of CCTV as a tool to address crime and disorder, and the impact of CCTV on fear of crime.

The UK leads the world in the use of CCTV (House of Lords, 2009) driven by political support from both Conservative and Labour administrations. CCTV was perceived as an answer to the rising crime rates experienced during the 1980s and was attractive to government because it met its 'ideological demands for privatisation of the public sector' (McCahill and Norris, 2002a: 12). Involving the private sector reduced costs for local councils. New Labour used CCTV to develop an image of being 'tough on crime' and moved away from previous accusations of being soft on crime and anti-police as they had been in the 1970s and 1980s (Reiner 1992 quoted in McCahill and Norris 2002a).

Central Government instigated the growth of CCTV in the UK by making funding available for local areas to bid for CCTV capital grants. Funding initially came from the CCTV challenge competition run between 1994 and 1999 that made

£38.5 million available and this was allocated across 585 schemes nationwide (Home Office, 2007). The Home Office funded Crime Reduction Programme (CRP) ran between 1999 and 2003, and resulted in the investment of £170 million of capital funding into CCTV development (Home Office, 2007). Clearly the Government viewed CCTV as an effective means of protecting the public and during the 1990s 78 percent of the Home Office crime prevention budget was spent on implementing CCTV and a further £500 million of public money was spent on CCTV between 2000 and 2006 (House of Lords, 2009).

McCahill and Norris (2003) estimated that there were approximately 4.3 million cameras in the UK but police investigations suggest that this may be an over-estimation (Home Office, 2007). The explosion of CCTV in the UK was not informed by an evidence-based approach that provided a comprehensive basis to inform where and how CCTV should be implemented. The ad hoc and unregulated nature of CCTV growth has produced a range of public CCTV systems that have different roles and levels of effectiveness (see below). Government funding played a crucial part in the escalation of CCTV in the UK but other key issues galvanised the growth and these are discussed below.

The bidding process that followed the release of funding allocated by government for CCTV (see above) was built around the rise of the multi-agency approach to crime prevention and reflected 'the drive towards new modes of governance in local crime control through the encouragement of local coalitions between police, private security, retailers, property developers, local government and insurance companies' (Colman and Sim, 1998: 28). The Crime and Disorder Act (CDA) (1998) had a major impact on CCTV policy contents and 'galvanised many existing informal arrangements and contained the first official and legal obligation for the creation of multi-agency crime control partnerships' (Fussey, 2004). The CDA and the Crime Reduction Strategy focused the work of partnerships on crime control but also public safety, tackling low level disorder and reduction in fear of crime. CCTV is perhaps a unique crime prevention strategy that manages to fulfil the diverse aims set out by the government (Fussey, 2004). The popularity of CCTV is due in part to its wide ranging uses that extend from a situational crime prevention method to facilitating reductions in fear of crime. Whether CCTV is effective across these different uses are discussed below.

Often partnerships bidding for CCTV funding did not have a clear idea of local crime and disorder problems or how CCTV would work to combat the problems. Many partnerships viewed CCTV as a desirable improvement to any area and were under pressure from communities to implement CCTV (Gill et al, 2003). Areas may have been motivated to implement CCTV due to the proliferation of other local areas gaining CCTV and the anticipation that crime may be displaced from areas under CCTV surveillance to their local area (Williams and Johnson, 2000). Partnerships were drawn towards CCTV funding through the financial backing of central government and often more lucrative regeneration grants 'required the provision of a "safe" environment' and to many local authorities CCTV fitted this purpose (Williams and Johnson, 2000: 189). CCTV has also been implemented as a counter terrorism measure and this has been the primary

objective of some systems such as the 'Ring of Steel' erected in London after the Bishopgate bombing (McCahill and Norris, 2003) but also formed part of the rational behind implementing CCTV across other public spaces (Gill et al, 2005b). Pressure to access grants meant that CCTV was prioritised and a detailed analysis of what might work locally to address crime and disorder issues was not undertaken.

Fussey (2004) examined some of the 'structural' influences of partnerships that can impact on objective and rational policy making. The police often have an elevated position in current partnership arrangements and this is significant in terms of CCTV as they consistently stress the importance of 'situational and enforcement' tactics when tackling crime and disorder. Conflict often arises in partnerships due to conflicting performance indicators or working cultures (Crawford, 1997). Therefore partnerships are drawn to CCTV as a popular strategy with universal appeal but there is little evidence that CCTV was identified through a rational approach that matched local needs to CCTV. Public consultation tends to indicate low-level disorder as problematic and this can 'heighten and legitimise public pressure for CCTV implementation' (Fussey, 2004: 262) as local communities consistently request CCTV. The public support of CCTV also leads elected members to favour it as it acts as a public demonstration that crime is being tackled and communities are being listened to. The widespread support of CCTV across the different groups discussed above is not based on robust evaluation and implementing CCTV is an easy win for practitioners because, even if reductions in crime and anti-social behaviour are not achieved, they are seen to be doing something. CCTV is highly visible unlike other offender centred approaches (e.g. drug rehabilitation centres and prisons) and can present the media with positive stories that are reinforced through the use of recorded images from the CCTV (McCahill, 2003).

The increase in CCTV surveillance across the UK led to academic debate about the impact of surveillance and one of the key themes that has been consistently revisited through the literature has been the Panopticon. This was a model prison designed by Jeremy Bentham which worked on the premise that prisoners could be controlled if they thought they were being potentially watched from a central control tower (McCahill and Norris, 2002). The increase in new surveillance technology has been seen as one of the symptoms of a transition from 'modernity' to 'postmodernity' and the spread of measurements, such as CCTV, is viewed as a sign of the 'dispersal of discipline' into public areas (Norris and McCahill, 2006). CCTV does not represent a mechanism for targeting known individuals who pose a risk to society but facilitates monitoring of 'geographical spaces, time periods and categories of people' (Norris and McCahill, 2006: 103). Norris and McCahill viewed CCTV as an actuarial technique that can be used to prevent future crimes rather than manage past crimes and this is one of the features that sets it apart from previous crime control tools.

8.4.2 CCTV effectiveness and Context

When the Government funded the massive growth in CCTV across the UK there was no body of research to justify and guide the implementation of CCTV (Ditton

and Short, 1999; Farrington and Walsh, 2002). Subsequently the effectiveness of CCTV across a number of contexts has been explored and research has started to establish an evidence base for where and how CCTV can be effective. Many of the studies into CCTV have produced contradictory results due to variations in the circumstances of the introduction of CCTV leading to varying effects (Tilley, 1998).

Research that utilises the scientific realism approach developed by Pawson and Tilley (1997) tried to identify how CCTV works and specifically in what contexts (see Tilley 1993, Gill and Spriggs, 2005). Academics (Armitage et al, 1999; Tilley 1993) have documented several ways or mechanisms that could result in CCTV bringing about change in an area and those devised by Tilley (1993, quoted in Gill and Spriggs, 2005) are as follows:

- Caught in the act - CCTV could reduce crime by increasing the likelihood that present offenders will be caught, stopped, removed, punished and therefore deterred.
- You've been framed - CCTV could reduce crime by deterring potential offenders who will not want to be observed by CCTV operators or have evidence against them captured on camera.
- Nosey Parker - a reduction could take place because more natural surveillance is encouraged as more people use the area covered by CCTV. This may deter offenders who fear an increased risk of apprehension.
- Effective deployment - CCTV may facilitate the effective deployment of security staff and police officers to locations where suspicious behaviour is occurring. Their presence may deter offenders, or may mean they are caught in the act.
- Publicity (general) - this may assist in deterring offenders.
- Publicity (specific) - CCTV cameras and signs show people are taking crime seriously, and thus offenders may be deterred.
- Time for Crime - CCTV may have less of an impact on crimes that can be done quickly as opposed to those that take a longer time, as offenders assume that they will have enough time to avoid the cameras, or to escape from police officers and security staff.
- Memory jogging - publicity about CCTV encourages potential victims to be more security conscious and to take precautionary measures.
- Appeal to the cautious - those who are more security minded use the areas with CCTV, driving out the more careless who are vulnerable to crime elsewhere.

The list above represents a starting point to consider how CCTV can impact on crime and numerous other mechanisms can be developed across a range of settings and offence types (Ratcliffe, 2006). Coupe and Kaur (2005) examined the impact of CCTV and alarms in detecting commercial burglary and they highlighted the complex interplay of mechanisms that can result in CCTV impacting on crime and how different crime prevention measures can have conflicting mechanism.

> *CCTV can provide evidence on film that leads to arrest, while visible CCTV cameras like alarms, may also deter burglars or displace them to other targets. In addition, visible or hidden CCTV cameras may alert a watchman or employee to the commission of a crime. On the other hand, activated alarms may frighten burglars so that they quickly flee the scene, reducing not only capture there, but also, where CCTV is additionally fitted inside the premises, of a subsequent arrest by catching the offender on film.*
> *(Coupe and Kaur 2005: 53)*

Sivarajasingam, Shepherd and Matthews (2003) examined the impact of CCTV in town/city centres and detailed how theoretically the cameras may impact on levels of violent crime:

> *Perpetrators may be detected and removed; CCTV may deter potential offenders who perceive an increased risk of detection; CCTV may direct security personnel to locations where precursors to offending have been detected, which may head off their translation into crime and reduce the severity of harm; CCTV could symbolise efforts to take crime seriously, and the perception of those efforts may both energise law abiding citizens and/or deter crime. The presence of CCTV may induce people to take elementary precautions, for fear that they will be shamed by being shown on CCTV.*
> *(Sivarajasingam et al, 2003: 315)*

The mechanisms outlined above highlight the potential problems of using recorded crimes rates to evaluate the impact of CCTV as the different mechanisms can have conflicting effects on crime rates (Ditton and Short, 1999: 212; Ratcliffe, 2006, Gill et al, 2007: 24). Although CCTV will not increase actual levels of crime the increased surveillance may result in more offences coming to the attention of the police, particularly violent offending (Brown, 1995). Using disaggregated crime data that identifies changes across individual offence types can help to understand the impact of CCTV across a target area. The range of additional crime reduction measures that often operate alongside CCTV system make if difficult to isolate the impact of the cameras and these can include changes to policing practices (Webb and Laycock, 1992), ad hoc police operations, improved lighting, community wardens and youth inclusion projects (Gill et al, 2007). Using crime statistics alone to evaluate CCTV means that many of the potential benefits of the cameras can be missed including supporting police activity leading to cost savings in relation to police time, increased detection rates, court time and the increased level of guilty pleas and guilty verdicts obtained when CCTV evidence in available (Home Office, 2007).

CCTV can work on a number of different levels across a range of different contexts and this has resulted in mixed research findings in terms of CCTV effectiveness. Welsh and Farrington (2002) conducted a meta-analysis on studies of CCTV effectiveness and collected 46 studies but only considered 22 of the

research papers to be rigorous enough for inclusion in their review. Half (eleven) of the studies found a desirable effect on crime, five found an undesirable effect on crime, five found a null effect, and one was classified as an uncertain effect. The largest impact on CCTV was found across car parks where there was evidence that crime reduced by 41% in the experimental compared to control area, which was significant. The research identified that CCTV had little or no effect on violent crime but the authors advocated the need for more high quality research that 'established the causal mechanism by which CCTV has any effect on crime' which should involve methodologically rigorous evaluations and interviewing offenders. A further meta-analysis of CCTV studies conducted in 2008 by Walsh and Farrington the confirmed earlier findings that CCTV was effective in car parks and they advocated narrowing the use of CCTV to reflect research findings related to its effectiveness.

The Home Office's National Evaluation of CCTV (Gill and Spriggs, 2005) attempted to address some of the deficiencies identified in previous CCTV evaluations by combining a process and impact evaluation that incorporated control areas and identified other crime control initiatives that were operating in the target area to evaluate their impact on recorded crime levels. Thirteen CCTV systems were evaluated across a range of system including town centres, city centres, car parks, hospital and residential areas. The inclusion of residential areas reflected the governments push to include these types of areas into the Phase 2 of the Crime Reduction Programme (Home Office, 2007). The main findings were:

> *Out of the 13 systems evaluated six showed a relatively substantial reduction in crime in the target area compared with the control area, but only two showed a statistically significant reduction relative to the control area, and in one of these cases the change could be explained by the presence of confounding variables. Crime increased in seven areas but this could not be attributed to CCTV. The findings in these seven areas were inconclusive as a range of variables accounted for the changes in crime levels, including fluctuations in crime caused by seasonal, divisional and national trends and additional initiatives.*
> *(Gill and Spriggs, 2005i)*

The quotation above highlights the difficulties in obtaining a true picture of the impact of CCTV schemes given the complex environments where they often operate. The research concluded that for CCTV to be effective it needs to be implemented with a clear strategy that takes into account local crime problems and identifies the mechanism by which the system will address the problems. CCTV should not be implemented as a stand alone crime prevention tool but needs to be integrated into prevention measures already in place and operate alongside local police structures to create rapid responses to incidents and effective use of images for evidential purposes.

Research has found mixed results regarding the effectiveness of CCTV but what has emerged is a body of literature that has started to identify the specific

context where CCTV works and types of mechanisms that need to be in place. Brown (1995) found that in certain circumstances CCTV can make a positive contribution to addressing crime and this was reliant on CCTV being used by the police as an integral part of a command and control strategy. The research highlighted the deterrent effects of CCTV but suggested that CCTV must also be used to effectively manage police resources through rapid responses to incidents. Brown found that the use of CCTV in Newcastle and King's Lynn resulted in a reduction in recorded crime particularly across burglary, criminal damage and vehicle crime offences. The research found CCTV had no overall impact in Birmingham on crime levels (Brown, 1995: 46). Research indicated that the layout of the streets has an impact on the ability of CCTV to detect crime and areas with less side streets and more long straight roads more conducive to CCTV (see also Gill et al 2005b).

Ditton and Short (1999) found that recorded crime fell and detections rose after CCTV was implemented in Airdrie but in Glasgow recorded crime increased and detection increased. The research found a differential effect of the cameras across crime type with drug offences, low-level public order and minor traffic violations increasing whilst various forms of acquisitive crime fell. Airdrie is a little town where awareness and a sense of ownership of the cameras were high compared to Glasgow where the cameras merged into the structure of the city, and these situational differences may have impacted on the effect of the cameras.

Most evaluations of CCTV in town/city centres have used recorded crime and found that cameras had very little impact on violent crime (Gill and Spriggs, 2005) but through the use of accident and emergency data Sivarajasingam et al (2003) found that the 'effectiveness of CCTV lies less in preventing assaults and their precursor, but more in preventing injury through increased police detection and intervention' (ibid: 315). CCTV was found to increase police detection but was associated with reductions in the seriousness of violent incidents. There was no evidence of the deterrent effect of CCTV in relation to violent crime but the effectiveness of CCTV within this context is related to surveillance facilitating a faster police response that limits the length of violent incidents and therefore the severity of injuries.

The body of CCTV research literature emphasises that it is more effective in relatively simple target areas with clear lines of sight. CCTV has been shown to reduce crime in car parks (Tilley, 1993; Gill and Spriggs, 2005) and this may be partly explained by the cameras monitoring an environment where access and egress can be carefully monitored. CCTV in car parks has reduced crime by acting primarily as a deterrent and this mechanism has been facilitated by clear CCTV signage and the visibility of the cameras (Gill and Spriggs, 2005). The impact on 'theft of' and 'theft from' motor vehicles was different with a larger positive impact across 'theft of' offences which may be due to these types of offences taking longer and offenders having to drive out of exits monitored by cameras (Tilley, 1993).

CCTV systems rarely work in isolation and often form part of a crime prevention strategy. Webb and Laycock (1992) found evidence that CCTV can reduce

robberies on the London Underground but the cameras were part of a package of measures to reduce crime in the area that made it difficult to identify the impact of the cameras alone. The research concluded that 'CCTV does not seem to be very useful in large complex and crowded environments to deal with surreptitious behaviour such as pick pocketing or shoplifting' (Webb and Laycock, 1992: 23) as the quick nature of the offences made it unlikely that they would be picked up by operators. Given that it was unlikely offenders would be detected by the cameras their effectiveness was mainly linked to whether offenders associated the cameras with an increased risk of getting caught on the London Underground.

CCTV is a type of situational crime prevention and is often used to facilitate a change in the behaviour of offenders. Mayhew (1984) suggested that formal surveillance would deter potential offenders and this follows the rational choice theory perspective (Clarke and Felson, 1993) that proposes offenders act in a rational manner and by calculating whether the perceived benefits outweigh the cost in a given situation. The application of the deterrent effect of CCTV to routine activity theory means that the presence of CCTV can be perceived to act as the capable guardian and therefore demotivate offenders. The majority of CCTV systems rely on the deterrent effect of the cameras but the deterrent is often symbolic and 'more or less incompetent deterrence because cameras are highly visible but those under surveillance are hardly visible for an observer due to irregular monitoring, informational overkill or even deployment of dummy cameras' (Hempel and Topfer, 2004: 33).

Research has examined the effect of CCTV on offenders' behaviour across a range of contexts and identified that CCTV tends to be an effective deterrent against planned offences. Allard, Wortley and Steward (2008) examined whether the presence of CCTV in prisons reduced the number of incidents that were defined as 'breaches of law or rules that may result in criminal prosecution or breach hearings and emergencies'. The research found that CCTV had a greater impact on non-violent than violent prisoner misbehaviour and affected planned behaviour to a greater extent than unplanned behaviour. The spontaneous nature of violence means that the deterrent effect of CCTV can be removed and it tends to be more 'effective when behaviour is motivated' (Allard et al, 2008: 416).

Research into public space CCTV has identified similar patterns and indicated that CCTV impacts more on premeditated crimes (Brown, 1995; Welsh and Farrington, 2002; Gill et al, 2005). Analysing the impact of CCTV on public behaviour, Mazerolle (2002) found that the cameras created an initial deterrence in the two-month period after installation but to prolong the effect recommended increasing the deterrence of using signs and short sporadic cameras deployment. Tilley (1993: 24) suggested that 'when the real potential of CCTV to lead to apprehension loses credibility amongst criminals, the effect will begin to fade, though by (over)-statement of successes periodic effectiveness can be re-established'. The positive impact of CCTV on levels of robbery in the London Underground was found to fade over time and this may have been due to offenders discovering that the CCTV did not increase the risk of being caught

(Webb and Laycock, 1992: 15). High camera density and quality lighting may increase the perceived risk for offenders (Gill et al, 2007). Research indicates that only by combining the different mechanism by which CCTV works (Armitage, et al, 1999, Tilley 1993, Gill and Spriggs, 2005) and integrating other crime prevention measures can the optimal use of CCTV occur and research is currently building the evidence base to fully understand where and how the mechanisms work.

CCTV does not create a physical barrier to crime and therefore can rely to a large extent on changing offenders' behaviour. Therefore key to the success of CCTV is offenders' views regarding its effectiveness. Evaluations that use crime levels to investigate the impact of CCTV on offenders need to be supplemented with offender interview based research to develop a full picture of how CCTV can be utilised fully to address criminal behaviour (Farrington and Walsh, 2002; Gill and Loveday, 2003). Gill and Loveday interviewed 77 convicted offenders in prison and the general consensus amongst those interviewed was that they did not worry about CCTV but there was evidence that some offenders chose to take precautions against the cameras by wearing clothes that hid their identity or offended in camera blind spots. Many of the offenders committed 'swift offences' and therefore believed that police notified by the cameras would not arrive in time to apprehend them (see also Short and Ditton, 1998). Roughly half the sample of offenders believed that CCTV increased the risk of getting caught but those that had been caught by CCTV perceived it as more of a threat. There was a lack of understanding amongst the offenders regarding image quality and how the images could be used to increase detection. The types of mechanisms that need to be utilised to increase the perceived risk of CCTV for offenders include using publicity detailing successes of the cameras and the capabilities of systems.

8.4.3 How CCTV operates

CCTV systems are not homogenous and, due to differences across management structures, operation procedures and the technological capabilities of the systems, they have levels of effectiveness in relation to combating crime (Gill and Spriggs, 2005). There is not scope within this unit for a full examination of the operational factors that impact on CCTV effectiveness therefore the following four themes developed by Machill and Norris (2002c: 44-46) will be used to draw out some of the factors that influence the impact of CCTV.

Diversity: One cannot make any generalisations about the extent, nature and impact of CCTV surveillance from the mere existence of a system. CCTV systems have diverse operating procedures, staffing policies and levels of technological sophistication.

The surveillance web: There is an increasing tendency for systems to become embedded in a complex social and technological web of surveillance which extends and diffuses the impact of the gaze of the surveillance to a range of other controls.

The human mediation of technology: The operation and impact of systems have to be understood as the outcome of the interplay between technological, organisational and cultural factors.

Exclusion: The growth of CCTV in semi-private spaces brings with it an increasing emphasis on exclusion as the dominant strategy of social control.

The four themes above will be used below as a framework to explore how CCTV systems differ and how their presence is experienced by individuals across their zones of surveillance.

8.4.3.1 Diversity

CCTV systems can vary in a number of ways from the technological specifications of the system to the human element in the system that directs the surveillance. This led authors from the Urbaneye Project to conclude that CCTV's 'operation and impact have to be understood as the outcome of the interplay between technological, organisational and cultural factors' (Hempel and Topfer, 2004: 1). The previous statement highlights the need to conduct a process evaluation as part of any CCTV evaluation to help identify the exact mechanisms that make systems effective or hinder their operation.

On a basic level the type of surveillance that occurs across systems can be divided into passive systems – where images are simple recorded and can be assessed to provide evidence retrospectively; and active systems – where a person monitors a series of displays and often has the ability to manipulate the cameras (McCahill and Norris, 2002b; Ratcliffe, 2006). Images are usually recorded 24 hours a day but some systems do not provide live monitoring services 24 hours a day (Gill and Spriggs, 2005; Wilson, 2005) and the nature of CCTV monitoring means that it is not possible for operators to continuously watch the screens (Armstrong and Norris, 1999).

Obviously the position of cameras is central to the success of schemes and there are often problems with cameras being obstructed (Brown, 2002; Smith, 2004; Gill and Spriggs, 2005; Conche and Tight, 2006), blind spots within the cameras target areas (Gill et al, 2005b), adverse weather conditions impacting on image quality (Mazerolle et al, 2002) and poor light levels (Smith, 2004). Cameras are positioned to address crime hotspots but the problems may subsequently move, reducing the effectiveness of cameras (Home Office 2007). Crime patterns across areas are not stable and can change as a result of a myriad of factors including changes to policing, types of offenders, seasonal variations and changes in the make up of areas. To be effective as a crime reduction tool CCTV should be adaptable and ultimately re-deployable to emerging crime hot-spots (McCahill and Norris, 2002: 52). The picture quality of images varies and the evidence from the Home Office suggests that 80 per cent of images supplied to the police may not be of a suitable standard therefore reducing their effectiveness as an identification tool for suspects or as an evidential tool in court (Home Office, 2007: 12).

There are dramatic differences across control rooms related to the management of systems and cultures across operators. CCTV managers can come from a range of backgrounds and their CCTV responsibilities can form only part of their role (Gill and Spriggs, 2005). The lack of effective management in control rooms has lead operators to develop their own styles of monitoring and work patterns (McCahill and Norris 2002c: 36; Lomwell, Saetnam and Wiecek, 2003). There is inadequate training of CCTV operators (Gill et al 2005; McCahill and Norris 2002c) and although the Security Industry Authority (SIA) licensing regime has been implemented from 2006 there is no obligation for operators to get the license which leads to a range of abilities across CCTV staff (Home Office, 2007). Training can be in-house and result in bad habits being passed from one operator to another and compounding the ineffective monitoring practices present in a control room (Smith, 2004; Gill et al, 2005a).

The types of groups that are categorised as problematic by operators depends on the target area under surveillance and may be influenced by national prejudices. Operators in a Berlin Shopping Mall identified suspicious groups as:

> *…school children/teenagers, men, alcoholics, homeless and mostly foreigners, especially southern Europeans such as Turks or eastern Europeans such as Romany (Gypsies), Poles and Romanians*
> *(Helton and Fischer, 2004: 340)*

There has been extensive research conducted related to target selection for CCTV operators and variations across systems were found with between 71 per cent and 93 per cent of targets being male (Norris and Armstrong, 1999; McCahill, 2002; McCahill and Norris 2002c). Race has been shown to be a factor in the selection of targets by operators with some operators targeting black males (Norris and Armstrong, 1999; Williams and Johnson, 2000; Smith, 2004). Operators have been shown to target certain dress codes that to them represent 'subcultures associated with crime and deviance' (Smith, 2004: 386). The make up of the population using surveillance areas has an impact on who is targeted but even when research has controlled for the demographic profile of who is using an area, it was found that that young scruffy males were most likely to be monitored (Williams, 2007).

The use of categorical suspicion based on a narrow range of observable traits rather than behavioural suspicions has been encouraged by the 'sensory limitations of the video screens and the distance between the observers and the observed' (Hempel and Topfer, 2004). The operators have no personal contact with the target they observe and are reduced to interpreting bodily movement from a two dimension image therefore the routine of surveillance 'makes the exercise of power almost instinctive: people are controlled, categorised, disciplined and normalised without any particular reason' (Koskela, 2002). The cameras are not effective at picking up many types of deviant behaviour that are not visually recognisable, including cases of harassment (Koskela, 2002: 255), and the inability of the cameras to offer operators a full sensory experience of

incidents may incline operators to follow their preconceived notions about suitable targets for surveillance.

Research has explored how the potential discriminatory use of CCTV can be tackled. Wilson (2005) examined CCTV systems across four sites in Australia and proposed that 'more systematic and uniform training of camera operators, incorporating instruction in the ethical conduct of surveillance might reduce the discriminatory potential of CCTV in public places'. Surette (2005:158) considered the use of computer enhanced self-monitoring CCTV systems that can be used to detect 'unusual behaviour, unauthorised traffic or surprising and unexpected behaviour and alert a human operator'. The computer aided systems can reduce some of the negative human factors that reduce the effectiveness of CCTV surveillance including data swamping, boredom, voyeurism and selectively targeting people based on which social group they belong to. The behavioural analysis capabilities of the computer enhanced systems rely on systems recognising target behaviours of interest. Troscianko, Holmes, Stillman, Mirmehdi, Wright and Wilson (2004) found that observers were able to make accurate judgements about whether antisocial and violent incidents were about to be carried out by individual or groups. Certain behaviours acted as cues that allowed prediction of deviant acts and this lends strength to the argument that it may be possible to design computer systems that can recognise potentially antisocial or criminal behaviour. The study points to the potential of CCTV to be an effective means of identifying inappropriate behaviour but relies on operators focusing on behavioural patterns within surveillance areas and not selecting targets based on the appearance of individuals.

8.4.3.2 The Human Mediation of Technology

CCTV systems can be used to monitor target areas but if systems are to increase detection of crime they rely on those responsible for authoritative intervention within their zones of surveillance. Public space CCTV systems often depend on the working relationships formed across crime and disorder partnerships and the link between the control room and police is critical (Home Office, 2007). The ownership and management of CCTV system varies across systems (Wilson, 2007) which can have a massive impact on the effectiveness of cameras and 'there exist some real shortcomings in the effectiveness of working relationships between CCTV stakeholders' (Home Office, 2007: 43).

The full engagement of the police can be crucial to the success of a CCTV system but responding to intelligence supplied through CCTV systems can put a strain on police resources that may already be overstretched which can produce limited police involvement (Honess and Charman, 1992; Gill et al, 2006). Areas with high CCTV coverage provide the police with the potential to gather evidence but there are issues concerning their capacity to collect and review all relevant evidence (Home Office, 2007). When CCTV control rooms are operated or located within police stations this increases the interaction between CCTV operators and officers leading to greater intelligence sharing (Brown, 1995; Lomell, et al 2006; McCahill and Norris 2002c). Many CCTV systems are managed by local

authorities and can cover extensive areas across a range of different contexts and are 'often loosely integrated with deployment forces' (Hempel and Topfer, 2004: 38). Police forces are inundated with requests that require police resources, particularly at peak times such as Friday and Saturday nights in City Centres, and requests from CCTV operators are often not prioritised above other incidents leading to weak working relationships between CCTV control room operators and police (Gill et al, 2005a).

Wilson (2005:48) documented a number of issues linked to police operating CCTV systems and indicated that monitoring cameras was not an appropriate duty for police personnel and they can be more effectively deployed on 'core policing duties'. Police use of the cameras may result in 'function creep' as officers take advantage of the system to intelligence gather or officers may view monitoring as a low priority leading to the systems becoming reactive as opposed to a proactive detection tool. An officer working in conjunction with operators at peak times to elicit rapid responses to incidents has been shown to be an effective working model (Wilson, 2005 Gill and Spriggs, 2005). The police need to be fully engaged prior to the commissioning of a CCTV scheme and during the implementation phase to ensure they engage in the day to day operation practices of a CCTV system and it is important that local authorities or other bodies running control rooms establish the roles of the control room staff and police.

8.4.3.3 The Surveillance Web

CCTV systems are used for a diverse range of operations and this can distract operators from surveillance of areas for the purpose of combating crime. Operators can be responsible for a range of responsibilities beyond monitoring the cameras and these may be prioritised above monitoring the cameras, so much so that in one study examining surveillance practices watching the cameras was equated with laziness (Helton and Fischer, 2004). Systems that employ fixed cameras require passive monitoring and are usually set up to collect retrospective evidence for incidents, therefore operators will normally carry out more administrative tasks (Gill and Spriggs, 2005; Wilson, 2005). Additional uses of cameras beyond addressing crime and disorder can include 'street cleaning' and 'traffic management' (McCahill and Norris, 2002). Research by Mackay across CCTV systems in Scotland found that CCTV was being utilised to perform a range of community safety tasks and the expanding uses of the systems have partly been driven by the finding that 'crime reduction is no longer regarded as an outcome that can be accomplished by public space CCTV systems'. The research found that CCTV is being used as an information system and the benefits for the police as 'a management tool' and 'a source of archive evidence' (2006: 131).

CCTV has not been found to result in massive reductions in levels of crime or proved a catalyst for regeneration, therefore systems are moving towards community safety concerns linked to addressing low level disorder and improving quality of life for residents. Cameras have been used to facilitate crime and disorder partnership work to address vandalism and anti-social behaviour.

In some areas CCTV systems have evolved beyond assisting the police and this trend has been encouraged by the CDA which 'positively encouraged diversification of services' (Mackay, 2006: 133). An additional factor that has lead to systems expanding beyond crime reduction has been the financial cost of maintaining CCTV systems. The Home Office provided capital funding to implement a range of CCTV but revenue funding was not made available and this has put a strain on the ability of some local authorities to maintain and expand systems (CCTV Today, 2001 quoted in McCahill and Norris, 2002).

8.4.4.4 Exclusion

The city centre partnership arrangements that underpinned the expansion of CCTV into many city centres included private business stakeholders and this, along with the regeneration agendas that were often being pursed across the areas, contributed to the ways that surveillance has been utilised across urban space. Coleman and Sims (1998, 2000) examined the operation of CCTV in Liverpool city centre to explore a number of political and sociological questions and their analysis highlights how CCTV within a partnership approach is 'reshaping the material and discursive forms of the city' (Coleman and Sim, 2000: 1). The regeneration of Liverpool in the 1990s occurred with increasing emphasis being given to neo-liberal politics brought together public and private agencies through flexible institutional arrangements (Coleman and Sims, 2000: 625). The elite partnerships in Liverpool developed a 'local ordering strategy' which resulted in a conception of power that was driven by the interest of consumerism.

Williams and Johnson (2000: 183) referred to 'the politics of the selective gaze' and they saw CCTV as helping to 'create and enforce socio-spatial divisions within and between towns and amongst those that use the open streets of the surveilled places'. CCTV cameras can facilitate the exclusion of certain groups from public spaces that lead to it being used as a 'tool designed to ensure continued economic vitality of urban spaces' (Williams and Johnson, 2000: 194). The research has suggested some surveillance systems being used for 'policing profit' not safety (Smith, 1998) and the pressures of managing the 'entrepreneurial city' means classifying people according to their economic purchasing power leading to the possibility of surveillance being used as a 'tool of social exclusion' (Hempel and Topfer, 2004: 39). Individuals have to conform to certain behaviour norms to participate in the life of a city centre being driven by leisure and consumption needs and this goes against the notions of a city centre being areas that bring together different social groups and symbolise diversity. The removal of the 'social richness of public places' sanitises the public realm and could lead people to become less tolerant and accepting of different social groups (Reeve, 1998).

8.4.4 Perception of CCTV

CCTV systems are often implemented to reassure the public (Webb and Laycock, 1992; Machill and Norris, 2002c; Gill and Spriggs, 2005, 2007; Ratcliffe, 2006). Research into public support for CCTV has produced mixed results with many

studies finding widespread support for CCTV (Bennett and Gelsthorpe, 1996; Honess and Charman, 1992; Gill and Spriggs, 2005; Hempel and Topfer, 2004) but others highlighted that levels of support may be overstated (Ditton and Short, 1999; Ditton, 2000). The impact of CCTV cameras on fear of crime is context specific and is influenced by the socio-demographic make-up of the respondents with males and young people more concerned about the growth in CCTV (Charman and Honess, 1992; Ditton, 2000: 700). The presence of cameras does not necessarily reduce fear of crime. The cameras are designed to increase offender's perceptions of risk but their presence can act as a warning sign to citizens about the dangers of crime.

If CCTV cameras are to reduce fear of crime then the public must be aware of the cameras' presence. Ditton (2000) found that 33 per cent of individuals in Glasgow city centre were aware of the presence of cameras and this increased to only 41 per cent 15 months after installation. Gill and Spriggs (2005) found that across eleven CCTV target areas the percentage of respondents that were aware of the cameras varied between 61 per cent and 97 per cent. Small residential schemes were found to result in high levels of awareness and city centres had the lowest awareness where the cameras may not be noticeable amongst the dense street furniture. The research found that respondents who were aware of the cameras expressed higher levels of worry about crime than those who were not. The presence of the cameras may be interpreted as a sign that the areas are problematic or people who are aware of the cameras may be more security conscious.

Public attitude surveys conducted into CCTV have produced contradictory findings and shown that the support for CCTV is not based on a belief that CCTV is an effective crime-fighting tool. Results from the Urbaneye research project showed that a London based survey revealed that 40.6 per cent of respondents agreed that CCTV displaced crime and under half the respondents (46.6 per cent) believed it protects against serious crime (McCahill and Norris, 2002c). Other public worries regarding CCTV were linked to operators possible abusing the system, the system being used in a covert way, a general unease at being watched, CCTV evidence could be misleading and an erosion of civil liberties (Charman and Honess, 1992).

The installation of CCTV does not appear to have a significant impact on the behaviour of the public with between 2 per cent and 7 per cent of individuals visiting places they previously avoided before CCTV was implemented (Gill and Spriggs, 2005) but, given many systems are poor at detecting incidents and producing a rapid response, the inability of the cameras to change how the public use areas may be viewed as a positive.

In residential areas support for and confidence in the cameras' effectiveness reduced once the cameras were implemented leading to the conclusion 'that CCTV was far more appealing in theory than it proved in practice' (Gill et al, 2007: 322). As the public become more familiar with the cameras and are increasingly aware that the methods by which CCTV can lower crime are often limited their high expectations of the cameras' abilities may be challenged.

Research has highlighted conflicting ways that CCTV can influence fear of crime by acting as a sign that people live in or have accessed a high crime area but they may also be reassured that something is being done about the crime problems. Koskela (2002: 259) stated that 'to be under surveillance is an ambivalent event' and this results from the paradox that 'cameras can make people feel both more secure and more fearful.

The media has played a major part in the widespread public acceptance of CCTV. Events such as the abduction of Jamie Bulgar thrust CCTV images into the public spotlight and the 'panoptic impulse was strikingly apparent: more surveillance, tighter security' (Hier, 2003: 404). The images of the young boy being lead away 'crystallise fears about public safety' creating public support for the explosion of CCTV during the 1990s (Machill and Norris, 2002a). There have been other high profile cases where CCTV images have assisted in the identification of perpetrators including the Brixton nail bomber in 1999, individuals involved in the terrorist incidents in London during 2005 (Home Office, 2007: 7) and the Soham murder cases.

Managers implementing CCTV have often kept the local media involved in the process and fed positive material to the media regarding the development of systems (Honess and Charman, 1992). Machill and Norris (2002) found that 47% of CCTV related media coverage was positive and media support was found for cameras being used to tackle offending behaviour but negative coverage included cameras being used against the general public in the form of speed cameras or being used to monitor employees. Given the important role that the media play in forming public opinions their support for CCTV in the context of crime fighting helps explain the positive public perception of cameras and the public acceptance of cameras as part of everyday life. CCTV schemes have identified using images of individuals apprehended through the use of cameras as a method of raising the profile of cameras and reassuring the public but identifying suitable cases can be difficult (Gill et al, 2005a)

Through the introduction of neighbourhood policing across the UK, and following recommendations proposed by the Casey Review (Cabinet Office, 2008), the Government tried to make the work of the police and the criminal justice system increasingly visible to communities with the aim of increasing peoples' confidence in these agencies. The nature of CCTV means that the public are not able to fully understand how it operates (Klauser, 2007) which has important implications for how it is perceived and the effect it has on the public. Klauser suggests that the spatial separation of CCTV operations to hidden control rooms 'distanciates' the regulation of public space and therefore removes the whole process from any form of participatory 'community led strategies'.

> *…CCTV both spatially and mentally disconnects the watched (monitored individual) from the watchers (operators). CCTV essentially deals with territorial separation, resulting in two distinct categories of space and in two distinct categories of people: while, on the one hand, the world spread below the camera embraces fully exposed publicity accessible places, the world behind the*

cameras consists of access-restricted places, destined for the visualisation, manipulation, interpretation and recording of decontextualised CCTV images.
(Klauser, 2007: 338)

Klauser found during a long term study of the impact of CCTV across an area where street prostitution operated that CCTV became a 'taken for granted feature' resulting in the cameras being mostly ignored by both potential criminals and the public users of the target area. The study questioned the long-term effectiveness of cameras to reassure the public and highlighted that CCTV needs to be implemented with additional measures including publicity to produce a positive prolonged impact. The study showed that CCTV surveillance was viewed as disconnected from the monitored areas and the 'spatial distance' would make it unlikely that 'real time police interventions' could be created from the control room and this belief was confirmed by a lack of any publicity of the cameras' success (2007: 343)

Koskela (2000) examined whether CCTV can be perceived as making space safer and 'more available'. In the analysis space is conceptualised as a container where social interaction occurs, and there are processes in place that shape and create the experience of the space including surveillance. A person viewing a camera has no knowledge of whether anyone is actually viewing the camera, or who or where the viewer may be. Cameras are passive and therefore have no ability to stop a crime, only perhaps solve it. The cameras add to the unpredictability of urban space as people are not aware of what the cameras actually do and the watched are left with the threat of being watched. Feelings of safety are not necessarily induced by the presence of cameras as people are always 'an object' to the cameras not able to control or influence their destiny. The anonymity of the cameras can lead to mistrust and produces uncertainty that may produce feeling of being unsafe rather than acting as a public reassurance measure. The findings above suggest that any good news stories from CCTV systems need to be publicised and the public's confidence in CCTV systems should not be taken for granted. The research reviewed above indicates that people's expectations of CCTV are often not met and this may link to the ineffective operational practices of systems that result in the symbolic (preventive) power of cameras being lost over time (Klauser, 2007).

Academic literature on CCTV has challenged the view that CCTV is a panacea for crime reduction and systems are often poorly implemented and operated. Research is still trying to identify the optimal conditions that make CCTV effective. Systems were often implemented without a clear idea of the actual mechanisms that would facilitate the cameras reducing crime. The Home Office (2007) in its 'National CCTV Strategy' document stated that the rapid expansion of CCTV has occurred 'in a piecemeal fashion with little strategic direction control or regulation'. There needs to be a fuller debate about whether CCTV is the most effective means of dealing with crime and disorder in public places.

8.5 Biometrics

8.5.1 Defining Biometrics

Biometrics is a technique for identification of people that uses body characteristics or behavioural traits and is increasingly being used instead of or in conjunction with other forms of identification based on something you have (e.g. ID card) or something you know (e.g. password or PIN) (Liu and Silverman, 2001). The basic processes in a biometric system involve biometric data being collected from the data subject via a sensor module, a feature module extracts the biometric data and compared it to templates in a database to identify the data subject (Jain, 2004). The templates are encrypted using algorithmic transformation of biometric samples meaning that the original biometric data cannot be obtained from the biometric databases. The systems that operate in a biometric identification process are beyond the understanding of most individuals processed and they occur in places removed from the individual being processed. This lack of understanding means it is not possible to question the identification practices.

There are a variety of biometric characteristics that can be collected from humans including iris recognition, hand geometry, fingerprint recognition, facial recognition, and voice recognition (Rosenzweig, Kochems and Schwartz, 2004). Biometrics technology is continuously developing to improve accuracy, robustness and security which has seen the emergence of second generation biometrics that utilise multi forms of biometrics together, behavioural biometrics and soft biometrics (e.g. gender, age, ethnicity) (Emilio and Massari, 2008). Any biological or behavioural characteristics could be used to identify individuals if it meets the following requirements:

> 1. *Collectability (the elements can be measured)*
> *2. Universality (the element exists in all person)*
> *3. Unicity (the element must be distinctive to each person)*
> *4. Permanence (the property of the element remains constant over time).*
> *(Emilio and Massari, 2008: 489)*

Biometric systems operate in two basic modes: verification and identification (Jain, 2008). Verification mode is used to validate a person against whom they claim to be and use one to one matches by comparing biometric data taken from an individual to a biometric template stored in a database. Verification relies on individuals enrolling on the system and registering their identity prior to providing biometric samples which is a massive administrative task when applied to international border control. Identification mode uses a one to many match and searches all the templates in a database to identify an individual therefore the system does not need the compliance of the data subject. The accuracy of biometric technology depends on the accuracy and number of records within the databases (Rosenzweig et al, 2004).

Biometric systems are not perfect and systems compare data collected from the data subject to algorithms to determine identification and, where matches are sufficiently close, they will indicate a match. Biometrics systems rely on

matching data to algorithms but they 'make two types of errors: 1) mistaking the biometric measurement from two different persons to be from the same person (called false match) and 2) mistaking two biometric measurements from two different persons to be from the same person (CALLED)' (Jain, 2004: 6). Biometrics systems view the natural patterns of the body as a 'source of order' and 'a source of unprecedented accuracy and precision' (Aas, 2006: 153). The body is a form of information and this can supersede and make redundant the 'talking individual, who owns the body' (Aas, 2006: 154), and they have been criticised for treating individuals as objects (Adey, 2004).

8.5.2 Prevalence of Biometrics

Using body characteristics to identify humans is not a new practice and Alphonse Bertillon whilst working for the Paris Police in the 19th century developed techniques for using body measurements to identify criminals (Jain, 2004). One of the major developments that has pushed forward the growth of biometrics has been digitalisation of the process that allows data to be captured and processed automatically as opposed to the lengthy human verification processes previously used. Technological advances have provided a catalyst for the explosion of biometric techniques but the increased need for certainty of identification within the context of global security risks has provided the political impetus and public support for widespread use of Biometrics (Lyon, 2003). Lyon identifies a major factor in the explosion of surveillance being related to 'disappearing bodies' which is linked to increased global mobility and stretched social relationships that are caused by 'new technologies of travel and communication' (2003: 673). There has been a reduction in the number of processes that are managed through face-to-face relationships and individuals are created as 'data images' in surveillance systems meaning that governments have identified an increased need to utilise data flows to track individuals.

Jain (2004) categorised the use of biometrics into the following three main areas: commercial (e.g. computer network login), government (e.g. border control) and forensic (e.g. criminal investigation). Biometrics has been applied across a range of contexts but the discussion below documents the growth of biometrics systems to produce secure borders. Biometric systems are used across border controls to increase security by providing certainty in the realm of identity leading to the identification of threats (Ceyham, 2008: 104).

One of the first uses of biometrics to secure borders was implemented in the early 1980s across the Mexican-American border for intercepting smugglers during the war on drugs. The European Union (EU) started to develop biometrics systems in 1997 through the creation of the Eurodac database and the systems used digitised fingerprints of individuals seeking access to EU countries to allow authentication of asylum seekers (Ceyham, 2008: 114). The "war on terror" that occurred after 9/11 acted as a catalyst for an 'exponential increase in the utilization of biometric technologies' (Wilson, 2007). Biometrics initially targeted specific groups of travellers including immigrants, asylum seekers and terrorists but the net of surveillance has been widened to 'whole national populations' (Wilson, 2007: 207).

The New York and Washington attacks intensified the dramatic emphasis on identity and identification means and technologies. Since then, knowing with certitude who is who and assigning a recognizable identity to someone, group or entity, have become important tasks for governments and law enforcements agencies. Now more and more governments seek to adopt new technologies of identification like biometrics in order to securtize identities and identification means and to monitor the movements of people inside and across borders.
(Ceyham, 2008: 109)

After 9/11, governments took advantage of widespread public support to push through the expansion of surveillance systems and rationalised the increase by developing political rhetoric that emphasised safety and predicting future dangers (Lyon, 2003). The anti-terrorist laws that followed the events of 9/11 provided the framework to authorise the increased use of surveillance techniques that were dominated by technological solutions. The growing size of government budgets allocated to biometric development since 9/11 is evidence of their growing commitment to securing their borders. The Australian government in 2005 dedicated $182 million to the development of biometric border controls including biometric passports and facial recognition systems (Wilson, 2007: 209). The growing demand for surveillance equipment has presented commercial opportunities for businesses to take financial advantage of the opportunities presented after 9/11 (Lyon, 2003: 675).

8.5.3 The Impact of Biometrics

When implementing biometrics system there are a number of factors that need to be considered and different types of biometric system are more appropriate for certain contexts and operational purposes. A key consideration is performance and this relates to the speed and accuracy of the recognition that can be affected by the environment where the system operates (Jain, 2004). Other considerations are the acceptability of the system by the data subjects and how easily the system can be fooled using fraudulent methods. Iris recognition systems are relatively easy to use allowing large numbers of individuals to be processed rapidly but problems can occur with reflection from glasses or the cameras. In the United Arab Emirates an iris recognition system has been found to be an effective method of detecting excluded individuals re-entering the country (Rosenzweig, 2004: 3). An average of 30 individuals were caught per day and statistical analysis of the system suggested that the likelihood of a false positive match is 1 in 80 billion. The systems are not cheap and they require continual management to up-date the system with new individual data.

The United States Visitor and Immigrant Status Indicator (US-VISIT) system is used in the US to track individuals entering the country by matching fingerprints of their left and right index finger and a facial image against a database of banned individuals which in 2007 contained 2.5 million names. Over a three-year period between its implementation in 2004 and 2007 more than 75 million individuals

were checked by the system resulting in 1,000 being denied entry (Jain, 2007: 39). Jain (2007) notes that there is no optimal biometric system and consideration needs to be given to the how the specific characteristics of a biometric system meet the application demands defined by the operational mode of the biometric system and the environmental characteristics of the deployment area.

Biometric system are based on matching data taken from individuals to an algorithm within the system and in a number of cases they have removed human discretion from the process meaning there is no appeal process built into the system and this can have exclusionary consequences (Graham and Wood, 2003: 232). Biometric applications can pose difficulties for certain groups and individuals with poor eyesight may have problems using iris recognition systems and the systems have difficultly recognising people with glaucoma or cataracts (Rosenzweig, 2004). Research conducted by The UK Passport Service (quoted in Wickins, 2007) found that biometrics systems have difficulties enrolling and identifying individuals who fall outside the range they define as normal. The research found that 0.62% of disabled people could not enrol any biometric data and, when translated into millions of individuals using a system, these could constitute large numbers of people. Elderly people and people of certain races also experienced difficulties enrolling data, and these problems could potentially exclude individuals from participation in society and deny access to services.

Biometrics can derive information beyond the identification of individual and this raises a number of questions related to whether this data could be used to profile individuals. Information taken from a retinal scan can provide medical information related to diabetes or high blood pressure levels for an individual and this information could subsequently be used 'in an unethical way for economic gains by denying benefits to a person determined to be of high risk' (Jain, 2007: 19). Biometric systems may never provide a perfect identification tool but many types of systems disadvantage specific groups and these issues need to be addressed to avoid negative societal and ethical consequences.

Many authors (Wickens, 2005; Ackleson, 2005; Wilson, 2007; Ceyham, 2008) have raised concerns regarding the possibility of that biometric systems may be responsible for social exclusion.

> *Biometric systems both serve then to accentuate and reproduce codes of inclusion and exclusion already embedded within social structuring. How such codes are configured within specific national contexts therefore affects how biometrics surveillance is mobilised and experienced.*
> *(Wilson, 2007: 208)*

Biometrics systems are a form of social sorting and aim to categorise people for various purposes and 'it is a means of inclusion and exclusion, of acceptance and rejection, of worthiness and unworthiness' (Lyon, 2003: 674). Lyon refers to the process of 'digital discrimination' where personal data is shifted to legitimise the presence or movement of some and reject others. The focus of the body as a

source of information and identification creates new forms of identity that are binary based on either acceptability or denial without providing any form of subjectivity (Aas, 2006).

> *In automated interaction there is no distinction between what is normative and what is practicable. All that works is norm and all that does not work is deviance. In an efficient socio-regulating package, deviance becomes impossible and the norm becomes a technical rule of action, a neural parameter independent of decision and values. This is probably the most important transformation in the area of social control ever, at least outside exceptional periods of massive change in regulation, such as wars, revaluations or major disasters.*
> *(Lianos and Douglas, 2000: 266)*

Liano and Douglas (2000) identified how automated systems such as biometrics differentiate from previous social control systems as they treat all prospective users of the system as potential offenders and therefore in a uniform manner. Previous systems have relied on surveying social spaces to identify threatening exceptions to the norm. A theme that emerges is that surveillance is 'completely dissociated from the social bond' (Liano and Douglas, 2000: 269) but this perspective ignores the cultural, political, economic and social factors that can modify the operation of biometrics systems. Amoore (2006) suggested that the biometrics systems that play a part in the management of US borders are not just a method of controlling the movement of bodies across space and should be understood 'as a matter of biopolitics, as a mobile regulatory site through which people's everyday lives can be made amenable to intervention and management'.

Graham and Wood (2003) noted that technological security systems are viewed as automated systems but are mediated by social practices and, due to their flexibility, are influenced by human judgements through their creation and operation. Human discretion is used when developing the algorithms and software that dictate how a system will impact on the individuals processed and the experience can significantly impact on their social mobility and life chances.

> *On the one hand, systems can be designed to be socially excluding, based on automated judgements of social and economic worth; on the other hand, the same system can be programmed to help overcome social barriers and processes of marginalization. The broad social effects and policy implications of digital surveillance are thus contingent and, while flexible, are likely to be strongly biased by the political, economic and social conditions that shape the principles embedded in their design and implementation.*
> *(Graham and Wood, 2003: 229)*

Emilio and Massari (2008: 497) suggested that when identification systems have historically been developed they have been embedded in 'a web of economic interests, political relations, symbolic networks, narratives and meanings'. The authors raise a number of concerns regarding the implementation of government controlled biometric systems but also highlight the potential for the

systems to have a positive benefit and provide the opportunity to turn individuals from excluded countries or groups into global citizens by challenging their powerless and anonymous identities. Wilson (2007:214) suggested that biometrics added to the 'historic categories of exclusion and criminlisation' and in the context of Australia this included the marginalised and indigenous, as they were the first to be enrolled on emerging biometric systems.

One of the major concerns that has been documented regarding biometrics system is 'function creep' which entails the data being used for a variety of reasons beyond why it was originally collected (Rosenzweig et al, 2004; Emilio and Massari, 2008). Emilio and Massari (2008) warned that 'function creep' has the potential to erode public trust and reduce confidence in biometric processes. The authors categorised 'function creep' as involving three elements: a policy vacuum, an unsatisfied demand for a given function, and a slippery slope effect or a covert application. Policy creep can occur when new technologies are deployed without the creation of specific policies to guide their operation that can result in stakeholders driving the process through their own interests. Unsatisfied demand involves data being collected for one purpose and, due to an unmet need within another area, being used above the purpose it was originally collected. The covert inappropriate usage of biometric data can occur due to gradual minor changes that can slowly divert the usage of the information or through a more planned hidden agenda. Biometric systems generate huge amounts of data some of which is beyond what is needed for personal recognition and this creates the potential for the data to be used for unintended or unauthorised uses.

As previously stated, biometrics is being marketed by governments as a solution to the post 9/11 terrorist threat but ultimately these systems may be flawed in that they rely on stored algorithms to identify threats, therefore they are not capable of monitoring 'previously unknown potential terrorists' (Lyon, 2003: 675). Ackleson (2005: 138) points to the political appeal of stricter border controls that offer some additional surveillance but have limited impact on 'terrorism given the macroeconomic pressures and flows under globalization and free trade'. Managing the data that is required to make biometrics systems run effectively is a significant challenge and records may not locate potential terrorists, for example, several of the 9/11 terrorists had expired visas but none were 'targeted for investigation as an absconder' (Ackleson, 2005: 150) The creation of biometrics systems creates another tool in the drive to increase security but human beings have the capacity to understand and evade the technologies.

> *In western liberal democracies the advantages of technology and other strategic surveillance developments are often short lived and contain ironic vulnerabilities. The logistical and economic limits on total monitoring, the interpretative and contextual nature of many human situations, system complexity and interconnectedness, provide ample room for resistance.*
> *(Marx, 2003: 369)*

The process of creating a technological fix to address security problems will be a constantly evolving problem that has huge financial implications for governments and the effectiveness of these systems has not been fully established. The biometric security industry markets their products as solutions to security problems post 9/11 but many of these systems have not be extensively tested in real world setting over sustained periods of time (Ackleson, 2005: 148). Biometrics systems also require 'complex bureaucratic' processes in place to operate successfully and more expertise and research needs to be developed in this area. Governments need to ensure that security across borders does not impact upon the legitimate international economic activities that are a large part of globalisation.

8.6 Radio Frequency Identification (RFID) Technology

8.6.1 Defining RFID

RFID technology facilitates the identification of objects, animals and people by using radio waves. RFID is an electronic identification device and is classified as an automatic identification tool along with biometric systems (Schmidt, 2007: 249). RFID can be used to store information beyond what is simply needed to identify individuals, which has potentially profound implications. A RFID system is made up of three main components:

1. the RFID tag or transporter, carries object identifying data
2. the RFID reader, or transceiver, reads and writes tag data
3. the back-end database associates records with tag data collected by readers

Every person or object that needs to be identified through an RFID system must have a tag physically attached. The tag reader gathers information from tags by sending out a radio frequency signal and a tag will respond to the signal by sending back identification information and/or other stored data. The reader converts data from the tag into digital data and this is sent through to appropriate agencies where either automated identification process occurs or there is human processing of the data. RFID readers and tags must be tuned to the same frequency and the range between the two devices depends on whether the tag is active – has an internal power supply, or passive – draws power from the field created by the reader. There are obvious threats to RFID systems that stem from physical attacks on the tag or reader devices but a number of other potential security and privacy threats have been identified including (adapted from Rieback et al, 2006: 65-66):

Sniffing: RFID tags are indiscriminate and could potentially be readable by any compliant reader therefore providing the potential for unauthorised readers scanning tags. Unrestricted access could mean personal information such as a person's medical predispositions could be extracted and used to inform insurance coverage.

Tracking: RFID technology could be used to track individual's movements through the use of strategically placed readers and this provides the opportunity for governments to monitor the movement of individual or groups.

Spoofing: Authentic RFID tags could be produced and attached to objects that could subsequently be used to falsify the identity of goods or gain unauthorised access to services.

Replay attacks: Replay devices can intercept and retransmit RFID queries from readers or tags which could be used to abuse various RFID applications.

Denial of Services: Tags can be removed from items or people or aluminium foil can be used to block RFID systems disrupting the system and subsequently causing systems to record useless data and discrediting the technology.

The first widespread commercial usage of RFID began in 1987 for electronic toll collection in the United States and the 1990s saw the widespread use of RFID to prevent shoplifting (Schmidt, 2007). RFID has been used across a number of security areas including anti counterfeiting (Tuyls and Batina, 2006), monitoring the movement of people into and out of buildings, preventing the unauthorised taking of goods (Bvoulard, 2005) and monitoring the movement of offenders through electronic tagging which are considered in more detail below.

8.6.2 Electronic Monitoring of Offenders

Electronic monitoring (EM) equipment is used as a surveillance tool to track whether offenders serving curfews comply with their curfews. The sanction has been criticised for emerging purely as a result of the new technology and as its implementation has been driven by technological advances (Padgett et al, 2006). The discussion below examines how the sanction impacts on people's lives and its effectiveness as a public protection tool and a rehabilitation technique.

Electronic monitoring works by attaching a tag the size of a watch around an individual's ankle. The tag contains a transmitter which sends a signal to a receiver that subsequently sends information via a phone line to a central computer (National Audit Office, 2006: 40). The receiver has a set range and this is usually the perimeter of an individual's house. When the tag is taken outside the range of the receiver there is a break in the signal and this information is relayed to a central computer and subsequent processed by an officer.

Electronic monitoring technology has made supervising curfews a precise science with the removal of the need for any human co-presence and the introduction of the 'electronically mediated remote monitoring' (Bottomley, Hucklesby, Mair and Nellis, 2002: 56). Electronic monitoring reflects a move away from processing humans through direct interaction and instead digital information is used to monitor and make decision regarding how they are processed and this reflects a theme drawn out across the two other security technologies covered in this module. Surveillance is undertaken at a distance through the 'the computerised creation of digital personae from a variety of data'

and in terms of electronic monitoring this includes 'risk profiles, curfew schedules and recorded conversations with monitors' (Bottomly et al, 2002: 78). Electronic monitoring is another example within this unit of a surveillance technique that is focused upon the body and this can remove the need to understand why an individual has behaved in a certain manner.

Initial criticisms of the technology indicated that the invasion of the private realm by governments using private bodies was intrusive and barbaric (Lilly and Ball, 1987). Electronic monitoring of offenders on curfews aims to protect the public by acting as a control mechanism and allowing offenders to rehabilitate within their own home with the additional benefit of removing individuals from custodial settings which can reinforce their offending behaviour. The UK has adopted two forms of electronic monitoring orders (National Audit Office, 2006):

Home Detention Curfews that allow prisoners sentenced to over 3 months in custody to be released early to an address to help individuals make the transition from custody to the community. Prisoners can only be released early if they meet the eligibility criteria and failure to keep to the conditions of the curfew means they will be returned to prison.

Curfew Orders can be imposed on an offender as a stand-alone community order or in conjunction with other sentences. The curfew hours are set by the court and must be between 2 and 12 hours a day. The curfew should be put in place to disrupt offending patterns and this may include shoplifting or alcohol related offences. The strength of the sanction is that it allows offenders to maintain their employment and family ties.

Bottomley et al (2004) examined the factors that made electronic monitoring a distinctive and new form of social control and suggested that it forms part of the managerialism approach of New Labour that is characterised by efficiency and real time control, risk management and enforcement. The technology represented a movement away from the humanistic values traditionally held by the Probation Service that involve the 'slow nurturing of inner change in offenders' and electronic monitoring represents a movement 'towards the galvanising of rapid processes of outward compliance' (Bottomley et al, 2004: 71). The technology provides the capacity for real-time monitoring of offenders' movements and this offers a new level of power to their supervisors. The risk management characteristics of electronic monitoring reflect the emergence of a 'risk society' and the influence of commercial agencies in the monitoring process leading to pro-active approaches. The technology addresses some of the uncertainties linked to other community sentences, as constant surveillance and accurate monitoring should in theory lead to higher levels of social control. Electronic monitoring is a surveillance device and does not put any physical limitations on offenders therefore the compliance and enforcement aspects of the sanction depends on offenders keeping to the conditions of their curfew due to the surveillance of the technology. The ability of the state to monitor the locations of offenders through electronic monitoring reflects a common experience for individuals within late modern society. Although it is different

from the 'self-chosen locatability' experience by the general public they are 'on the same continuum of experience (Nellis, 2003: 73).

8.6.3 Growth of Electronic Monitoring

Electronic monitoring technologies have been developed to facilitate management of offenders in the community through 'control at a distance in real time' (Bottomley et al, 2004: 79) and the new technology has changed the way offenders are controlled. Electronic monitoring first appeared in Mexico in 1984 and subsequently the United States adopted the technology (Whitfield, 1997). Electronic monitoring trials were conducted across the UK for ten years before it was finally integrated into the criminal justice system in 1999 (Bottomley at al, 2004). In the UK there was initially a slow take up of electronically monitored curfews and this pattern has been attributed to a lack of confidence in the measure from magistrates, youth offending teams and probation officers (Richardson, 1999; Nellis, 2003: 68). The initial apprehension has given way to widespread acceptance and across England and Wales there has been a dramatic increase in the usage of electronic monitor curfews with the number of cases rising from 9,000 in 1999/00 to 53,000 in 2004/05 (National Audit Office, 2006).

In the UK the growth of electronic monitoring has been driven by a need to address the problem of prison overcrowding in a cost effective manner (Payne and Gainey, 2000: 497; Nellis, 2002) and the technology was adopted in Canada for similar reasons (Bonta et al, 2000b). A National Audit Office report (2006: 13) stated that on average 90 days on home detection curfew cost £1,300 and the same length of time on a curfew order cost £1,400, compared to 90 days in custody which costs £6,500.

There has been widespread academic debate about whether electronic monitoring achieves the goal of reducing the prison population as it may widen the net of the criminal justice system.

> *Critics also claimed that the sanction was not really an alternative to incarceration but simply a new sentence alternative. The belief was that this new sanction would simple widen the new of criminal justice control. In effect, some believe that offenders sentenced to electronic monitoring are actually offenders who in the past would have been informally diverted from the justice system altogether. (Payne and Gainey, 2004: 414)*

The research literature on net widening has highlighted that relatively low risk offenders are often placed on electronically monitored curfew (Padgett et al, 2006). When the risk to public safety of offenders on electronic monitoring sanctions was compared to other community orders evidence was not found of a net widening effect with offenders having a high likelihood of a custodial sentence if they were not given a electronically monitored curfew. The intense surveillance could potentially increase the likelihood of offenders being caught violating their curfews which may lead to the possibility of tougher penalties and ultimately prison. Pidgett et al (2006: 64) found that the intensive surveillance

offered by the technology did not lead to more breaches and prison sentences compared to other community sentences.

The government allowed the private sector to manage the delivery of electronic monitoring in the UK and the delivery was characterised by a lack of 'managerial or operational' contact between the private sector and the probation and youth offending services (Nellis, 2003: 62). Nellis suggested that electronic monitoring was a 'parallel not an integrated development' referring to its place in the offender management of individuals within community settings (2003:62). The commercial influence within the realm of electronic monitoring reflects a general a pattern that is witnessed across the implementation of security technologies.

8.6.4 The effectiveness of electronic monitoring

In the UK the roll out electronic monitoring was not informed by a large body of research that had established the effectiveness of the intervention and this matches a similar trend witnessed during the widespread implementation of CCTV. The introduction of electronic monitoring has resulted in a number of studies being conducted into its effectiveness (e.g. Mair and Nee, 1990; Mair and Mortimer, 1996). Although electronic monitoring has been widely adopted in the UK, United States and across a number of European countries, 'there is insufficient evidence available to determine whether electronic monitoring helps to reduce re-offending or promote rehabilitation' (House of Commons, 2006).

The effectiveness of electronic monitoring has mainly been evaluated using two measurements: whether individuals finish their orders and the impact of the curfew on offending behaviour. Evaluating completion rates of electronically monitored curfews represents the viewpoint that the role of the technology is to deter offenders from breaking their curfews therefore helping to ensure public safety whilst reducing the prison population (Bonta et al, 2000b, 64). Public interest, the media and public official often portray offenders as dangerous and concerns have been raised regarding the fact that curfews could easily be broken and they result in an increased risk to the community (Painey and Gainey, 2000: 84)

Early research focused on completion rates for electronically monitored curfew. The first trials of electronic monitoring in the UK were evaluated in terms of how the technology worked in the context of bail curfews and found that 58 per cent of the sample abused their bail (Mair and Nee, 1996). This related to 22 per cent offending on bail and a further 36 per cent violated the conditions of their bail, but the sample population was small. The Criminal Justice and Public Order Act (1994) introduced electronic monitoring as a means of enforcing a curfew order as part of a community sentence and a Home Office funded study found a 75 per cent completion rate for the orders (Mair and Mortimer, 1996). Dodgson et al (2001) found that around 5% of those placed on Home Detention curfew breached their curfews and were recalled to prison. There was variation in compliance rates across different offender types with burglary offenders being most likely to be recalled and fraud or forgery offenders being most compliant. Breach rates may be lower for home detention curfews compared to curfew

orders as part of a community sentence because violations result in recall to prison whilst any breach of a community order results in an individual being resentenced at court.

Padgett et al (2006: 81) showed that electronic monitoring 'significantly reduces the risk to public safety from offenders living in the community' as they reduced the likelihood of individuals committing a new offence and acted as a deterrence in relation to absconding from a curfew. When offenders were asked why they complied with curfews their responses fell into four categories: threat of punishment, monitoring potential, conventional ties and offender characteristics (Payne and Gainey, 2004: 423). Technology facilitates compliance as they help offenders promote the view that any breaches of the curfew will be instantly detected and an appropriate sanction would follow. The study found that some offenders perceived that they had too much to lose by trying to escape and the controlling nature of the electronic monitoring technology can make the offenders experience the sanction as omnipresent. How the technology impacts on individuals and seeks to produce social ordering has been criticised by Nellis (2003: 77)

> *Integral to this longing for omniperception and perfect meticulous control is a Manichean sensibility – a composite mood of suspicion, fear and hatred – which sees threat and danger everywhere and encourages the development of a permanent watchfulness, tight controls and as the ultimate backstop, tough punishment. Judged against this ideal of meticulous order the 'normal' vitality and unpredictability of human beings is interpreted to indicate their inherently unruly or intractable wicked nature – A chilling perception, which in turn galvanizes renewed attempts at exclusion or repression.*

Offenders who have experienced electronic monitoring indicated that one of the negative aspects of electronic monitoring was the loss of privacy as the equipment provides constant surveillance of their compliance (Painey and Gainey, 2000: 88; Nellis, 2004: 72).

Evaluating the impact of electronic monitoring on recidivism rates involves some considerable methodological challenges. Quasi-experimental studies have studied the impact of electronic monitoring by matching experimental and control groups but identifying suitably matched groups can be difficult given the range of factors that can influence recidivism including age, gender, marital status, employment status and the overall risk levels of offenders as measured by various tools (Bonta et al, 2000b). Research has been critcised for selecting low risk offenders to test the effectiveness of electronic monitoring (Gainey et al, 1998) and using relatively short evaluation time periods (Finn and Muirhead-Steves, 2002: 298).

An evaluation of three Canadian electronic monitoring programmes found no clear evidence that they had a positive impact on re-offending (Bonta et al, 2000b). When offender risk levels were controlled for rates of recidivism for

electronically monitored offenders were not significantly different from probationers not under surveillance and prisoners. A study (Finn and Muirhead-Steves, 2002:307) found that electronic monitoring for male violent parolees did not have any significant effect 'on the likelihood of a parolee being committed to prison during the follow up period or on the amount of time before recommitment to prison'. The research did find that electronic monitoring was more effective for sex offender compared to other violent offenders which suggest that the sanction may have beneficial effects for some types of offenders. Suggs et al (2001) found that there were no significant differences in compliance levels for electronically monitored curfew orders compared to a comparison group serving other community penalties.

Research has examined how individuals experienced electronic monitoring and this research is important in the context of widespread condemnation of the punishment as too lenient. Payne and Gainey (2004) interviewed 49 offenders and found that the sanction was not overly lenient and aspects of the experience that were problematic were the shameful nature of the sanction and the limitations imposed on social interactions. Physiological needs that were flagged up as issues were limitations on exercise and the ability to visit shops to buy food.

The advocates of electronic monitoring suggest it offers offenders the opportunity to rehabilitate at home with their families engaging in pro-social activities away from criminal associates within custody or the community that may prove a negative influence and lead to further offending (Ball and Lilly, 1986; Richardson, 1999: 161). Research found that 95 per cent of offenders agreed that the sanction had rehabilitative benefits related to maintaining ties with families, keeping jobs and helping with household duties (Payne and Gainey, 2000, 2004) and these positive aspects of the sanction highlighted that individuals with certain lifestyles benefit more for electronic monitoring punishments. Research has highlighted women and married people as benefiting from electronic monitoring (Painey et al, 1998; Painey and Gainey, 2002). Younger offenders may experience electronic monitoring as difficult as many do not have home-centred lifestyles (Nellis, 2003: 72). Certain types of offenders have been shown to be more likely to benefit from electronic monitoring including lower level offenders (Gainey et al, 2000).

Evidence has been found that suggests in some circumstances electronic monitoring can create tensions within a household (National Audit Office, 2006; Gibbs and King, 2003) but generally the sanction provides the opportunity for offenders to gain structure in their life and contemplate their past misdemeanours and make positive changes to their lifestyles (Gainey and Payne, 2000). The experience of being at home for prolonged periods of time meant that some individuals engaged in more pro-social activities and took on family responsibilities (King and Gibbs, 20003).

As with other technological developments considered in this unit the effectiveness of electronic monitoring is increased when it works in conjunction with other interventions (Payne and Gainey, 2000). Support from probation

officers was highlighted as being important in relation to compliance levels (Gibbs and King, 2003: 122). Research has found that high risk offenders being electronically monitored and in treatment had lower levels of recidivism compared to probationers in treatment (Bonta et al, 2000a). An evaluation of curfew orders conducted in the UK found that practitioners believed that electronic monitoring could be beneficial used with other types of community orders (Walters, 2002).

In the context of offender management, research suggests that the role of electronic monitoring is mainly controlling the risk to the public of offenders living in communities (Bonta et al, 2002b; Pidgett et al, 2006). The research on electronic monitoring has not found that the intervention has a significant impact on recidivism (Whitfield, 1997; Suggs et al, 2000; Finn and Muirhead-Steves, 2002) but further research is needed to ascertain whether certain types of offenders may benefit from the sanction. The role of electronic monitoring is essentially to control offenders and act as a deterrent and the role of technology is to ensure that the monitoring is a precise science through the provision of data related to offenders' behaviour. Problems have been noted in relation to the reliability of the monitoring equipment (King and Gibbs, 2003) but generally studies have found that the equipment proved to be robust (National Audit Office, 2006) and this helps ensure the positive impact the technology can have over offender.

8.7 Integrating Security Technologies

Security technologies are often used alongside other crime prevention measures or integrated with other technologies to enhance their effectiveness. For example, the security solution that has been put in place to address the risk posed by terrorism in London is a convergence of target hardening and CCTV surveillance practices (Fussey, 2007). The anti-terrorist strategies put in place to counter the effects of potential major terrorist threats, such as vehicle-based bombs, include traditional situational crime prevention measures (e.g. introducing barriers and bollards, reducing the number of entrances to buildings, restricting parking) which work alongside surveillance technologies.

The three security technologies discussed above are often linked to computer databases that help process the data collected. Lyon (2002: 246) made the following comment when examining security technologies and the opportunities they provide for intensive surveillance:

> *It is their dependency on computer-based information infrastructures that gives them their peculiar power. Without the assistance of complex and sophisticated data processing power, these new technologies would remain relatively weak as surveillance tools*

Digital CCTV systems have been linked to various computer programmes to help operators identify 'unusual events' such as a person behaving suspiciously, problematic individuals or specific vehicles (Graham, 2000: 47). The purpose of

the technologies is to help law enforcement agencies 'in their decision-making coordination, control, analysis and visualisation (Ceyham, 2008: 109). Biometrics systems depend heavily on connective technologies because without the system's ability to compare the captured data to individuals in a searchable database, the process would not have the capacity to efficiently identify individuals and threats.

Facial recognition technology is a security measure that integrates CCTV and biometric systems. The process involves CCTV cameras surveying individuals and attached to the cameras are "Face Grabbers" which are devices that extract face images from the continuous video stream (Gates, 2002). The images are converted into templates that are compared to templates stored in a database of risky individuals such as terrorists or criminal suspects. When a match is found the system will alert a human operator who takes appropriate action.

Introna and Wood (2004) suggest that the processing of people through facial recognition systems has a number of political implications that are not fully understood. The systems depend on algorithms that define when individuals are matched to samples taken by the cameras. These algorithms have a profound impact on how the systems work and the systems make use of computer programmes 'to provide more than the raw data observed' (Introna and Wood, 2004: 181) through the CCTV cameras. Research has found that the algorithms display identification biases and recognition rates are higher for males and older people. Green et al (2003: 9) came to the conclusion that 'some people are easier to identify than others' and this included the finding that other races were easier to identify than white including Asians and Afro-Americans. The technology is not intrusive and data can be collected and processed without individuals' knowledge and the algorithms at the centre of the process are very difficult to scrutinise due to their complex nature.

The effectiveness of facial recognition technologies relies heavily on the quality of the image captured and in crowded or outdoor environments capturing a high quality image can be problematic. A number of other factors can impact on the identification process and these include the length of time between when the image in the database was captured and when the image was taken by the camera (ibid: 189). If systems have to compare images to large numbers of records in a database this can have a detrimental effect on the system's ability to identify people. Lyon (2003: 671) argued that facial recognition technology has only limited uses and will probably be ineffective against terrorism as capturing high quality images of terrorists to store in data is difficult and they can wear disguises to avoid recognition.

A facial recognition system was linked to 300 cameras in the Newham district of London. Introna and Wood (2003) reported that the police admitted the system had not led to any positive identifications, despite being linked to a small database of offenders. The integration of security technologies appear to offer ways of processing data collected about individuals and alerting agencies to risky individuals. The technological fix that many of the systems offer has many weaknesses and the technology has to prove itself in real world environments

before it will become a widespread technique of surveillance. Many terrorist threats are not from individuals who are known to law enforcement agencies meaning their data will not be stored on databases which allows them to avoid automated recognition.

8.8 Summary

The widening usage of technologies for security purposes has produced a plethora of research papers and one of the central themes that emerged was that any technology should not be viewed as a panacea but one element of a security process. The implementation of security technologies has often been characterised by an absolute belief in their effectiveness and there has not been enough debate concerning whether the systems are appropriate for the specific security requirements of a given context. Research has started to identify where CCTV may be effective and what operational processes need to be in place but work on biometric technologies is in its infancy regarding the effectiveness of systems, particularly the impact that algorithms within the system may have upon on their operation.

Research has started to establish a body of work that identifies some of the ways that the new technologies are impacting on society. Graham and Wood (2003: 232) point to the importance of working to 'expose the ways in which these systems are used to prioritise certain people's mobilities, service quality and life chances, while simultaneously reducing those of less favourable groups'. The impact of these technologies can be subtle and individuals may be unaware of how their lives are being affected which creates real challenges for researchers.

This unit has explored some of the reasons why security technologies have dramatically increased and some of the key drivers behind the growth including the use of digitalisation to support neoliberal economic agendas. The influence of the private sector within public services has been raised as a concern by academic authors and increased regulation has been proposed to address the challenges to civil liberties that the technologies represent. The current legislation designed to protect privacy is not adequate to limit the unregulated growth of surveillance systems (Lyon, 2003). Lyon (2004: 137) suggested that the technological fixes and the associated surveillance systems might be creating another form of risk due to the inadequate safeguards in place to protect an individual's personal data.

Currently there is a wave of public support for increased security technologies which is built on perceived high levels of risk across societies. Research examining the sustained impact of the technologies has shown that public support can reduce if their experiences of the technology do not meet their expectations (Gill and Spriggs, 2005). Concerns have been raised that the technological solutions to surveillance 'hold significant symbolic appeal' rather than offering real protection from threats (Ackleson, 2005). Different technological security measures have been implemented at different rates across the world and there is the opportunity to learn from the experiences of others and this remains one of the challenges for researchers (Lyon, 2004).

8.9 Guide to Reading

You should now access the following two journal articles:

Dubbeld, L. (2005) 'The role of technology in shaping CCTV surveillance practices', *Information, Communication and Society,* 8 (21): 84-100.

Lyon, D. (2002) 'Everyday Surveillance: Personal data and social classifications', *Information, Communication and Society,* 5 (2): 242-257.

Additional Reading
Visit the 'Surveillance and Society' website (http://www.servillance-and-society.org) and download the paper below to gain more insight into the human element of CCTV systems

Smith, G. (2007) 'Exploring Relations between watchers and watched in control (led) systems: Strategies and tactics', *Surveillance and Society,* 4 (4): 280-313.

The following article explores many of the biometric issues discussed above within the context of Foucault's notions of discipline and power:

Epstein, C. (2007) 'Guilty Bodies, Productive Bodies, Destructive Bodies: Crossing the Biometric Borders', *International Political Sociology;* 1 (2): 149-164.

8.10 Study Questions

You should now write approximately 300 words in answer to each of the questions below. We believe that this is an important exercise that will assist you comprehension of the material and aid your progress on the course. Your answers are intended to form part of your own course notes and should not be forwarded to the University.

What are the main the strengths and weaknesses of using quasi-experimental and realistic evaluation models in relation to evaluating the impact of security technologies?

What are the advantages and disadvantages of the automated processes of identification contained in biometric systems?

Critically analyses whether offenders should be kept in prison or released early on Home Detention Curfews.

References

Aas, F.K. (2006) ''The Body does not lie': Identity, Risk and Trust in Technoculture', *Crime Media Culture,* 2: 143-158.

Ackleson, J. (2005) 'Border Security Technologies: Local and Regional implications', *Review of Policy Research*, 22 (2): 137-155.

Adey, P. (2004) 'Secured and Sorted Mobilities: Examples from the Airport', *Surveillance & Society,* [Online]. 1(4): 500-519. Available at: http://www.surveillance-and-society.org/articles1(4)/sorted.pdf [Accessed 5th March 2009]

Allard, T.J., Wortley, R.K., and Steward, A.L. (2008) 'The effect of CCTV on Prisoner misbehaviour', *The Prison Journal,* 88: 404-422.

Amoore, L. (2006) **'**Biometric Borders**:** Governing Mobilities in the war on terror**'** *Political Geography*, 25: 336-351.

Armitage, R., Smyth, G., Pease, K. (1999), 'Burnley CCTV evaluation', in Painter, K., Tilley, N. (eds), *Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention*, Criminal Justice Press, Monsey, NY, pp.225-50.

Ball, K. and Haggerty, K.D. (2005) 'Editorial: doing surveillance studies'. *Surveillance and Society,* [Online]. 3 (2/3): 129-138. Available at: http://www.surveillance-and-society.org/Articles3(2)/editorial.pdf [Accessed 1 April 2009]

Ball, K., Lyon, D. Wood, D.M., Norris, C. and Raab, C. (2006) A Report on the Surveillance Society for the Information Commissioner by the Surveillance Studies Network. [Online]. Available at: http://www.cosantasonrai.ie/docs/Surveillance_Society_Full_Report/378.htm [Accessed 1 April 2009]

Barr, R. and Pease, K. (1992) 'Crime Displacement to Crime Placement', in D.J. Evans, N.R. Fyfe and D.T. Herbert (eds) *Crime, Policing and Place: Essays in Environmental Criminology*, London: Routledge.

Bennett, T. and Gelsthorpe, L. (1996) 'Public Attitudes towards CCTV in Public Places', *Studies on Crime and Crime Prevention*, 5 (1): 72-90.

Bonta, J., Wallace-Capretta, S. and Rooney, J. (2000a) 'A quasi-experimental evaluation of an intensive rehabilitation supervision program', *Criminal Justice and Behaviour*, 27: 312-329.

Bonta, J., Wallace-Capretta, S. and Rooney, J. (2000b) 'Can electronic monitoring make a difference? An Evaluation of Three Canadian Programs, *Crime Delinquency,* 46: 61-75.

Bottomley, K., Hucklesby, A., Mair, G., and Nellis, M. (2004) *Electronic Monitoring of Offenders: Key Developments Issues in Community and Criminal Justice—Monograph 5* London: NAPO, 2004.

Bottoms, A. (2000) 'The relationship between theory and Research in Criminology'. in King, R. and Wincup, E. (eds) *Doing Research on Crime and Justice*. Oxford: University Press.

Boulard, G. (2005) 'RFID: Promise or Peril? It may be easier than ever to track information, but it is causing concerns over privacy and civil liberties', *State Legislatures Online,* [internet] 29th November. Available at: http://ecom.ncsl.org/programs/pubs/slmag/2005/05SLDec05_RFIDBadges.pdf [accessed 3 May 2009]

Brown, B. (1995) *CCTV in Town Centres: Three Case Studies*, Crime Prevention and
Detection Series, no.73. London: HMSO.

Cabinet Office (2008) Engaging Communities in fighting Crime: A review by Louise Casey, [Online]. London: Cabinet Office. Available at: http://www.cabinetoffice.gov.uk/media/cabinetoffice/corp/assets/publications/crime/cc_full_report.pdf [accessed 1 June 2008]

Ceyham, A. (2008) 'Technologization of Security; management of uncertainty and risk in the age of biometrics', *Surveillance and Society,* [Online]. 5 (2): 102-123. Available at:
http://www.surveillance-and-society.org/articles5(2)/technologization.pdf [accessed 4 March 2009]

Clarke, R. V. (2004) 'Seven misconceptions of situational crime prevention' in Tilley, T. (ed.), *Handbook of Crime Prevention and Public Safety*. Portland: Willan Publishing.

Clarke, A., and Dawson, R., (1999) *Evaluation research: an introduction to Principles, Methods and Practice*. Sage: London.

Clarke, Ronald V. and Marcus Felson (1993) 'Introduction: Criminology, Routine Activity and Rational Choice'. in (eds.) Clarke R. V. and Felson, M., *Routine Activity and Rational Choice, Advances in Criminological Theory* (Vol. 5). New Brunswick, NJ: Transaction Press, 1993: 1-14.

Colman, R. and Sim, J. (1998) 'From the Dockyards to the Disney Stores: Surveillance, Risk and Security in Liverpool City Centre', *International Review of Law, Computers and Technology,* 12 (1): 27-45.

Coleman, R. and Sim, J. (2000)'"You'll Never Walk Alone": CCTV Surveillance, order and Neo-liberal rule in Liverpool City Centre', *British Journal of Sociology,* 51 (4): 623-39.

Conche, F. and Tight, M. (2006) 'Use of CCTV to determine road accident factors in urban areas', *Accident Analysis and Prevention,* 38: 1197-1207.

Coupe, T. and Kaur, S. (2005) 'The Role of Alarms and CCTV in Detecting Non-residential Burglary', *Security Journal,* 18 (2): 53-72.

Crawford, A, (1998) *The Local Governance of Crime.* Oxford: Clarendon Press.

Ditton, J. (2000) 'Crime and the City: Public Attitudes to CCTV in Glasgow', *British Journal of Criminology*, 40: 692-709.

Ditton, J. and Short, E. (1999), 'Yes, It Works, No, It Doesn't: Comparing the Effects of Open CCTV in Two Adjacent Scottish Town Centres,' in Painter, K. and Tilley, N. (eds) *Crime Prevention Studies*, Vol 10: 201–224. Special edition entitled 'Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention'.

Dodgson, K., Goodwin, P., Howard, P., Llewellyn-Thomas, S., Mortimer, E., Russell, N., and Weiner, M. (2001) *Electronic Monitoring of Released prisoners.* Home Office Research Study 222. London: Home Office.

Emilio, M. and Massari, S. (2008) 'Body, Biometrics and Identity', *Bioethics,* 22 (9): 448-498.

Farrington, D. P. (2002) *Methodological Quality Standards for Evaluation Research*
Paper Presented at the Third Annual Jerry Lee Crime Prevention Symposium, University of Maryland.

Farrington, D. P., Gill, M., Waples, S. and Argomaniz, J. (2007) 'The effects of closed-circuit television on crime, meta-analysis of an English national quasi-experimental multi-site evaluation', *Journal of Experimental Criminology,* 3: 21-38.

Finn, M.A. and Muirhead-Steves, S. (2002) 'The Effectiveness of Electronic Monitoring with Violent Male Parolees', *Justice Quarterly,* 19 (2): 293-312.

Fussey, P. (2004) 'New Labour and New Surveillance: Theoretical and Political Ramifications of CCTV Implementation in the UK', *Surveillance & Society*, [Online]. 2 (2/3): 251-269. Available at: http://www.surveillance-and-ociety.org/articles2(2)/newlabour.pdf [Accessed 8th March 2009]

Gainey, R. R. and Payne, B. K. (2000) 'Understanding the experience of house arrest with electronic monitoring: An analysis of quantitative and qualitative data', *International Journal of Offender Therapy and Comparative Criminology,* 44: 84-96.

Gainey, R. R., Payne, B. K. and O'Toole, M. (2000) 'The relationship between time in jail, time on electronic monitoring, and recidivism: An event history of a jail-based program' *Justice Quarterly,* 17 (4): 733-752.

Gates, K. A. (2002) 'Wanted dead or digitized: Facial recognition technology and privacy', *Television New Media,* 3: 235-238.

Gerrard, G., Parkins, G., Cunningham, I., Jones, W., and Douglas, S. (2007) *National CCTV Strategy*. London: Home Office.

Gibbs, A. and King, D. (2003) 'Is home detention in New Zealand disadvantaging women and children' *The Journal of community and Criminal Justice,* 50 (2): 115-126.

Gill, M. and Turbin, V. (1999) 'Evaluating Realistic Evaluation: Evidence from a Study of CCTV', in K. Painter and N. Tilley (eds.), *Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention*, Monsey, NY: Criminal Justice Press, 179-200.

Gill, M. and Loveday, K. (2003) What Do Offenders Think About CCTV?, in M Gill (ed.): *CCTV*, Leicester: Perpetuity Press.

Gill, M., Smith, P., Spriggs, A., Argomaniz, J., Allen, J., Follett, M., Jessiman, P., Kara, D., Little, R. and Swain, D. (2003) *National Evaluation of CCTV: Early Findings on Scheme Implementation, Effective Practice Guide*, Home Office Development and Practice Report , no.7, London: HMSO.

Gill, M., Spriggs, A., Allen, J., Hemming, M., Jessiman, P., Kara, D., Kilworth, J., Little, R. and Swain, D. (2005a) *Control Rooms: Findings from Control Room Observations*, Home Office Online Report, London: Home Office.

Gill, M., Swain, D., Spriggs, A., Allen, J., Argomaniz, J. and Waples, S. (2005b) A*ssessing the Impact of CCTV – The South City Case Study*, Home Office Online Report, London: Home Office.

Gill, M., Little, R., Spriggs, A., Allen, J., Argomaniz, J. and Waples, S. (2005c) *Assessing the Impact of CCTV – The Hawkeye Case Study*, Home Office Online Report, London: Home Office.

Gill, M. and Spriggs, A (2005) *Assessing the Impact of CCTV,* Home Office Research Study 292. London: Home Office.

Gill, M., Rose, A., Collins, K. and Hemming, M. (2006) 'Redeployable CCTV and drug-related crime: A case of implementation failure', *Drugs Education, Prevention and Policy,* 113 (5): 451-460.

Gill, M., Bryan, J. and Allen, J. (2007) 'Public perceptions of CCTV in residential area: "It is not as good as we thought it would be', *International Criminal Justice Review*, 17: 304-324.

Givens, G., J.R. Beveridge, B.A. Draper and D. Bolme, (2003), *A Statistical Assessment of Subject Factors in the PCA Recognition of Human Faces.* [Online]. Available at: http://www.cs.colostate.edu/evalfacerec/papers/csusacv03.pdf [accessed 1 May 2009]

Goold, B. J. (2003) 'Public area surveillance and police work: the impact of CCTV on police behaviour and autonomy', *Surveillance and Society,* [Online]. 1 (2): 191-203. Available at: http://www.surveillance-and-society.org/articles1(2)/publicpolice.pdf [Accessed 3rd March 2009]

Graham, S. (2000) 'The fifth utility', *Index on Censorship,* 29 (3): 45-49.

Graham, S. and Wood, D. (2003) 'Digitizing surveillance: Categorisation, space, inequality', *Critical Social Policy,* 23: 227-248.

Hier, S.P. (2003) 'Probing the Surveillant Assemblage: On the Dialects of Surveillance Practices as Processes of Social Control'. Surveillance and Society, [Online]. 1, 3: 399-411. Available at: www.surveillance-and-society.org/articles1(3)/probing.pdf [Accessed 4 March 2009]

Hier, S.P. (2004) 'Risky Spaces and Dangerous Spaces: Urban Surveillance, Social Disorder and CCTV', *Social and Legal Studies*, 13, 4: 541-554.

Helton, F. and Fisher, B. (2003) CCTV in Berlin Shopping Malls. Working Paper no. 11. Centre for technology and Society, Technical University of Berlin. [Online]. Available at: http://www.urbaneye.net/results/ue_wp11.pdf [accessed 3rd March 2008]

Hempel, L. and Töpfer, E. (2004) Final Report: CCTV in Europe. Working Paper no. 15. Centre for technology and Society, Technical University of Berlin. http://www.urbaneye.net/results/ue_wp15.pdf [accessed 3rd March 2008]

Home Office (2002) *Passport to evaluation: an introduction to evaluating crime reduction initiatives and projects*. York: Home office Crime Reduction College. http://www.crimereduction.homeoffice.gov.uk/evalintro.pdf [accessed 3rd March 2009]

Honess, T. and Charman, E. (1992): '*Closed Circuit Television in Public Places: Its Acceptability and Perceived Effectiveness*', Police Research Group Crime Prevention Unit, 35, London: Home Office Police Department.

House of Lords (2009) *Surveillance: Citizens and the State*, *Volume I: Report*, London: The Stationary Office limited.

House of Commons (2006) *The electronic monitoring of adult offenders*, Sixty Second Report of Session 2005-06, London: The Stationary Office Limited.

Introna, L.D. and D. Wood (2004) 'Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems', *Surveillance & Society, [Online].* 2 (2/3): 177-198.
http://www.surveillance-and-society.org/articles2(2)/algorithmic.pdf [accessed 15th March 2009]

Jain, K. A. (2004) 'An introduction to biometric recognition', *IEEE Transactions on circuits and systems for video technology,* 14 (1): 1-10.

Jain, A. K. (2007) 'Biometric recognition', *Technology,* 499 (6): 38-40.

Klauser, F. R. (2007) 'Difficulties in revitalising public space by CCTV: Street prostitution in the Swiss City of Olten', *European Urban and Regional Studies,* 14 (4): 337-348.

Koskela, H. (2000) ''The gaze without eyes': video-surveillance and the changing nature of urban space', *Progress in Human Geography*, 24 (2): 243-265.

Koskela, H. (2003) ''Cam Era – the contemporary urban panopticon', *Surveillance and Society,* [Online]. 1 (3): 292-313. Available at: http://www.surveillance-and-society.org/articles1(3)/camera.pdf [accessed 7 March 2009]

Layder, D. (1998) *Sociological Practice: Linking Theory and Social Research.* London: Sage Publications.

Lianos, M. and Douglas, M. (2000) 'Dangerization and the end of deviance: The institutional Environment', *British Journal of Criminology,* 40: 261-278.

Lilly, J.R., and Ball, R.A. (1987) 'A brief history of house arrest and electronic monitoring', *Northern Kentucky Law Review*, 13, 343-374.

Lomell, H. M., Saetnan, A. R. and Wiecek, C. (2003) *Flexible technology, structured practices surveillance operations in 14 Norwegian and Danish organisations*. Working Paper no. 3. Centre for technology and Society, Technical University of Berlin. [Online]. Available at: http://www.urbaneye.net/results/results.htm [accessed 4 may 2009]

Lyon, D. (2003) 'Technology vs Terrorism': Circuits of city surveillance since September 11th', *International Journal of Urban and Regional Research*, 27 (3): 666-678.

Lyon, D. (2004) 'Globalising surveillance: comparative and sociological perspectives', *International Sociology,* 19: 135-149.

Mackay, D. (2006) 'The changing nature of public-space CCTV', *Security Journal,* 19: 128-142.

Mair, G. and Mortimer, E. (1996) *Curfew orders with Electronic Monitoring,* Home Office Research Studies no. 163, London: Home Office.

Mair, G. and Nee, C. (1990) *Curfew orders: the trials and their results*, Home office Research studies no. 120, London: Home Office.

Marx, G. T. (2003) 'A Tack in the shoe: Neuralising and resisting the New Surveillance', *Journal of Social Issues,* 59 (2): 369-390.

Mayhew, P. (1984)'Target-Hardening: How much of an answer?', in Clarke. R.V.G. and Hope, T. (eds) *Coping with Burglary,* Boston: KluwerNighoff.

Mazerolle, L., Hurley, D. and Chamlin, M. (2002) 'Social Behaviour in Public Spaces: An Analysis of Behavioural Adaptations to CCTV', *Security Journal,* 15: 59-73.

McCahill, M. (2002), *The Surveillance Web: The rise of Visual Surveillance in an English City*, Devon: Willan.

McCahill, M. and Norris, C. (2002a) *CCTV in Britain* Urbaneye, Working Paper no. 3. Centre for technology and Society, Technical University of Berlin. [Online]. Available at: http://www.urbaneye.net/results/results.htm [accessed 7 May 2009].

McCahill, M. and Norris, C. (2002b) *CCTV in London* Urbaneye, Working Paper no. 3. Centre for technology and Society, Technical University of Berlin. [Online]. Available at: http://www.urbaneye.net/results/results.htm [accessed 6 May 2009].

McCahill, M. and Norris, C. (2002c) *CCTV Systems in London; Their structures and practices* Urbaneye Working Paper no. 10. Centre for technology and Society, Technical University of Berlin. [Online]. Available at: http://www.urbaneye.net/results/results.htm [accessed 7 May 2009].

McCahill, M. and Norris, C. (2003), 'Estimating the Extent, Sophistication and Legality of CCTV in London', in M. Gill (ed.) *CCTV*, Perpetuity Press.

Mordini, E. and Massari, S. (2008) 'Body, Biometrics and Identity', *Bioethics,* 22 (9): 488-498.

National Audit Office (2006) 'The Electronic Monitoring of Adult Offenders' [Online]. Available at: http://www.nao.org.uk/publications/0506/the_electronic_monitoring_of_a.aspx [accessed on 4th May 2008]

Nellis, (2003) 'They Don't Even Know We're There: The electronic monitoring of offender in England and Wales', in Ball, K. and Webster, F. (eds) *The Intensification of Surveillance: crime, terrorism and warfare in the information age.* London: Pluto.

Norris, C. and Armstrong, G. (1999) *The maximum surveillance society. The rise of CCTV,* Oxford: Berg.

Norris, C. and McCahill, M. (2006) 'CCTV beyond Penal Modernism?, *British Journal of Criminology,* 46: 97-118.

Padgett, K.G., Bales, W. and Blomberg, T. (2006) 'Under surveillance: An empirical test of the effectiveness and consequences of electronic monitoring', *Criminology and*
Public Policy, 5: 61-92.

Pawson, R. and Tilley, N. (1997) *Realistic Evaluation*, London: Sage Publications.

Payne, B. K., and Gainey, R. (2004) 'The electronic monitoring of offenders released from jail or prison: safety, control and comparisons to the incarceration experience', *The Prison Journal*, 84: 423-434.

Ratcliffe, J. H. (2006) Video surveillance of public places**,** Problem Oriented Guides for Police, Response Guides Series, No. 4. Office of Community Oriented Policing Services (COPS office), US Department of Justice; Washington DC.

Reeve, A. (1998) 'The panopticisation of shopping: CCTV and leisure consumption', in Norris, C, Morran, J. and G. Armstrong (1998) *Surveillance, CCTV and Social Control*. Ashgate: Aldershot.

Reibeck, M. R., Crispo, B. and Tanenbaum, A. S. (2006) 'The Evolution of RFID Technology, *Pervasive Computing.* [Online]. Available at: www.cs.vu.nl/~ast/publications/ieeepc-2006.pdf [accessed 2 May 2008].

Reppetto, T.A. (1976) 'Crime Prevention and the Displacement Phenomenon', *Crime Prevention*, 22: 166–77.

Richardson, F. (1999) 'Electronic Tagging of Offenders: Trails in England', *Howard Journal of Criminal Justice,* 28 (2): 158-172.

Rosenzweig, P., Kochems, A. and Schwartz, A. (2004) 'Biometric Technologies: Security, legal and policy implications', *Legal Memorandum,* 12: 1-10.

Savona, E. U., and Mignone, M. (2004) 'The Fox and the Hunters: How IC Technologies Change the Crime Race', *European Journal on Criminal Policy and Research,* 10 (1): 3-26.

Schmidt, J. (2007) 'RFID and Privacy: Living in Perfect Harmony', *Rutgers Computer & Technology Law Journal,* 34: 247-272.

Sherman, L. W., Gottfredson, D., Mackenzie, D., Eck, J., Reuter, P. and Bushway, S. (1997) *Preventing Crime: What Works, What Doesn't, What's Promising*. Report to the U.S. Congress. Washington, D.C. U.S. Dept. of Justice.

Short, E. and Ditton, J. (1995) *Does CCTV Prevent Crime? An Evaluation of the Use of CCTV Surveillance Cameras in Airdrie Town Centre*, Edinburgh: Scottish Office.

Short, E. and Ditton, J. (1998): 'Seen and Now Heard: Talking to the Targets of Open Street CCTV', *British Journal of Criminology*, 38 (3): 404-428.

Simon Liu**,** Mark Silverman**,** (2001) 'A Practical Guide to Biometric Security Technology', *IT Professional*, 3 (1): 27-32. www2.computer.org/portal/web/csdl/doi/10.../6294.899930 [accessed 6 June 2008]

Sivarajasingam, V., Shepherd, J.P. and Matthews, K. (2003) 'Effect of urban closed circuit television on assault injury and violence detection. [Online]. 9: 312-326. Available at: http://www.injuryprevention.bmj.com [accessed on 5 December 2008]

Skinns, D. (1998) Crime reduction, diffusion and displacement: evaluating the effectiveness of CCTV. In Norris, C., Moran, J., and Armstrong, G. (eds0 *Surveillance, Closed Circuit Television and Social Control*. Ashgate: Aldershot.

South, N. (1998) Policing for profit, London: Sage.

Smith, G. (2004) 'Exploring Relations between watchers and watched in control (led) systems: Strategies and tactics', *Surveillance and Society,* [Online]. 4 (4): 280-313. Available at: http://www.surveillance-and-society.org/articles4(3)/watchers.pdf [accessed 8 June 2009].

Suggs, D., Moore, L. and Howard, P. (2001) *Electronic Monitoring of Offending behaviour: reconviction results from the second year of trails,* Home Office Research Finding 141. London: Home Office.

Surette, R. (2005) 'The thinking eye: Pros and cons of second generation CCTV surveillance systems', *Policing: An International Journal of Police Strategies and Management*, 28 (1): 152-173.

Tilley, N. (1993): *Understanding Car Parks, Crime and CCTV: Evaluation Lessons From Safer Cities*, Crime Prevention Unit, no.42, London: HMSO.

Tilley, N. (1998) Evaluating the effectiveness of CCTV schemes, in Norris, C., Moran, J., and Armstrong, G. *Surveillance, Closed Circuit Television and Social Control*. Ashgate: Aldershot.

Tilley, N. (2000) Realistic Evaluation: An Overview. Presented at the Founding Conference of the Danish Evaluation Society. September 2000. [Online]. Available

at: www.danskevalueringsselskab.dk/pdf/Nick%20Tilley.pdf [accessed 15 May 2009].

Troscianko, T., Holmes, A., Stillman, J., Mirmehdi, M., Wrights, D., and Wilson, A. (2004) 'What happens next? The predictability of natural behaviour viewed through CCTV cameras, *Perception,* 33: 87-101.

Tuyls, P. and Batina, L. (2006) RFID-Tags for anti-counterfeiting, [Online]. Available at: www.cosic.esat.kuleuven.be/publications/article-621.pdf [accessed 2 June 2008].

Webb, B. and Laycock, G. (1992) *Reducing Crime on the London Underground: An Evaluation of Three Pilot Projects,* Crime Prevention Unit: Paper no. 30, London: Home Office.

Welsh, B. and Farrington, D. (2002) *Crime Prevention Effects of Closed Circuit Television: A Systematic Review*, Home Office Research Study, no. 252, London: HMSO.

Welsh, B. P. and Farrington, D. C. (2003) 'Effects of Closed-Circuit Television on Crime', *The ANNALS of the American Academy of Political Social Science*, 587:110-135.

Welsh, B. P. and Farrington, D. C. (2008) 'Effects of closed circuit television on crime', [Online]. Lowell: Campbell Collaboration. Available at: http://db.c2admin.org/doc-pdf/Welsh_CCTV_review.pdf [Accessed 9th June 2009]

Whitfield, D. (1997) *Tackling the tag: the electronic monitoring of offenders.* Winchester: Waterside Press.

Wickens, J. (2006) 'The ethics of biometrics: The risk of social exclusion from the widespread use of electronic identification', *Science and Engineering Ethics,* 13 (1): 45-54.

Williams, D. (2008) 'Effective CCTV and the challenge of constructing legitimate suspicion using remote visual images', *Journal of Investigative Psychology and offender Profiling,* 4 (2): 97-107.

Williams, K. and Johnstone, C. (2000) 'The politics of the selective Gaze: closed circuit television and the policing of public space, *Crime, Law and Social Change, 24: 183-210.*

Wilson, D. (2005) 'Behind the cameras: Monitoring and open street CCTV surveillance in Australia, *Security Journal*, 18 (1): 41-54.

Wilson, D. (2007) 'Australian biometrics and global surveillance', *International Criminal Justice Review,* 17: 207-219.

Yar, M. (2003) 'Panoptic power and the pathologisation of vision: Critical reflection on the foucauldian thesis, Surveillance and Society, [Online]. 1 (3): 254-271. Available at: http://www.surveillance-and-society.org/journalv1i3.htm [Accessed 6 June 2009].

Zender, L. (2003) 'Too Much Security?', *International Journal of the Sociology of Law,* 31 (3): 155-184.