

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/232844116>

Securing the Neurocity

Article in *Criminal Justice Matters* · March 2008

DOI: 10.1080/09627250708553286

CITATIONS

2

READS

606

1 author:



David Murakami Wood

Queen's University

45 PUBLICATIONS 596 CITATIONS

SEE PROFILE

Some of the authors of this publication are also working on these related projects:



Big Data Surveillance [View project](#)



cjm

Criminal Justice Matters

No. 68 Summer 2007

Price £8.00

Security and Surveillance

contents

cjm no. 68 Summer 2007

EDITORIAL – SECURITY AND SURVEILLANCE Kevin Stenson puts this issue in context.	3	RISKY OR AT RISK? YOUNG PEOPLE, SURVEILLANCE AND SECURITY Surveillance strategies need to focus more on young people as victims rather than potential criminals write Denise Martin, Caroline Chatwin and David Porteous.	27
HOW DID WE GET HERE? David Lyon examines the background to our surveillance society and calls for vigilance to keep it under control.	4	BALANCE, SCRUTINY AND IDENTITY CARDS IN THE UK Cheryl A Edwardes, Ian Hosein and Edgar A Whitley contend that the government's argument that ID cards are for the 'greater good' needs to be scrutinised and balanced against the needs of the individual.	29
SECURITY, SURVEILLANCE AND COUNTER-LAW Richard Ericson reviews the changing face of the law relating to security and surveillance.	6	OPEN-STREET CCTV CANADIAN STYLE Randy Lippert describes how Canada is moving towards increased CCTV presence.	31
POLICING OPERATION ORE Caroline Metcalf examines the difficulties British police face in tackling child sexual abuse through the internet.	8	THE ARCHITECTURE OF SURVEILLANCE Richard Jones writes about the politics and design of surveillance systems and compares the views of leading theorists.	33
TRACKING OFFENDERS BY SATELLITE – PROGRESS OR COST-CUTTING? Mike Nellis is concerned about the effect of satellite technology on the supervision of offenders.	10	ELECTRONIC MONITORING, COMMERCIAL SURVEILLANCE AND THE 'MALFUNCTIONING SUBJECT' Craig Paterson looks at the implications of electronic monitoring for modern society.	35
MUSLIM COMMUNITIES UNDER SURVEILLANCE Basia Spalek and Bob Lambert argue that anti-terrorism policies and increased police activity have alienated Muslims and failed to improve national security.	12	SECURING THE NEUROCIITY David Murakami Wood warns that cities could be transformed beyond recognition by hi-tec surveillance if protocols are not put in place.	37
US AND THEM – THE SOCIAL IMPACT OF 'NEW SURVEILLANCE' TECHNOLOGIES Michael McCahill argues that new surveillance technologies are reinforcing and worsening social inequalities.	14	STOLEN IDENTITIES Jennifer Whitson and Kevin D Haggerty argue that companies' zest for customer data and the huge growth in e-commerce is exacerbating the problem of identity theft.	39
ASK THE CHILDREN Zoë Hilton and Chris Mills summarise their research on what young people think about the government's information sharing proposals.	16	DILEMMAS OF PRIVACY AND SURVEILLANCE: CHALLENGES OF TECHNOLOGICAL CHANGE Nigel Gilbert looks at future advances in electronic data collection and surveillance and urges engineers and government to work together to maintain the public's trust.	41
ENHANCED SUPERVISION OR SURVEILLANCE? THE USE OF CCTV IN APPROVED PREMISES Bernie Heath is concerned about the wholesale introduction of CCTV in probation hostels and the implications for high-risk offenders.	18	CJM UPDATE Enver Solomon writes on recent developments in criminal justice.	43
POLICING PRIVATE SPACE – A THREE DIMENSIONAL ANALYSIS Mark Button looks at security officers and their contribution to policing and surveillance.	20	NOTES FOR CONTRIBUTORS	47
TAKING SURVEILLANCE OUT OF THE ISSP Tony Goodman hopes that the Brown administration will take a more welfare approach to working with young offenders.	22		
'DRAWING THE LINE' AND 'APPLYING THE BRAKES': AN INTERVIEW WITH RICHARD THOMAS, THE UK'S INFORMATION COMMISSIONER Enver Solomon and Kevin Stenson ask Richard Thomas how he sees the future of surveillance and information collection.	24		

Cover photo: © ID8 Photos.

COPYRIGHT

We know that CJM is popular, and widely used in educational and training contexts. We are pleased you like the magazine. However we are concerned about an apparent proliferation of photocopying. You may be breaking the law.

The Copyright Licensing Agency permits the copying of ONE article per issue of a journal or magazine, under its current licensing arrangement. As a rule, no more than NINE copies may be made. The CLA is being increasingly strict about infringements of its scheme. And you need to have a license. If you find CJM valuable, and want to share it with your students, trainees or colleagues, why not order in bulk? Discount of 50p per copy for 10-50 copies. Discount of £1 per copy for 50+ copies.

editorial

security and surveillance

Kevin Stenson puts this issue in context.

Market-driven liberal democracies face threats to their security and also media and politically-stoked crises of anxiety and fear. These factors create opportunities for the security industry and the rapidly advancing surveillance technologies it markets to citizens, commercial firms and public bodies, to flourish.

This issue assembles a distinguished international cast of theorists and researchers of security and surveillance. Key dilemmas include debates about the trade off between allaying fears with greater security, and not sacrificing the liberties which distinguish our societies from authoritarian ones that rule through torture, intimidation, fear, the control of information and the suppression of dissent. Furthermore, increased security can amplify our risks. For example, as Whitson and Haggerty argue, fear of identity fraud and other internet crime occasions greater extensions of surveillance, profiling and data banks that, ironically, increase our vulnerability to predators. And the internet creates new temptations, for example, to download child pornography, to which many thousands succumb, straining the capacity of the police and justice agencies to manage the shoals caught in the surveillance nets (Metcalf).

Montesquieu, Adams, Locke and other Enlightenment architects of liberal democracy devised laws and constitutional measures to provide checks and balances to concentrated power, traditionally understood in terms of the (separate powers) of the executive, legislative and judicial branches of authority. A new industry of interpretation has emerged to make sense of and balance new technological powers and their design, inconceivable to eighteenth century Enlightenment thinkers (Lyon, Jones).

New satellite tracking makes possible 24/7 incessant monitoring, the elimination of hiding places and the dissolution of the boundaries between public and private spaces (Nellis,

Paterson). Yet, it is heartening, as Gilbert shows, that engineers are struggling to escape their comfort zone of technical problem-solving language to confront the ethical use of their technologies. However, Edwardes et al. remind us that politicians now justify the introduction of intrusive technologies like ID cards in the name of the 'common good', using a communitarian emphasis on the needs of the many rather than the liberal emphasis on individual and minority rights. Spalek and McCahill show how this can have a troubling and polarising impact on Muslim minorities and the 'usual suspects', the poor, homeless, mentally ill, addicted, and illegal immigrants. But, it remains unclear who monitors how our leaders define the common good. Who guards the guards?

We await a Montesquieu for the surveillance age, but we do have the recent 'Report on the Surveillance Society' from the UK Information Commissioner, Richard Thomas, which has achieved greater global impact than any other document in presenting the core issues to opinion leaders and the public. In our interview with the Commissioner, without endorsing gloomy dystopian visions, he eloquently argues for the need for public awareness, vigilance and applying the brakes to the rapid advance and application of surveillance technologies by public and commercial institutions. It is appropriate that this document comes from the UK. Just as Northern Ireland during the Troubles provided an experimental chamber for new security technologies and systems later used on mainland Britain, so the UK now provides such a benchmark for the globe; as Lippert shows this even inspires liberal Canada. Our citizens are the most watched in the world. We have about 4.2 million CCTV cameras and it is estimated that urban citizens are caught on camera around 300 times a day. This reaches its peak in the City of London, the richest spot on earth (Wood), surrounded by a 'ring of steel' following a devastating IRA bomb, and pioneering

automatic car number plate recognition and other sophisticated technologies.

9/11 and the 7/7 tube bombings have accelerated long-term trends in legislation and technology roll out. Against opposition from sections of the judiciary and civil liberties lobbies, the UK has echoed the US Patriot Act in constructing this armoury, for example with the Terrorism Act 2000, the Anti-Terrorism, Crime and Security Act 2001, the Prevention of Terrorism Act 2005 and the Terrorism Act 2006. This builds upon the provisions against anti-social behaviour in the Crime and Disorder Act 1998 and later legislation introducing Anti-Social Behaviour Orders, acceptable behaviour contracts, curfews, dispersal orders, long-term detention without charge or trial and other constraining measures. These tend to dissolve the boundaries between criminal and civil law, the maintenance of order in peace time and the waging of war. Ericson sees this international trend, linked with the new surveillance technologies, as the development of 'counter law', eroding the foundations of liberal conceptions of justice and due process.

For academics, police and criminal justice professionals, this adds to our agendas of work and keeps us in business. As yet, we know little about the long-term impact of CCTV and other surveillance technologies on behaviour and the attitude of citizens (Goodman). Research with young people, the target of much surveillance, indicates a deep ambivalence about welcoming the possibility of greater protection but fear of being labelled categorically as deviant (Martin et al., Hilton and Mills). For example, the pervasive use of CCTV in probation hostels may quieten residents but how far does it displace troublesome conduct to other spaces (Heath)? And the use of surveillance technologies can create a taken for granted conformity within industrial complexes and retail parks (Button), but how far does this expand a population of dangerous and unwanted 'others' excluded from such places and the bosom of 'respectable' society?

Kevin Stenson is Co-Director, Crime and Conflict Research Centre, Middlesex University, London.

How did we get here?

David Lyon examines the background to our surveillance society and calls for vigilance to keep it under control.

‘Surveillance society’ is making headlines and provoking official inquiries, especially in the UK. Although this attention is welcome, it comes rather late in the day. However, it is still worth reminding ourselves of some of its vital features.

‘Surveillance society’ describes an angle of vision, a way of seeing our contemporary world. It includes not only the Radio-frequency Identification (RFID) scanners in passports or the CCTV cameras in the street but also the pervasive surveillance systems that are the infrastructure of daily life. Garnering and processing personal data is both an industry – the ‘personal information economy’ – and a means of governance.

‘Surveillance society’ has a place in the social science lexicon and, alongside other concepts, plays a significant role in highlighting some key dimensions of current social formations and transformations. Importantly, it is a useful bridging concept, between academic social science use and more popular understandings of the social world (Surveillance Studies Network 2006).

A working definition of surveillance is ‘the purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection’ (Lyon 2007). The personal details may be of many kinds, including CCTV images, biometrics such as fingerprints or iris scans, communication records or the actual content of calls, or most commonly, numerical or categorical data.

This last type, created in bureaucratic organisations and referring to transactions, exchanges, statuses, accounts and so on, is ‘dataveillance’ (Clarke 2006). Dataveillance monitors or checks people’s activities or communications in automated ways, using information technologies. It is far cheaper than direct or specific electronic surveillance and thus offers benefits that may sometimes act as incentives to extend the system even though the data are not strictly required for the original purpose.

Origins

In the early 1970s James B. Rules suggested that new technologies were rapidly augmenting the surveillance capacities of large organizations, and used a model of a ‘total surveillance society’ to gauge how close any given society might be to that reality (1973: 37). Significantly, he showed that surveillance was as visible in the commercial world of credit cards as in departments of state, such as driver licensing. This insight took a long time to catch on, although Gandy’s work on database

marketing in the 1990s did much to highlight it.

‘Surveillance society’ was first used as a term in its simple form in 1985 by Gary T. Marx, who described it as an increasingly ‘Orwellian’ situation in which ‘with computer technology, one of the final barriers to total social control is crumbling’ (Marx 1985) and by Oscar Gandy, who looked with concern at the growth of ‘bureaucratic social control’ facilitated by information technology. In the same year, Canadian David Flaherty published his work on threats to privacy – largely because of the rise of computing technologies – in several ‘surveillance societies’.

Confusion often exists about surveillance because of the original focus on specific individuals because of some suspected infraction of law or rule. What historically was the case has now been generalised using new technologies. Dataveillance and the use of searchable databases means that anyone may be ‘suspect’ by virtue of their appearance in some category that is marked for attention. Having ‘nothing to hide’ is no longer grounds for complacency.

Well before 9/11 I wrote that ‘surveillance society denotes a situation in which disembodied surveillance has become societally pervasive’ (2001: 33). Surveillance has spilled over mere government bureaucracies to flood all social conduits. State surveillance was still significant, I noted, especially against terrorism such as the ‘Ring of Steel’ in London or against Aum Shinrikyo in Tokyo. But, I went on, insurance logics, risk management and now simulation and precaution drive surveillance into all areas of social life.

The rise of information technology systems enabled all kinds of organisations to utilise essentially similar means of seeking efficiency, productivity and convenience, many of which involve personal data. As this occurred, surveillance started to permeate the routines of everyday life in all social sectors and layers and invited analysis of how governance works in each of them. Our Surveillance Project at Queen’s University in Canada is one unit that tries to explore contemporary surveillance, and the journal *Surveillance and Society* (www.surveillance-and-society.org) is another.

Sociologies of surveillance society

To emphasise recent technological changes, however, is to risk forgetting that surveillance seems to be a feature of all societies at all times. However, the ‘rational’ methods of modernity transformed organisational practice, eroding informal social networks and controls on which everyday business

and governing previously relied. Ordinary social ties were downplayed so that family connections and personal identities would not interfere with their smooth running. By this means citizens and eventually workers could expect that their rights would be respected because they were protected by accurate records as well as by law.

Impersonal and rule-centred practices spawned surveillance. Business practices of double entry book-keeping and of trying to cut costs and increase profit accelerated and reinforced such surveillance, which had an impact on working life and consumption. And the growth of military and police departments in the twentieth century, bolstered by rapidly developing new technologies, improved intelligence-gathering, identification and tracking techniques. Surveillance grows as a part of just being modern.

Today, information infrastructures facilitate surveillance and degrees of integration in many spheres (even though actual joined-up services and even state-commercial integration face technical and legal obstacles). At any rate, forms of 'social orchestration' and 'disorganised surveillance' are visible today, rather than fully co-ordinated surveillance.

Understanding surveillance society as a product of modernity helps us avoid two key traps: thinking of surveillance as a malign plot hatched by evil powers and thinking that surveillance is solely the product of new technologies (and of course the most paranoid see those two as one). But getting surveillance into proper perspective as the outcome of bureaucratic organisational practices and the desire for efficiency, speed, control and co-ordination does not mean that all is well. Rather, that we have to be careful identifying the key issues and vigilant in calling attention to them.

Surveillance is two-sided, and the benefits of correct identification, screening, checking, appropriate classification and other tasks associated with it must be acknowledged. Yet at the same time risks and dangers are always present in large-scale systems and of course power does corrupt, or at least skews the vision of those who wield it.

Surveillance society after 9/11

In the post-9/11 world of Europe and North America, certain surveillance trends have become dominant and these require redoubled efforts of analysis and political understanding. The safety state (Raab 2005) now has security as one of its highest priorities and this puts pressure on surveillance society. The 'safety state' prioritises risk management and permits 'states of emergency'.

Cultures of fear, suspicion and secrecy are all prominently implicated in surveillance processes since 9/11 (Lyon 2003). Many corporations, encouraged by governments, capitalised on the opportunities. What Bigo and others call 'illiberal practices of liberal regimes' (Bigo *et al* 2007) include the growth of suspicion fostered by surveillance.

Climates of fear seem to paralyse conventional checks and balances. Not knowing where or who the elusive 'enemy' is has encouraged the quest for tools to seek out any sharing characteristics associated with violence; race, nationality, gender, religion, profession.

Rather than choosing limited and focused means of seeking suspects, tighter nets are thrown wide, using diverse databases, data-mining (for example on visitors to the USA) and de facto national registries. Such tactics are used in the EU as well, albeit in the face of greater opposition. The co-ordination of intelligence services with policing and the transnational exchange of personal data is evidence of such 'illiberality' and the spread of suspicion (Guittet 2006). Any 'exceptional circumstances,' especially when the exceptions seem permanent as in an endless 'war on terror,' are ones that require special vigilance from those who care about human and civil rights.

Not only is there increasing transnational personal data exchange, different kinds of data have come to be seen as desirable and useful in the 'war on terror.' This includes, prominently, consumer data, such that a curious assemblage of information takes shape. Moreover, these data are used in an anticipatory way, to try to pre-empt violence or disorder, rather than in the more classical sense of 'preventative' policing where detailed and specific existing intelligence is used.

The 'surveillance society' is a feature of today's world. It is ambiguous and complex, but today's context of 'states of exception' seen particularly in the 'war on terror', and of rampant commercial promotion of new surveillance technologies, invites serious social, political and ethical analysis. New technologies involve remote and automated systems, increasingly calibrated to exclude. Fear and suspicion are reinforced. Imagination and courage are urgently needed to develop alternatives that promote trust, inclusion, recognition and respect.

David Lyon is Professor of Sociology at Queen's University, Kingston, Ontario.

References

- Bigo, D., Carrera S., Guild E. and Walker R. (2007) 'Changing Landscapes of European Liberty and Security' available at www.libertysecurity.org/article1357.html
- Lyon, D. (2007) *Surveillance Studies: An Overview*, Cambridge: Polity Press.
- Lyon, D. (2001) *Surveillance Society: Monitoring Everyday Life*, Buckingham: Open University Press.
- Rules, J. B. (1973) *Private Lives and Public Surveillance*, London: Allen Lane.
- Surveillance Studies Network (2006) *The Surveillance Society*, London: Information Commissioner's Office.
- Webb, M. (2007) *Illusions of Security: Global Surveillance and Democracy in a post-9/11 World*, San Francisco: City Lights.

Security, surveillance and counter-law

Richard Ericson reviews the changing face of the law relating to security and surveillance.

We live in insecure times, with problems with national security (threats of terrorism), domestic security (anti-social behavior), social security (benefit system fraud), and corporate security (liabilities for harm) at the top of the political agenda. Enormous expenditures on risk assessment and management ironically reveal the limits of risk-based reasoning and intensify insecurity. Images of catastrophe are fuelled, precautionary behaviour is pervasive, and extreme security measures are institutionalised in the form of ‘counter-law.’

The notion of counter-law includes both ‘law against law’ and surveillance. New laws are enacted, and new uses of existing law are invented, to erode or eliminate traditional principles, standards and procedures of criminal justice. New surveillance infrastructures are developed, and new uses of existing surveillance networks are extended, to also erode or eliminate traditional principles, standards, and procedures of criminal justice. The two forms of counter-law treat everyone as if they are guilty of criminal intent. They criminalise not only those who actually cause harm, but also those merely suspected of being harmful, as well as authorities deemed responsible for security failures.

An obvious example of counter-law is anti-terrorism measures. For example, the USA Patriot Act places no limit on presidential authority to criminalise ‘unlawful enemy combatants,’ including US citizens. Criminalisation can occur on the basis of categorical suspicion: the wrong face in the wrong place at the wrong time. There is also suspicion by association: someone is suspected because they know someone suspected. Those arrested can be detained without specific charges for an indefinite period, and subject to state-sanctioned torture. *Actus reus*, the principle that criminalisation must be based on a specified criminal act, is eliminated. There is not even a pretense of what might be termed *probabilis reus*: criminalisation based on actuarial knowledge of risk. There is only the counter-law principle of *finis reus*: when criminalisation appears necessary for security, no other justification is called for and legal principles are preempted, finished.

The USA Patriot Act also enables unprecedented powers of surveillance. Based on the premise that malicious demons may be sleeping anywhere, law enforcers are given far-reaching access to private spaces and communication networks. The old model of resourceful police intelligence is replaced with one of universal suspicion that spells the end of innocence. The strategy is to cast the net as widely as possible, identify suitable enemies, not worry about

false positive identifications, drop any pretense of due process of law, and accomplish summary justice.

Counter-law was normalised in other fields of security well before 9/11. A prime example in the field of domestic security is measures to combat anti-social behavior in England and Wales. The legal definition of anti-social behavior is left purposefully vague, providing scope for whatever may be defined locally by neighbours or other undesirables as terrorism. The only statutory definition is in section one of the Crime and Disorder Act 1998: conduct ‘causing or likely to cause harassment, alarm or distress’. The culprit is subject to an anti-social behavior order (ASBO) made in civil proceedings. This order not only obligates him or her to desist from the harmful activity, but also requires submission to surveillance-based regimes that restrict time, place, and association (curfew and ban orders), involve disciplinary programs of behavioral change (counseling and courses), and compel compensation (community service and restitution). Breach of the civil order can result in strict liability criminal proceedings and imprisonment. Sentencing for breach can take into account previous behavior that may be known through surveillance and hearsay but not proven in court, undermining fairness standards that punishment should be proportionate to proven offences and not be retrospective.

ASBO legislation was passed in the same year as the first human rights legislation in England and Wales. Some ASBO provisions were explicitly constructed to limit the scope and application of the rights stipulated in the Human Rights Act and its cousin, the European Convention on Human Rights. Again, counter-law appears as a response to the law itself, as a source of uncertainty. When law sustains high standards of due process, evidence, proof, and culpability, it creates a great deal of uncertainty in the capacity of the criminal justice system to prevent, discover, build a case against, and successfully prosecute criminal behavior. In the demand for greater certainty, the standards of criminal law are undercut, the lower standards of civil and regulatory law ascend, and the urge to broaden and deepen surveillance intensifies.

Counter-law is also evident in the field of social security. In my home province of Ontario, Canada, the Ontario Works Act of 1997 shifted social benefits from a welfare needs-based system to one of temporary assistance to the unemployed person actively committed to seeking work. This legislation requires the claimant to enter into a ‘participation agreement’ similar to the contract-

based governance of ASBOs. They must consent to surveillance of personal circumstances, grant access to personal records in various institutions, and accept random home checks and substance abuse screening. The agreement also includes employment-related activities such as job searches, skills training, and acceptance and maintenance of employment. The implementation of this regime was accompanied by deep cuts to benefits. Taking inflation into account, there was a 34 per cent decline in the purchasing power of benefits between 1995 and 2002. In 2003, a single person received benefits at 65 per cent below the poverty line, a single person with a child was at 44 per cent below.

At the same time there was a shift from seeing welfare fraud as a minor but inevitable aspect of the benefits system, to treating all welfare as a kind of fraud against the commonwealth and therefore in need of stringent control. The crackdown included additional legislation in 2000 that made a claimant convicted of benefits fraud permanently ineligible for future benefits, giving in effect a life sentence of poverty without parole. The surveillance 'package' was elaborated to scrutinise the minutiae of the claimant's life. Unreported cohabitation, gifts, casual work paid in cash, or too many visits to the food bank might constitute fraud. Eligibility review officers operate with full search powers, including warrants, and an obstruction of investigation provision whereby anyone – the claimant's family, friends, neighbours, landlord, employer, or teachers – giving false information or otherwise interfering with an investigation – is subject to criminal sanction. Data matching systems across institutions red flag suspects for further investigation. A 'snitch line' was established which, in the 2001/02 reporting year, led to 6,527 investigations of claimants.

Government data for 2001/02 indicate that two-thirds of 35,452 fraud investigations were unfounded, and that where there was a problem the typical solution was summary administrative justice through reduction or termination of benefits. This data suggests that in most cases, 'governing through fraud' functions primarily as a means of obtaining acquiescence to surveillance and claims suppression. At the same time it is not surprising that some 'fraud' – in the form of unreported cohabitation, gifts, and informal economy income – is easy to uncover when claimants are kept so far south of the poverty line that they cannot survive without such activities.

No one escapes counter-law, including corporate 'actors' far north of the poverty line. Corporate activities with potential for catastrophic loss are at the forefront of the politics of security, surveillance, and counter-law. Controversies rage over the security of food supplies, medical services, nuclear, biological and chemical production, financial institutions, and environments. The response is counter-laws that criminalise corporate officials deemed responsible for catastrophe, even if they had no control over, or knowledge about, practices that led to the catastrophe, and even if these practices were widely

regarded in corporate culture as acceptable before the catastrophe. A rotten apple view of rogue employees is extended to the corporate entity as a rotting barrel. Corporations are depicted as aggrandising monsters seeking only profits and leaving destruction in their wake. This anthropomorphisation of the corporation as pathological constructs a view of it as criminal. This view is radically different from the one that has traditionally granted the corporation enormous rights and privileges. Various forms of group liability, for example regarding conspiracy and incitement, are constructed. There are also efforts to make corporate manslaughter a statutory offence, as has occurred in the UK with the Corporate Manslaughter and Corporate Homicide Bill.

These manifestations of counter-law are nascent and largely symbolic, feeding into the rituals of visible precaution that characterise the politics of security, surveillance and counter-law. The real counter-law revolution is taking place at the level of surveillance-based internal controls of corporate conduct. These controls are enabled through legislation such as the Sarbanes-Oxley Act that followed Enron and other corporate scandals in the USA. New surveillance technologies, inspections, audits, and private policing expand after each catastrophic loss. Organizing organisations – state regulatory bodies, professional associations, industry associations, insurance bodies, and internal control units – proliferate as part of the frenzy to risk manage everything through corporate surveillance and criminalise those deemed responsible for security failures. Through these new mechanisms of surveillance, the corporate world has become more visible and subject to regulation than ever before. However, the resulting emphasis on risk aversion, defensive compliance, and reputation management fosters a corporate culture of deep suspicion. Employees feel criminalised because their everyday environment of security, surveillance and counter-law treats them as if they are operating with criminal intent.

Ironically, when law and other democratic institutions are most threatened by seemingly intractable problems, the response is to devise new forms of counter-law that further threaten those institutions. Law is transformed into an institution of suspicion, discriminatory practices, invasion of privacy, denial of rights, and exclusion. To borrow the legal definition of anti-social behavior, law itself becomes a source of 'harassment, alarm and distress.' Security trumps justice, and insecurity proves itself.

Richard Ericson is Professor and Director, Centre of Criminology, University of Toronto.

References

- Ericson, R.V. (2007) *Crime in an Insecure World*. Cambridge: Polity.
- Haggerty, K.D. and Ericson, R.V. eds. (2006) *The New Politics of Surveillance and Visibility*. Toronto: University of Toronto Press.

Policing Operation Ore

Caroline Metcalf examines the difficulties British police face in tackling child sexual abuse through the internet.

The growth of the internet in recent years is at the heart of current anxieties about child sexual abuse images, internet chat rooms, and the lack of suitable protection for children using this new-found technology (Kennison and Read, 2003). Concerns about these issues focus broadly on how to police the internet (*ibid.*) because unlike traditional methods of policing, there is no scene of crime and the methods of investigation are not conducted entirely within the parameters of the physical domain. It represents challenges to traditional methods of policing which 'collapse the notions of time, space and geography' (Wall, 1997). Interest in this phenomenon has expanded, not only with the public and the media but also within the political agenda.

In April 2001, the National High Tech Crime Unit (NHTCU) was introduced as part of a multi-agency organisation to offer resources to local and regional forces to carry out investigations relating to 'cybercrime' (Jewkes, 2003). This includes hacking, virus writing, drugs trafficking and child abuse (*ibid.*). In July 2002 the US Postal Inspection Service discovered a website providing adult pornography as well as child abuse images. The website was called 'Landslide Productions', and following its detection the matter was handed to the Federal Bureau of Investigation (FBI). The FBI passed on intelligence to the National Criminal Intelligence Service (NCIS) relating to some 7,272 British individuals suspected of downloading images of child abuse on the internet. This was to become known as Operation Ore – the largest ever national investigation. Since Operation Ore the HTCUC's operations have been stifled.

According to an internet source, under Operation Ore the UK police carried out 4,283 searches, made 3,744 arrests, (Warren 2005) and 35 suspects/offenders had committed suicide. And in 2005, there were 800 investigations pending (Warren 2005). It is well documented that the police are limited in resources and, since Operation Ore British forces are being launched into a technological field where computer expertise is becoming a necessity for effective investigation. This clearly presents a problem for the police given that those downloading abusive images of children are often highly computer-literate.

During the initial stages of Operation Ore, there were more than 750,000 British suspects. This figure alone illustrates the enormity of such an investigation. According to my research findings (Metcalf 2006), the enormity of the task relates not only to the vast number of suspects but also to issues regarding the sheer range of evidence seized. It does

not involve simply examining the hard drives of the suspects' computers. It also includes a phenomenal number of floppy discs, zip files, CD ROMs, palm top computers, laptop computers, printers, scanners, cameras, game consoles, fax machines, telephones, pagers, answerphones, DVDs, tapes, solid state cards, thumb drives, not to mention the endless hours of examining every VHS tape the suspect owns (personal communication 2003). This only accounts for the multi-media type evidence; there are also credit card bills, bank statements, diaries and personal organisers, which may link to the purchasing of child abuse images.

Staff at the computer units tend to be police officers that are untrained in the area of computer crime, and so money must be spent on upgrading their knowledge and skills (author's unpublished PhD thesis 2006). The HTCUC also deal with crimes of fraud, blackmail and extortion, hacking and virus attacks, software piracy and Class A drug trafficking. There is other computer related crime that needs to be investigated at the HTCUC, and if something more urgent arises, then it is quite likely that Operation Ore would no longer be their highest priority. Indeed, the success of policing investigations like Operation Ore can depend on the priorities of any given force. For example, if such investigations are not part of a policing plan then it might be that they are low on the list. Certain forces might prioritise burglary, car crime, robbery, and drugs, as part of their policing plan and this will remain their focus. Furthermore, the enormity and ambiguity of Operation Ore left some forces not knowing 'where on earth to start'.

Another issue relates to the tracing of suspects. The Federal Bureau of Investigation (FBI) provided the National Criminal Intelligence Service (NCIS) with the credit card details of British suspects. NCIS gathered intelligence on each suspect and passed the data on to the relevant forces across England and Wales. However, security and surveillance surrounding the internet was not as reliable as it seemed; the information could be somewhat broad and required time-consuming work to establish its accuracy in order to pursue the investigation. At first glance it appears that every person who used their credit card to obtain images of child abuse via the Landslide website got 'caught in the loop'. However, it soon became apparent that despite the so-called financial and security procedures of Landslide Productions, it was not quite as strict as it initially appeared. Because of this generic information, the investigation became a lengthy process for British forces and that was before the operation even got started.

Perhaps the most pressing issue around policing Operation Ore was the problem of resources. The National Steering Group acquired £500,000 from the Home Office to support police forces dealing with Operation Ore. The money, managed by the National Crime Squad, was able to provide training, hardware and software equipment for at least one and up to five police officers in every force across the country (personal communication 2003). The issue of resources is both human and non-human. Indeed, human resources should increase along with financial resources although arguably, viewing such material is an unattractive job. One British police officer emphasised the need for manpower, stating 'you only have manpower if you've got money to buy it. You can't go out and say, we'll take out some temporary staff to come in and do it. The staff are what we've got and if you want more man hours under that number of staff then you've got to pay them to work the man hours so it all comes down to money' (personal communication 2003).

The resourcing of manpower is stretched between the sheer enormity of the task, and the willingness of officers to be involved in such work. 'Cop culture' could be the underlying reason for the unwillingness, given it is not seen as 'real police work'. Jewkes (2003) points out that most UK police forces are still paper-based organisations and refers to a Detective Superintendent at West Yorkshire police who complained that most of his colleagues do not feel computer-based investigation is 'normal' work, and that their ability to respond to internet crime is 'haphazard and based on luck rather than a prepared and researched provision of a service to the public' (Hyde, 1999:7 cited in Jewkes 2003:17). Compounding this is many officers' lack of computer and technical knowledge. Officers that were interviewed were aware that there was a recognition at a national level of the need for police training in computer crime (unpublished PhD thesis).

There is clearly a range of difficulties involved in the policing process of investigations like Operation Ore. As this article has demonstrated, forces might not be effective if such offences are not prioritised. Furthermore, the problem of resources is an ever-present feature in policing, particularly in an investigation that involves tens of dozens of suspects in each force area. This has a significant impact on policing internet sex offenders since it is not only manpower that is required but *specialised* manpower. In other words, Operation Ore and similar investigations require firstly, an officer or civilian willing to work within the HTCUC, and secondly, they must be 'technologically trained', which of course requires time and money. It is a case of 'time will tell' about how future similar investigations are managed. Ever-changing social conditions require the police to become more specialised and professionalised through the development of specialist units dealing with specific crimes.

Caroline Metcalf PhD, is Programme Specific Facilitator for a Community Sex Offender Groupwork Programme.

References

Hyde, S. (1999) 'A few coppers change', in *Journal of Information, Law and Technology*. Available Online at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/1999_2/hyde/

Jewkes, Y. (2003) 'Policing the Net: crime, regulation and surveillance in cyberspace', in Jewkes, Y. ed. (2003) *Dot Cons:*

Crime Deviance and Identity on the Internet. Cullompton: Willan Publishing.

Kennison, P. and Read, M. (2003) 'Policing the Internet, part one; The Internet and child protection' in *Community Safety Journal* 2(2), University of Middlesex: Pavillion.

Metcalf, C. M. (2006) *Making Sense of Sex Offenders and the Internet*. Unpublished PhD Thesis: Brunel University.

Wall, D. S. (1997) 'Policing the virtual community: The Internet, cybercrimes and the policing of cyberspace', in Francis, P., Davies, P. and Jupp, V. (1997) *Policing Futures*. London: MacMillan.

Warren, P. (2005) 'UK police tackle mounting internet porn caseload', in *The Register*. Available Online at http://www.theregister.com/2005/04/22/uk_police_internet/print.html.

Tracking offenders by satellite – progress or cost-cutting?

Mike Nellis is concerned about the effect of satellite technology on the supervision of offenders.

The satellite tracking of offenders using GPS and GSM mobile phone technology began in the USA in 1997. By 2004 – when the 17-month English pilots began – it had been used in 32 states. It has been piloted (briefly) in Bavaria and also in New Zealand, France and the Netherlands (see Elzinga and Nijboer 2006). Nova Scotia has been experimenting with it since spring 2006, and in September 2007 a pilot will start in Manitoba, Canada. It is probably too early to say what the future holds in regard to satellite tracking, but some insight into its significance and possible trajectory, might be gained from looking at the new fields of ‘surveillance studies’ and ‘mobility studies’.

The surveillance of mobility – of people, artefacts and information – has become an established area of sociological enquiry, with a wide-ranging focus (Molz 2006). As yet, few theoretical insights from mobility studies have been assimilated into criminology, possibly because there has been only limited criminological interest in offenders ‘on the move’. The satellite tracking of offenders seems very novel to criminology, and even more so to many professionals involved in traditional forms of offender supervision such as probation or community service.

Satellite tracking exemplifies the surveillance of mobility, insofar as it involves the automated monitoring (and sometimes restriction) of convicted criminals’ routine and everyday movements in limited spatial settings – quite often poor neighbourhoods – and the transfer of digitised data, including digitised maps, between a range of criminal justice agencies. It cannot, however, be understood merely as an isolated and self-contained development in criminal justice; rather it bears out Bennett and Regan’s (2004:450) observation that ‘the spaces in which the surveillance of mobilities regularly occurs [has] expand[ed] beyond those that are arguably hubs of mobility, such as airports, and now extend[s] to any space in which people, objects or words move’ (emphasis added). It uses technical systems which have been created for military intelligence, transport control (vehicle, boat and plane tracking, and the as yet rare road tolling systems) and facilitates cellphone communication to track mobile individuals, as, in different ways, do CCTV systems and the audit trails left by digitised financial transactions.

‘With the surveillance of mobilities there is potentially no ‘hiding’. There is no room to walk anonymously down a street, drive through a neighbourhood, or talk on the phone. All these movements and flows are subject to scrutiny, captured, stored, manipulated and subsequently used for purportedly benevolent or underhandedly sinister purposes. The objects we use (cars, phones, computers, electricity) in turn become tools for surveillance. Movement is not a means of evading surveillance but has become the object of surveillance.’ (Bennett and Regan 2004:453).

These, of course, are the routine experiences of ordinary citizens, whose immersion in such systems demonstrates a

mixture of casual assent, begrudging acquiescence and active desire. Given the affordances of the technologies available, and the likely future direction of such technologies, it was arguably only a matter of time before specific and sophisticated forms of mobility monitoring were applied to those about whom there was probable cause for suspicion, fear or hostility. As Hannam, Scheller and Urry (2006:1) put it ‘fear of illicit mobilities and their attendant security risks increasingly determine the logics of governance and liability protection within both the public and private sectors’. Thus, while many citizens will choose *voluntary locatability* for their own convenience and security, some citizens will have *enforced locatability* imposed on them, using variants of the very same technologies.

The concept of tracking offenders by satellite crystallised within specific crime control discourses, developed by rising elites within an evolving ‘commercial-corrections complex’ (Lilly and Knepper 1993) – and was further aided by straightforwardly political and media discourses about the *failure and inadequacy* of existing humanistic forms of offender supervision in the community.

It is against the backdrop of an existing, multiple-use technological infrastructure that the emergence of satellite tracking must be understood. Mobile communication and geolocation technologies enable connectivity across space in ways that produce a sense of human proximity without the element of physical presence that would once have been required; they facilitate ‘new ways of organising the spatial scale and temporal rhythms of interaction’ (Scheller 2004:42). Within criminal justice, the spectrum of electronic monitoring (EM) technologies – house arrest/curfew tagging, voice verification and now satellite tracking – are just such means of connectivity, and are aptly thought of as ‘automated *socio*-technical systems’ (Lianos and Douglas 2000) because, despite being defined by their *technological* nature, a human element remains (at least for now).

It is said of ‘virtual communication’ that it sustains a sense of relationship, solidarity and community among spatially dispersed networks of people. But EM merely facilitates data gathering *about* someone rather than knowledge *of* someone, and it entails a dyadic link between a single (or split) authority (law enforcement agency/monitoring centre) and a subject, rather than multiple links within a network. One of the paradoxes of satellite tracking offenders – given the vast global reach of GPS – is that the degree of spatial separation between authority and subject may not be great: it is relatively local, parochial, behaviours which are being monitored and regulated. While the monitoring centre itself may be hundreds of miles away from the monitored subject, police and probation officers involved in the broader supervision programme are likely to be in the same neighbourhood.

Virtual communication technologies have created ‘economies of presence’ (Mitchell 1999) where the accomplishment of a

Do you know your offenders are compliant when they're away from home?

We check every 10 seconds!

iSECUREtrac GPS systems offer you the truth. You can hold your offenders accountable to the places they've been and the times they've been there, 24/7/365, anywhere in the world. Additionally, GPS tracking systems can greatly increase your level of offender supervision without adding to officer workload. iSECUREtrac alone can provide you with:

- ▶ Location and compliance verification every 10 seconds
- ▶ Fastest violation reporting on the market
- ▶ User-friendly, yet powerful, web-based software
- ▶ Proven GPS policies and best practices for agencies

For more information or to request an on-site demo, please call 866.537.0022 or visit www.isecuretrac.com

 **iSECUREtrac**
GPS OFFENDER MONITORING

particular social task can now be subject to routine cost-benefit analysis. The emergence of EM, which is often justified by its low cost relative to imprisonment, strikingly illustrates the way in which 'economies of presence' are migrating from the commercial field where they originated directly to the offender supervision field thereby transforming what is meant by 'supervision'. The periodic meeting up of supervisor and supervisee was once integral to the very meaning of supervision; it was via their structured personal encounters (and sometimes through the relationship which grew between them) that an impact on behaviour was effected. Remote monitoring technologies have enlarged the spatial range over which supervisory influence can be exerted – even house arrest/curfew and tagging added a surveillant means of gaining compliance with a court order or release licence as opposed to the incentive-based, trust-based and threat-based means of gaining compliance which have traditionally comprised the social work/law enforcement repertoire.

However, even more importantly, remote monitoring technologies have extended the *temporal range* of supervision within a given 24-hour period. In the past, the most intensive forms of personalised, humanistic supervision have rarely been more than intermittent, daytime encounters, while curfew tagging only added in an element of control over night-time activities. Both approaches leave offenders with significant periods of time when they are without the oversight of supervisors, when their whereabouts are *uncertain*. It is the temporality of satellite tracking that most distinguishes it from humanistic and relational forms of offender supervision, because it seemingly makes possible *incessant oversight* – round the clock knowledge of an offender's location, in real-time or (more

usually) some approximation to it – that no personal supervisor could manage and that no traditionally-oriented social work or law enforcement agency could afford. This quality of incessance has become, quite literally, a major 'selling point' of satellite tracking, dominating commercial advertisements for it (and indeed other monitoring technologies).

US company iSECUREtrac, for example, plays directly on probation officers' anxieties with the headline: 'Do you know your offenders are compliant when they're way from home? – We check every 10 seconds!' – followed by 'iSECUREtrac' GPS systems offer you the truth. You can hold your offenders accountable to the places they've been and the times they've been there, 24/7/365, anywhere in the world. Additionally GPS tracking systems can greatly increase your level of offender supervision without adding to officer workload. iSECUREtrac alone can provide you with location and compliance verification every 10 seconds, fastest violation reporting on the market, user-friendly, yet powerful, web-based software; proven GPS policies and best practice for agencies' (see illustration). (*Journal of Offender Monitoring*, 19(2), 2007)

Marketing a full case management package, Syscon dispels anxieties about offenders' nocturnal activities with a picture of a contentedly sleeping probation officer who rests easy because 'at work he is using Syscon's automated systems to manage his low risk caseload with a range of kiosk, voice recognition and GPS technologies handling report-ins, the collection of fines, fees and restitution, and secure monitoring - all wrapped up in a fully integrated system. Only Syscon can offer you the full service package from end to end.' (*Journal of Offender Monitoring*, 19(2), 2007).

Sadly, he doesn't know that his computer-printed redundancy notice is coming in the morning post.



Mike Nellis is Professor of Criminal and Community Justice at the Glasgow School of Social Work, University of Strathclyde.

References

- Bennett, C. J. and Regan, P. M. (2004). Editorial: Surveillance and mobilities. *Surveillance and Society* 1(4), 449-445.
- Elzinger, H. K. and Nijboer, J. A. (2006). Court orders, probation supervision through GPS. *European Journal of Criminal Law and Criminal Justice*, 366-388.
- Hannam, K., Sheller, M. and Urry, J. (2006). Editorial: Mobilities, immobilities and moorings. *Mobilities*, 1(1), 1-22.
- Lianos, M. and Douglas, M. (2000). Dangerisation and the end of deviance: The institutional environment. In Garland, D. and Sparks, R. (Eds.), *Criminology and Social Theory*. Oxford: Oxford University Press.
- Mitchell, W. J. (1999). *E-topia: Urban life, Jim, but not as we know it*. Cambridge: Mass.: Massachusetts Institute of technology.
- Molz, J. G. (2006). 'Watch us wander': Mobile surveillance and the surveillance of mobility. *Environment and Planning A*, 38(2), 377-393.

Muslim communities under surveillance

Basia Spalek and Bob Lambert argue that anti-terrorism policies and increased police activity have alienated Muslims and failed to improve national security.

The events of 11 September 2001, and more recently, the 7 July 2005 bombings and attempted bombings on 21 July 2005, have stimulated much research interest and policy attention towards Muslim minorities living in the UK, as well as in other liberal democratic societies. The national security measures that have been put in place since 2001 are underpinned by a new apprehension of the challenges posed by minority and immigrant populations as not only current or prospective citizens, but also as the potential targets of recruitment for terrorist groups. Ethnic minorities associated with Islam are therefore experiencing increased attention from the police and security services, invoking an 'othering' of the communities concerned.

In the aftermath of the 7 July 2005 bombings in London, with the dawning realisation that the terrorists were home-grown British citizens, much political and media attention has focused on potential pathways to radicalisation, and identifying possible web sites that may aid and abet the transmission of extremist Islamist viewpoints and violent action. The risks posed by marginalised Muslim youth, the extent to which Muslim communities are 'assimilated' within British society, whether Muslim converts, particularly those who convert to Islam inside prison, are at risk from 'radicalisation', and whether Islamic institutions and organisations are 'out of touch' with their young people, and whether this also creates the potential for 'radicalisation' are all the frequent focus of media and political discourse. In many ways, this exploration, and the anxiety which goes with it, mirrors the conditions of contemporary western society, characterised as late modern society. Late modern society is defined as a continuous probing of established beliefs and increasing reflexivity, where 'the deviant other is everywhere' and 'everyone is a potential deviant' (Young, 1999: 15).

In the UK, a series of anti-terror laws have been implemented, including the Terrorism Act 2000, the Anti-Terrorism, Crime and Security Act 2001, the Prevention of Terrorism 2005, and the Terrorism Act 2006. These new anti-terror laws have been criticised by civil liberties organisations as being draconian, making little, if any, impact on national security. These laws have also provoked outrage amongst Muslim communities, who feel that they are being unfairly targeted.

For instance, in Britain, figures for police stop and searches in 2002/03 under counter-terrorism legislation, revealed that the number of stops and searches of Asians had increased by 302 per cent in a year compared to a rise of 230 per cent for blacks and 118 per cent for whites. The Muslim Council of Britain claimed that '... the police are misusing their new powers ... We think that the institutional racism highlighted by the Macpherson Report is morphing into institutional prejudice against Muslims. We are worried a generation of young Muslim men is being criminalised' (Cowan, 2004: 8). Similarly, the Preventing Extremism Together Working Group on security/policing, assembled in the aftermath of the 7 July bombings, made up of Muslim community representatives, has raised concerns about the possible breadth of new powers being introduced by the Terrorism Act 2006:

'Inciting, justifying or glorifying terrorism as currently formulated could lead to a significant chill factor in the Muslim community in expressing legitimate support for self-determination struggles around the world and in using legitimate concepts and terminology because of fear of being misunderstood and implicated for terrorism by the authorities (Home Office: 2005a: 77).'

It might be argued that the implementation of anti-terror laws which could be used disproportionately against Muslims, with the potential for increased surveillance and control, stands at odds with another core component of counter-terror policing: the importance of the involvement of Muslim communities in helping to combat extremism, as highlighted in a series of government policy documents. For example, in the National Policing Plan 2005-08 (Home Office, 2005b) it is stated that the 'counter-terrorism strategy of Government is underpinned by strong intelligence processes within each force area and strong communities to build and increase trust and confidence within minority faith communities'. Muslims' responsibilities as active citizens are therefore being increasingly framed by anti-terror measures which encourage internal community surveillance so that the responsible Muslim citizen is expected to work with the authorities to help reduce the risk of terrorism. Moreover, Muslims who retain strong visible allegiances to Islam – in some cases giving them an outward and superficial resemblance to Osama

bin Laden – and strong adherence to the political grievances bin Laden skilfully exploits, become less congenial partners for government Ministers and counter-terrorism officials. To become a counter-terrorism partner it helps a Muslim community representative to become less critical of the global war on terror and more compliant to government policy.

In the event, such a narrow focus on the responsibilities of a faith community exposes further tensions within and between counter-terrorism and counter-radicalisation policy. Asking a faith community to share ownership of a terrorism problem is to overlook the extent to which the overwhelming majority of Muslims in the UK know very little about it. That is to say, the ideology that inspires and promulgates suicide bombing in the UK has been nurtured over a long period in a very small section of what are very heterogeneous and independent Muslim communities in the UK. It is not uncommon, for instance, within one London borough to find five or more mosques that represent different ethnic and religious groups with no history of interaction between them. Yet unwittingly, they share a common ignorance of violent extremism. As a result, the overwhelming majority of Muslims in the UK have no more knowledge of al-Qaeda-related terrorist ideology and how young people are attracted to it than the rest of the population.

Consequently, when government and police chiefs prevailed upon mainstream Muslim leaders to help tackle the problem in the immediate aftermath of 7/7 some responded by highlighting just how little they understood about what was happening. That was one important reason why they called for a public enquiry: they wanted to be given an authoritative and independent explanation for 7/7 before deciding what, if anything, they could do in response.

Ironically, those Muslim communities where there was an understanding of the problem, combined with real experience in tackling it, were the ones that bore the main brunt of a wide-ranging counter-terrorism policy. Indeed, their representatives had long complained to the authorities that insufficient was being done to counter the adverse influence of notable violent extremists in their midst. For at least seven years before 9/11 influential and active promoters of al-Qaeda terrorism had made it their business to subvert Muslim youth to their cause. Influential extremist figures such as Abu Qatada, Abu Hamza and Abdullah el Faisal infiltrated minority sections of the UK Muslim community that are best described as Salafi – Muslims who value a literal, textual approach to their religion in much the same way that many Protestant Christians do. From a mainstream UK Salafi perspective al-Qaeda terrorism is totally unjustified. Yet when Salafi leaders raised the problem posed by the likes of Abu Qatada to the authorities prior to 9/11, they were met with indifference.

After 9/11 the situation got worse – instead of being ignored they were associated with the terrorist

problem itself. Their experience was similar to those sections of Irish nationalist communities in the UK during an earlier terrorist campaign. Salafis had become ‘suspect communities’. Thus, just as Protestants from Northern Ireland living on the mainland had a largely benign experience of counter-terrorism policing compared to their Republican and nationalist counterparts during ‘the Troubles’, so will the different Muslim community experiences be imperfectly understood until its internal conflicts and rich diversity is acknowledged.

Nearly two years after 7/7 stigmatisation has increased considerably for Salafis, more so than for most other Muslims who have nonetheless faced instances of a less discerning Islamophobia. Influential commentators appear to have succeeded in convincing government and the public that the terrorist threat is rooted in a Salafi or Islamist hatred of the West, that was imported to the UK from Saudi Arabia and elsewhere in the Middle East. As a result long-standing points of religious and cultural tension between different Muslim communities – for example between majority, more traditional Barelvis and minority Salafis – have been heightened by government policy, which now seeks partnerships with the most compliant sections of the faith community.

Thus it has become commonplace to see government and Muslim community leaders sharing platforms to cast further suspicion on those ‘other’ sections of Muslim communities where al-Qaeda propagandists seek most recruits. For Salafi community leaders working against al-Qaeda influence in their communities, the pressure of a double stigmatisation – association with terrorists from without and the slur of informant from within – can be hugely stressful. Only a more enlightened counter-terrorism policy that empowers all sections of Muslim communities, rather than one that empowers one section against another, will reduce the risk of further alienating small but important sections of a stigmatised faith community.

Dr Basia Spalek is Senior Lecturer in Criminology and Criminal Justice at the Institute of Applied Social Studies, University of Birmingham. **Bob Lambert** is a PhD candidate at Exeter University.

References

- Cowan, R. (2004) ‘Young Muslims “Made Scapegoats” in Stop and Search’, *The Guardian*, 3 July, 2004.
- Home Office (2005a) *Preventing Extremism Together Working Groups August-October*. London: HMSO.
- Home Office (2005b) *National Policing Plan 2005-2008*. London: HMSO.
- Young, J. (1999) *The Exclusive Society*. London: Sage.

Us and them – the social impact of ‘new surveillance’ technologies

Michael McCahill argues that new surveillance technologies are reinforcing and worsening social inequalities.

While the emergence of a ‘surveillance society’ is often described in ‘dystopian’ or ‘Orwellian’ terms, surveillance is something which has always existed and is always ‘Janus-faced’, involving both care and control (Lyon, 2001: 3). As proponents of DNA testing have pointed out, while this new technology may provide the police with a powerful tool in the fight against crime, it can also exonerate the innocent. Similarly, CCTV systems have been used to check on the well-being of elderly tenants in high-rise flats and to protect shopkeepers from racial harassment (McCahill, 2002). However, in the context of ‘criminal justice’, it is clear that surveillance practices do not fall equally on all members of society. Surveillance has the capacity to reinforce existing social divisions along the lines of age, ethnicity, gender and class.

This article draws upon research conducted in the UK which examined the ‘social impact’ of ‘new surveillance’ technologies. It concludes by positioning the discussion in a broader ‘global’ context by showing how the ‘war on terror’ is intensifying discriminatory surveillance processes through the disproportionate targeting of ethnic minorities.

Disproportionate targeting and exclusion

While everyone in society in their day-to-day living is subject to surveillance by a wide range of agencies, for some people surveillance is experienced as a totalising and encompassing force. For instance, according to Youth Justice Board research over half of those subject to the Intensive Supervision and Surveillance Programme (ISSP) are unemployed, with poor literacy skills, while 40% of black males have their profiles stored on the National DNA Database, compared with 9% of white males (*The Guardian*, 5 January 2006). Similarly, Norris and Armstrong have shown that the operation of open-street CCTV systems leads ‘to the over-representation of men, particularly if they are young or black’. In the semi-public space of the shopping mall, the disproportionate targeting of young working class males by CCTV operators is accompanied by exclusionary strategies of social control.

In my study of two shopping malls in a northern city, (McCahill 2002) I found that almost nine out of ten (88%) of those targeted were either in their teens or twenties and that ‘when a guard was deployed to deal with a group of teenagers there was a fifty-

fifty chance that someone would be ejected’ (2002: 135). In terms of the social impact of surveillance, exclusionary strategies of social control raise some important questions. The formalised exclusion of young people, for example, draws our attention to competing definitions of ‘risk’ and ‘safety’, particularly as in one study, school children were often excluded from what could be seen as a relatively safe environment (a busy shopping mall full of people) to the ‘less safe’ spaces of public streets. Also, how do those who are banned from the semi-public space of the shopping mall gain access to basic public goods and services (Job Centre, health centre, etc.) which are provided on private property from which they are denied access? (McCahill, 2002).

Central state co-option of ‘private’ surveillance systems

While the expansion of CCTV in the semi-public space of the mall and other retail environments is often driven by the ‘corporate’ mentality of ‘loss prevention’ and ‘commercial image’, these systems can be easily and routinely co-opted for traditional policing. In my study of a housing estate mall in a northern city, for example, (McCahill (2002) I found that the localised knowledge of private security officers was very useful for the police who used the control room as an intelligence base to monitor the local suspect population. Some uses of the system included: CID officers sitting in the control room and using the cameras to zoom in on a local public phone booth to record the telephone numbers dialled by suspected drug dealers; police officers asking the CCTV operators to film the registration number of cars driven by suspected drug dealers; and security officers liaising with the local pharmacist responsible for dispensing methadone to pass the names and addresses of ‘wanted’ persons to the police so that they could be arrested.

‘Function creep’ and the misappropriation of personal information

Surveillance systems also produce information which can be used in ways that are inappropriate or not in accordance with stated aims and objectives (McCahill and Norris, 2003). For instance, while CCTV systems are usually installed for the purposes of crime control, empirical research suggests that CCTV operators also monitor women for voyeuristic purposes (Norris and



CCTV cameras target young black men

Armstrong, 1999: 115). In Australia, it is reported that CCTV operators in Burswood Casino 'videotaped women in toilets and artists' changing rooms, zooming in on the exposed parts of their bodies and editing the video sequences on to one tape that was shown at local house parties' (Koskela, 2000). The use of surveillance for voyeuristic purposes can have serious social and psychological consequences. From his experience of consultation with those subject to voyeuristic surveillance, Simon (1997: 886) suggests that women can develop 'psychological symptoms and disorders, distrust in relationships, fear for personal safety, and shame and humiliation (narcissistic injury)'.

The social impact of surveillance post-9/11

Many of the issues raised above on the social impact of surveillance have much wider relevance as the so-called 'global war on terror' has illustrated. Central state co-option of 'private' surveillance systems, for example, is clearly evident in the Patriot Act and subsequent legislation which has expanded the state's powers to require businesses to turn over records to the FBI; Internet Service Providers (ISPs) to preserve all data specific to a client or for a specified period of time; proposals to make medical records of suspects available to investigators; and an expansion of government powers to spy by wiretaps. 'Function creep' also increases as surveillance systems introduced to monitor 'external' threats posed by terrorists, are used to monitor the behaviour of the wider civilian population. An example is provided by police chiefs in Liverpool who are planning to use unmanned aerial vehicles (UAVs) similar to those used by the CIA, 'to hover over problem estates as part of plans for Britain's first 'yob squad' to tackle anti-social behaviour'. Meanwhile, the misappropriation of personal

information may increase following suggestions by the EU Security Research Programme (ESRP) that all data held by a law enforcement agency in one state should be automatically available to all the others.

Finally, the 'war on terror' has also highlighted issues of immigration and race and encouraged further disproportionate targeting of ethnic minorities. In the immediate aftermath of the attacks on September 11 in the United States, it is reported that up to 5,000 men aged between 18 and 33 from Middle Eastern countries were rounded up for questioning in what has been described as 'a dragnet based on ethnic profiling, not evidence' (*The Guardian*, 22 June 2002). In France it has been reported that 'young people of Algerian or Moroccan descent' are having their ID papers 'checked six times a day' (*The Guardian*, 15 November, 2003). Similarly, in the UK, the uneven impact of surveillance 'is writ large through the seven-fold increase in the number of Asian people stopped and searched by the British Transport Police following the 7 July bombings' (Mythen and Walklate, 2006: 132).

Meanwhile, the introduction of biometric ID systems at border controls means that 'racial profiling' is being coded into the software and has given rise to a new category of suspicion - 'flying while Arab' (Lyon, 2003: 99). In terms of social impact, the disproportionate targeting of many innocent individuals because they fit the profile of 'terrorist', is likely to lead to further alienation as ideological 'fence sitters' begin to take sides and loose alliances become more cohesive groupings whose unwarranted targeting reinforces the view that they do not belong.

Michael McCahill is a Lecturer and Director of the MA Criminology in the Department of Criminology and Sociological Studies at the University of Hull.

References

- Hayes, B. (2006), 'Arming Big Brother: The EU's Security Research Programme', Transnational Institute, TNI Briefing Series, No. 2006/1.
- Lyon, D. (2001), *Surveillance Society: Monitoring Everyday Life*, Buckingham: Open University Press.
- McCahill, M. (2002), *The Surveillance Web: The Rise of Visual Surveillance in an English City*, Cullompton: Willan.
- McCahill, M. and Norris, C. (2003), 'Victims of Surveillance', in *Victimisation: Theory, Research and Policy*, P. Davis, V. Jupp and P. Francis, (eds.) Macmillan.
- Mythen, G. and Walklate, S. (2006), 'Communicating the terrorist risk: harnessing a culture of fear', *Crime, Media, Culture*, Vol. 2, No. 2, pp. 123-142.
- Simon, R. I. (1997), 'Video Voyeurs and the Covert Videotaping of Unsuspecting Victims: Psychological and Legal Consequence', *Journal of Forensic Science*, Vol. 42 (5), pp: 884-889.

Ask the children

Zoë Hilton and Chris Mills summarise their research on what young people think about the government's information sharing proposals.

A key duty of the Children's Commissioner for England is to bring children and young people's views into the national public arena. Major changes are underway to how information on children and young people is gathered and shared. How do they view these changes? The Commissioner asked the authors to conduct a small research project to find out.

Improved sharing of information about children and young people is central to the government's *Every Child Matters* strategy (HMSO 2003). The report of Lord Laming's enquiry into the death of Victoria Climbié concluded that the failure of agencies to share information effectively was an important cause of the tragedy (Department of Health, Home Office 2003). Accordingly, Section 12 of the Children Act 2004 provides for the setting up of an information sharing database containing a record of each of the 11 million children in England. In December 2005, Beverley Hughes, the Minister of State for Children, Young People and Families, announced that the government had approved the necessary expenditure with an intended completion date of 2008.

of Commons 2005). In addition, unease about critical issues such as security, confidentiality and access arrangements was also expressed by the Committee.

The Information Commissioner has also raised concerns about children's and young people's rights to privacy and the need to justify the sharing of information (Information Commissioners Office 2005). These themes are developed in detail in a report for the Information Commissioners Office by the Foundation for Information Policy Research (Anderson *et al.* 2006).

Between September 2005 and January 2006, we convened seven separate focus group discussions across England and one group in Wales to explore young people's views of the database and general issues around information sharing. In all, 71 children and young people were consulted. They included young people in mainstream youth settings, groups of homeless young people, young people in care and young offenders. Importantly nearly all had been in contact with various types of welfare practitioners and professionals and so had experience of information about them being shared (or not shared) by those

Although some of the children wrestled with understanding what the proposals would mean in practice, the overall tenor of their responses was critical.

The database (originally called the 'Information Sharing Index' but now re-named 'ContactPoint') will include information identifying the child, parents or carers, school and GP. It will not include detailed 'case information', and consent will be required for 'sensitive services', but it will contain the name and contact details of agencies and practitioners involved with the child. Additionally, an indicator will be included denoting whether an assessment has been completed.

It is intended that the database will facilitate information sharing between practitioners who have concerns about a child or young person. The government hopes that it will thereby enable earlier identification of specific needs, and earlier and more effective action to address them.

These proposals have attracted considerable criticism. In April 2005, a report of the Education and Skills Select Committee voiced concerns that current research evidence does not demonstrate that information sharing of this type is the best way of improving outcomes for children (House

trying to help them or provide them with services. A 'toolkit' of scenarios was used to help the children and young people discuss the issues and express their views.

The research found a number of concerns (Hilton and Mills 2006). Although some of the children wrestled with understanding what the proposals would mean in practice, the overall tenor of their responses was critical. The young people strongly stated that their confidences should be respected. They expressed concerns about the quality of data in information systems and asserted their rights to access and to quality check their own 'files'. They were particularly reluctant to share information of a sensitive nature (for example concerning sexual health) and some said that they would prefer to forego vital services if their need for privacy in these areas was not respected. They placed emphasis on data security and expressed cynicism about the extent to which IT systems can be made secure.

The young people were concerned about the possibility of labelling and self-fulfilling prophecies

as a result of information sharing. They expressed the view that some problems could be exacerbated, rather than improved, as a result of information sharing, especially where a child was being bullied: in the school context young people expressed strong anxieties about the security of personal information. Many described experiences where information had been passed around the school without their permission. Overall, the young people insisted that all information sharing should be linked to the provision of services which they need and that information should only be shared without the consent of the young person if a high threshold of risk has been reached.

The young people saw trust as being central to the issue of sharing information. As one fifteen year-old respondent put it: 'I think it's about trust, trust is an important thing especially between children and adults ... if there's no trust there, they ain't going to tell you nothing. If you break that trust and you do tell someone else next time you have another situation like that, they ain't going to tell no one and it could have more serious consequences'

The policy implications of this research are clear. Although the young people accepted that information sharing may sometimes be in their best interests, they wished to retain control of what was shared and when it was shared. They implied that if they were unable to trust practitioners and agencies with their personal information, then it would sometimes be withheld. Therefore, the government needs to devise information sharing initiatives which will win the support of children and young people. There is no evidence from this research that the ContactPoint database project has succeeded in this regard. However, in response to these and other findings, the Government has undertaken to involve children, young people and families in the development of ContactPoint and to seek their views. (Great Britain: Department for Education and Skills 2006).

House of Commons (2005). *Education and Skills Committee*. Ninth Report of Session 2004-05 <http://www.publications.parliament.uk/pa/cm200405/cmselect/cmeduski/40/4002.htm>.

Information Commissioners Office (2005) 'Information Commissioner's Memorandum to the Education and Skills Select Committee in respect of the committee's enquiry into Every Child Matters'. http://www.ico.gov.uk/upload/documents/library/corporate/notices/memo_to_the_education_and_skills_select_committee_-_every_child_matters.pdf.

Anderson, R. Brown, I. Clayton, R. Dowty, T. Korff, D and Munro, E. (2006) 'Children's Databases – Safety and Privacy: A Report for the Information Commissioner'. Foundation for Information Policy Research. http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/fipr%20report.pdf.

Hilton, Z. and Mills, C. (2006) 'I think it's about trust': the views of young people on information sharing London: Office of the Children's Commissioner https://www.childrenscommissioner.org/documents/Report_VulnerableChildren_InfoSharing_NSPPCCIndexRep_0%201.pdf.

Department for Education and Skills (2006) 'The Information Sharing Index: Children, young people and families have their say'. <http://www.everychildmatters.gov.uk/>

Dr Zoë Hilton is Policy Adviser (Child Protection) at the National Society for the Prevention of Cruelty to Children (NSPCC).

Chris Mills is a freelance researcher and writer on children's policy. He also holds a part-time teaching post in information management at the University of Warwick, Business School.

References

Chief Secretary to the Treasury (2003) *Every Child Matters* CM 5860. Norwich: HMSO. <http://www.everychildmatters.gov.uk>

Department of Health, Home Office (2003) *The Victoria Climbié Inquiry: Chairman Lord Laming* CM 5730 Norwich: HMSO. <http://www.everychildmatters.gov.uk>

Enhanced supervision or surveillance? The use of CCTV in approved premises

Bernie Heath is concerned about the wholesale introduction of CCTV in probation hostels and the implications for high-risk offenders.

I ncreasing use is being made of CCTV within the 101 'approved premises' (probation hostels) in England and Wales. These hostels provide approximately 2,200 beds for adult offenders. Staffed 24 hours a day, they arguably represent the most intrusive, yet potentially the most constructive, intervention within the Probation Service's responsibilities. The purpose of hostels has historically been concerned with reform and rehabilitation but their function today is arguably more concerned with control with the boundaries between liberty and custody becoming increasingly blurred.

The explanation for this shift in emphasis is that the resident profile has changed in recent years largely as a result of the scarcity of suitable accommodation for released high-risk offenders. Figures demonstrate that the percentage of sex offenders alone has doubled between 1998 and 2004 and that 50% of residents are now on prison licence as opposed to community orders (Foster 2004). The capacity of hostels to manage difficult, damaged and potentially dangerous offenders has increasingly been recognised and this valuable resource has now been explicitly earmarked for those offenders representing a high or very high-risk with the core purpose of hostels described as "the provision of enhanced supervision as a contribution to the management of offenders who pose a significant risk of harm to the public" (National Probation Service 2005). Predictably therefore, the notion of enhanced supervision within hostels is concerned not only with constructive interventions that aim to rehabilitate but also punitive and restrictive measures concerned with control of offenders and protection of the public. In addition to standard rules such measures may include extended curfews, regular 'signing in', drug testing, electronic tagging, and the checking and recording of incoming post. Hostels are therefore becoming softer forms of prison whereby offenders lead a marked monitored existence – a change in emphasis that reflects Garland's (2001) notion of 'penal marking' with punishment continuing into the community.

Increased monitoring and surveillance is an essential part of restrictive measures but it is also about public reassurance. Consequently there has been a steady increase in CCTV cameras, initially funded by individual hostels and located around exits and entrances, to support security and aid verification of curfew arrangements. Whilst there

is legitimacy in the use of such measures, recent years have seen the expansion of extensive CCTV coverage into the semi-private space of all 101 hostels. These are being funded centrally, with the number of cameras ranging between 30 and 40 depending on the size of the building. Although individual bedrooms and bathrooms are excluded, all other areas (including corridors between bedrooms and bathrooms) are under constant surveillance with staff able to routinely observe residents via monitors usually positioned within their office. The extent of its usage is undoubtedly intrusive but nevertheless it has been introduced and accepted by staff, residents and unions with no obvious concerns raised in relation to human rights, its potential benefits or unintended consequences. It is also extraordinary that in an organisation that is concerned with evidence-based practice the use of such costly technology across the whole hostel estate is not subject to evaluation.

The use of CCTV within a confined space naturally bears comparison with Bentham's nineteenth century design of the panopticon prison which enabled covert observation of prisoners who were conscious of that surveillance. Foucault (1977) cited in Norris (1999:91) suggests such surveillance is corrective as not only does it enable a fast response to misdemeanours but it also facilitates individual self-control through 'anticipatory conformity'. In the case of hostels, such conformity is likely to be greater when misdemeanours can be proved on camera and used as evidence for breach and recall to prison.

As part of a planned piece of research, I made preliminary enquiries with a small number of hostel staff who indicated that a calmer atmosphere is evident, they feel safer since the introduction of whole scale CCTV, and there is less conflict and damage within the building. This feeling of safety and security was mirrored by a few offenders I spoke with – although the similarity to the Big Brother House was acknowledged – the difference being 'there are no winners and you can be voted out by the staff'. Other seemingly beneficial aspects of CCTV have been the ability to monitor the administration of medicines, prove an offender's presence or absence within the hostel, offer details as to what they were wearing or who they were with and thus include/exclude them from police enquiries – a significant change in role for probation staff.

CCTV does however have unintended consequences, one of which is that the 'watchers'

also become the watched and it is understandable that in the current blame culture it is used as part of an investigation into deaths or serious incidents to confirm that staff did all they could to avoid tragedy, or, on the other hand, could have done more. Its usage can be further extended to pick up staff misdemeanours, confirm the accuracy of timesheets and verify routine checking of the building and residents.

My initial enquiries indicate that few offenders anticipate or are warned of the extent of surveillance before their admission, and it may be the case that some offenders, uncomfortable with the gaze of the camera, may prefer to remain out of view and spend the majority of their time within their rooms. Alternatively they may want to be less conformist and spend their time outside the hostel environment. Individual responses to intensive CCTV surveillance therefore warrant further research and analysis.

Hudson (2001) has argued that our current 'risk society' tolerates threats to justice and rights and suggests that any new criminal justice interventions should be subject to a 'rights audit' whereby proportionality and fairness are considered. However, the concept of proportionality for certain categories of people has been eroded in the name of public protection, and the hostel population, now designated as 'posing a significant risk of harm to the public' would appear to have had their right to privacy diminished with apparently few misgivings. Currently the use of CCTV is not subject to legislation and is therefore regulated by good practice codes of individual agencies and the Data Protection Act which does not view privacy as a fundamental right but one that has to be balanced against other interests. Hudson warns against the steady erosion of rights, and counsels that the Probation Service, which is involved in the curtailment of rights, should question 'which rights of which parties are brought into question' or the extent to which their rights can be or should be diminished.

The role of hostels in managing dangerous individuals has now been repositioned which means that the restrictive aspects of enhanced supervision are prioritised over constructive measures. (Bridges 2007, Cherry & Cheston 2006.). CCTV is a useful tool but its main downfall is that it has the potential to discourage the active engagement of staff with offenders in favour of surveillance from a safe distance. Effective risk management relies on competent staff really getting to know offenders, building up trust and recognising and responding to behaviour that may trigger a harmful event, and this cannot be done from a distance. Hostels therefore relinquish rehabilitative and constructive measures which facilitate contact with high risk offenders at their peril, as regimes that are predominantly concerned with monitoring and surveillance cannot contribute to effective practice and public protection and can easily be undertaken by external contractors.

Bernie Heath is Senior Lecturer in Criminology at University of Portsmouth.

References

- Bridges, A. (2007). 'Not Locked up but Subject to Rules'. An inquiry into managing offenders in Approved Premises (hostels) following the Panorama programme broadcast on 8 November 2006. London: HMIP.
- Cherry, S. & Cheston, L. (2006). 'Towards a model regime for Approved Premises'. *Probation Journal* 53(3): 248-264
- Foster, S. (2004). 'Approved Premises: Results of a snapshot survey 2003'. (Findings 230). Research, Development & Statistics Directorate. London: Home Office.
- Garland, D. (2000). 'The Culture of High Crime Societies. Some Preconditions of Recent 'Law and Order' Policies'. *British Journal of Criminology* 40, 347-375.
- Hudson, B. (2001). 'Human Rights, Public Safety and the Probation Service: Defending Justice in the Risk Society'. *The Howard Journal* 40(2): 103-13.
- National Probation Service (2005). 'The Role and Purpose of Approved Premises. Probation Circular 37/2005'. London: National Probation Directorate.
- Norris, C. (1999). *Maximum Surveillance Society: The Rise of CCT*. Oxford: Berg Publishers.

Policing Private Space – a three dimensional analysis

Mark Button looks at security officers and their contribution to policing and surveillance.

The importance of private security officers in policing has begun to be recognised by a burgeoning literature on this subject, although there have only been a handful of empirical case studies which explore their contribution (South, 1988; Rigatos, 2002; and Wakefield, 2003). To begin to fill this gap research was conducted which examined the involvement of private security in policing at two sites, typical of many places where they are employed: a retail leisure complex (Pleasure Southquay) and a large factory (Armed Industries) (Button, 2007). A wide range of issues were explored at the two sites, from security officers' knowledge of their legal powers, the extent of use of those powers and some of the occupational hazards faced, as well as their occupational culture. The main focus of this article will be how security officers fit into the broader systems of policing, with brief reference to their occupational culture.

Three dimensions as a tool for analysis

A useful framework to examine the contribution of security officers to policing is to use Luke's (1974) three dimensional concept of power. Power is ultimately about achieving outcomes, and a wide range of strategies, of which security officers are one, are applied to achieve those outcomes. The third dimension of power Lukes proposed rested on the ability of A to get B to pursue a particular course of action by shaping their very needs in such a way that they do not even realise A is exercising power. The second dimension relates to A exercising power over B without any observable conflict, where B knows what A wants and does it, but A does not have to do anything. Finally there is the first dimension where there is observable conflict and B does what A tells them to do.

Put simply in the context of a shopping centre and desire to exclude an undesirable group of young people, the first dimension would be a security officer telling them to leave when they do not want to. The second would be mere officer presence leading them to leave. While the third would be the group not even considering entering such a shopping centre.

The research at the two sites revealed that

the third dimension strategy was most common, using design, image, rules and sanctions, as well as reputation. There is not the time to focus on all of these elements in depth, but it is perhaps worth looking at 'image'.

At Pleasure Southquay marketing and image were very important and played a part in almost all decision-making, including security. Indeed there is considerable research that illustrates how the image of a place can create certain expectations of behaviour, so called 'domestication by cappuccino' (Atkinson, 2003). The promotional literature for Pleasure Southquay sought to create an image of an exclusive shopping location that would discourage many from the neighbouring council estate from even thinking of visiting. This promotional literature contained pictures of yachts and sailing – a very exclusive and expensive pastime. Fashionable 'designer' outlets such as 'Ralph Lauren', 'Tommy Hilfiger' and 'Paul Smith' were promoted. Literature also focused upon restaurants and cafes and dining al fresco as well as entertainment from 'contemporary artists' and comedians – a style of entertainment distinctly different from the traditional working class pubs across the road from Pleasure Southquay.

It is with the second dimension that the main roles of security officers can begin to be seen, where their mere presence achieves the desired outcome. This was the fundamental role of security officers at both of the case study sites. The presence of security officers – in effectively a scarecrow function – meant they did not have to actually do anything to achieve security specific outcomes. Hence at Armed Industries, where it was necessary to show an identity pass to gain entrance, workers in a trance-like state would show their passes to the security officers on the gates in the vast majority of cases, without officers having to say anything. At Pleasure Southquay guards stood on the entrance deterring certain groups from entering and would also stimulate compliance from the public on site by their mere presence. For example, teenagers got off their bikes on sight of an officer.

The last resort at the two sites was the first dimension strategy whereby security officers had to actively confront people.

The research illustrated a scale of strategies

employed. At the base a security officer might ensure consent to their request by asking a question. There was evidence of this at Pleasure Southquay when apprehending shoplifters, and at Armed Industries when carrying out searches. The next level was a verbal request to do something using any 'legal tools' available. Again there was evidence of this at both research sites, particularly at Pleasure Southquay when securing order in the night time economy (NTE). If these failed the next stage was to resort to threats. This might be to threaten to call management or even the police. Again there was evidence of both these types of strategies being used at both sites, particularly in relation to searching employees at Armed Industries. If all these failed, and there was a legal tool available – or the situation already rendered the previous strategies useless – then the next course of action was coercion. This was particularly common amongst some of the security staff at Pleasure Southquay in dealing with disorder in the NTE. Force was not something that officers would universally engage in, and some would move straight to the final strategy of calling a line manager and/or the police to resolve the situation.

Occupational culture

The importance of security officers rests largely on the first and second dimensions (though success at these is likely to contribute to image and reputation in the third dimension). The research also showed that the nature and quality of their contribution to the first dimension did vary and the findings on occupational culture shed more light on this.

The defining characteristic of the occupational culture of a security officer is to 'wannabe somewhere else or doing anything else'. The research found evidence of a low commitment to the job. The main reasons for their dissatisfaction were their challenging working conditions which included long working hours, lack of breaks, poor facilities, and the extremes of weather, as well as their poor pay.

Despite this, a strong degree of solidarity was also found, though for slightly different reasons in the two cases studies. At the retail facility, where there were dangers from arresting shoplifters and dealing with incidents in the NTE, feelings of danger encouraged solidarity. Only if they worked together strongly as a team could they confront these problems. At the factory their solidarity was based on isolation and a sense of inferiority, in that they united in the face of what they saw as 'them and us' – a much less positive reason.

There was also a degree of machismo amongst the security officers studied. At one level this manifested itself in views that women should not be doing certain types of security work, such as patrolling a factory at night alone. At another level this manifested itself in observing the opposite sex during working hours either through the job or in the literature viewed to pass the time. Indeed such were the delights for some officers in watching the 'eye candy' and 'totty', I was told by one officer the job gave him 'ball ache'.

Another characteristic observed amongst security officers was suspicious and risk-focused minds. Many of the officers would naturally look out for potential hazards and risks for the organisation they worked for. This ranged from identifying potential troublemakers who enter the leisure facility to switching off lights and electrical equipment that have been left on by staff. Most were good at this, but there was a minority who did not pursue this, because of their low commitment to

the job. Some, for instance, would pick vehicles to search at the factory because they were 'easy' rather than because there was a genuine suspicion about them.

The research identified different orientations of security officers based upon an 'old watchman parapolice' continuum. At one extreme of the continuum is the 'old watchman' orientation. These officers have little commitment to their role, see their job to observe and report, seek to avoid confrontations and also have little interest in the quality or importance of their work. At the other extreme is the 'parapolice' orientation where there is greater commitment, a preoccupation with 'real work', and a willingness to engage in dangerous situations. These are two extremes of orientation and although many of the officers at the factory could be seen as representing the 'old watchmen' and the retail/leisure facility as the 'parapolice', there were exceptions within these groups of officers.

The research highlights that the primary focus of the two sites was to minimise the need for security officers to resort to third dimension strategies. The security officers played a significant part in policing but the quality of that contribution was compromised by the occupational culture. A number of traits were identified that undermined their competence and commitment, perhaps further reinforcing the need to focus upon the third dimensional strategies.

Dr Mark Button is Principal Lecturer and Associate Head at the Institute of Criminal Justice Studies, University of Portsmouth.

'Security Officers and Policing: Powers, Culture and Control in the Governance of Private Space' is published by Ashgate and can be ordered at <http://www.ashgate.com>.

References

- Atkinson, R. (2003), 'Domestication by Cappuccino or a Revenge on Urban Space? Control and Empowerment in the Management of Public Spaces', *Urban Studies*, 40:9, 1211-1245.
- Button, M. (2007), *Security Officers and Policing: Powers, Culture and Control in the Governance of Private Space*. Aldershot: Ashgate.
- Lukes, S. (1974), *Power: A Radical View*. London: Macmillan.
- Rigakos, G. S. (2002), *The New Parapolice: Risk Markets and Commodified Social Control*, Toronto: University of Toronto Press.
- South, N. (1988), *Policing for Profit*. London: Sage.
- Wakefield, A. (2003), *Selling Security: The Private Policing of Public Space*. Cullompton: Willan.

Taking Surveillance out of the ISSP

Tony Goodman hopes that the Brown administration will take a more welfare approach to working with young offenders.

This is an interesting time to be writing about youth justice, with a change in leadership possibly heralding a change in criminal justice policy away from custody. It's thought that the Treasury was never convinced by a 'prison works' policy so now that Gordon Brown has moved next door might he consider a more imaginative way of dealing with young offenders than stricter community sentencing? When New Labour was first elected, Jack Straw, the then Home Secretary, set out his strong opinions on young offenders in a White Paper *No more excuses* (1997). It is worth recalling his words from the foreword:

'An excuse culture has developed within the youth justice system. It excuses itself for its inefficiency, and too often excuses the young offenders before it, implying that they cannot help their behaviour because of their social circumstances. Rarely are they confronted with their behaviour and helped to take more personal responsibility for their actions. The system allows them to go on wrecking their own lives as well as disrupting their families and communities.'

Intervene hard and enter Big Brother

The ethos of the youth justice system was to become one of early intervention, with young offenders being given a reprimand and/or final warning before they would enter the criminal justice system. No more cautions. It is interesting to note that the word *surveillance* does not appear in this formative White Paper. However the characteristics for offending were spelt out in frightening simplicity:

- being male;
- being brought up by a criminal parent or parents;
- living in a family with multiple problems;
- experiencing poor parenting and lack of supervision;
- poor discipline in the family and at school;
- playing truant or being excluded from school;
- associating with delinquent friends; and
- having siblings who offend. (Home Office, 1997, 9, 1.5).

The Intensive Supervision and Surveillance Programme or ISSP, which was launched in 2001, as its name suggests, attempts to give intensive support to offenders, but simultaneously is heavy on restricting liberty. It did not require a separate piece of legislation. Surveillance had entered the youth justice lexicon in the intervening four years

with a vengeance. The Youth Justice Board (YJB) describes ISSP as:

'the most rigorous non-custodial intervention available for young offenders. As its name suggests, it combines unprecedented levels of community-based surveillance and sustained focus on tackling the factors that contribute to the young person's offending behaviour.' (YJB, 2007)

An ISSP can be imposed as part of a bail condition, Supervision Order or on discharge from a Detention and Training Order (DTO). Clearly in terms of bail the young person is presumed innocent, but they can still be given this intensive order:

'Although the offending behaviour and restorative justice elements of ISSP are not appropriate before a guilty verdict has been established, the young person still receives a minimum of 25 hours supervision and additional surveillance. Schemes are also able to deploy electronic tagging on bail under Section 131 and 132 of the Criminal Justice and Police Act 2001.' (YJB, 2007)

So what does surveillance mean in terms of the ISSP? It can take the form of *at least* one of the following four activities: electronic tagging (to reinforce a curfew), voice verification (done over the telephone to check that the person is where they are supposed to be), tracking (taking the young person to appointments and following up non-attendances) and intelligence-led policing (the overt monitoring of movements and exchange of information with ISSP staff).

When ISSPs started, the offender could be given in a six month programme a minimum of 25 hours per week supervision, with further evening and weekend support in the first three months. For the subsequent three months there had to be provision for daily contact with access to support at evenings and weekends. However following the implementation of the Anti-social Behaviour Act 2003 the maximum number of specified activity days for Supervision Orders has been raised from 90 to 180 days. Increasing the length of time of the curfew from three to six months is being piloted for those under 16 on conviction; this is already the case for 16 and 17 year olds. Cynics might say that this gives plenty of time for the offender to breach the order!

Treatment has got to be good for you?

Back in 1979 Stanley Cohen wrote three articles in *New Society* and these are even more relevant today. In the first article he suggested that the 'back to justice movement' represented a liberal disenchantment with the treatment ideal, which led him to consider social

control alternatives. In the second, he produced a devastating critique of the problems of community control that some readers will be familiar with. He considered the notion of *blurring* the boundaries of social control. In the case of ISSP his words are frighteningly apposite when one considers bail ISSP for the unconvicted: 'The same treatment is used for those who have actually committed an offence and those thought 'at risk' of committing an offence.' He continued (with great resonance for DTO ISSP) that treatment could be used for those coming in and out of institutions with the latter getting a form of diversion as they were not yet 'ready' for the open community. Thus there was the halfway in and halfway out inmate. 'Widening' referred to the process whereby 'alternatives became not alternatives at all, but new programmes which supplement the existing system or else expand the system by attracting new populations ... diversion becomes not movement out of the system, but movement into a programme in another part of the system. The mesh of social control is thinned.' Finally, *masking* is the way that benevolent intentions 'disguise the intrusiveness of the new programmes.'

In the third article he made the point that 'Crime is rooted in the overall social system: political structure, economy and values. There is no evidence that the rate of crime rises or falls with such changes in policy as the intensity of punishment.' With this latter point in mind it is instructive to take into account the evaluation of ISSP by Gray et al. (2005). After all, if it was shown to be a success then Cohen, if not refuted, could be judged as dated.

ISSP on trial

This detailed analysis of ISSP showed some diversion from custodial disposals but 'that ISSP has also replaced some less intensive community disposals as well.' Thirty-one per cent of ISSP cases that breached the requirements of the ISSP were recalled or sentenced to custody: 'Strict enforcement of ISSP therefore did result in a number of young offenders eventually entering custody.' The drop in youth custody between April 2000 and December 2004 was a national trend in both ISSP pilot and non-ISSP areas and could not 'be attributed to the introduction of ISSP.'

From the qualitative data collected on the young ISSP clients they comprised a highly socially excluded group. Indeed comment was made that: 'In many instances, families had already asked for help but had been unable to get any assistance.' Whilst the staff that ran the ISSP programmes were highly committed to the youngsters, 'they lamented the poor statutory services in their area, and felt at times this undermined the ability of ISSP to meet the needs of young people with the most severe underlying problems.' Whilst the programmes met the target of reducing reoffending by 5% and worked best with those with fewest personal problems 'the comparison groups did equally as well in achieving this objective.' Those on DTO ISSP actually performed worse than those released from the DTO without an ISSP. One might ask whether the most successful youngsters needed this level of intrusion into their lives? Finally, research revealed similarities with adult treatment approaches (Merrington and Stanley, 2004), which indicated that the impact of ISSP lessened over time and had almost completely disappeared at 24 months (all citations from Gray et al., 2005, pp8-12).

Most recently the YJB has introduced some changes to mitigate the stringency of ISSP. Employed offenders will have

seven hours of contact per week (which can be at the weekend) and there will be a junior ISSP which will require 12 and-a-half hours per week rather than 25 hours. Whilst these changes are to be welcomed, they do not affect the surveillance component of ISSP.

So was Cohen right after all?

Writing back in 1979 Stanley Cohen could have had no inkling that the reliability of electronic tagging technology would improve so much. This improvement has given credence to the myth that surveillance techniques are more important than welfare considerations, which has a very seductive appeal to our policy makers. The Deputy Chief Constable of Hampshire perpetuated the feeling that Britain was turning into an Orwellian nightmare when he commented that the growth of CCTV could turn the country into 'a surveillance society with cameras on every street corner' (BBC News, 20 May 2007). His prophetic insights should be a warning to us to remember that young offenders are still children and should not be subjected to severe control mechanisms that set them up to fail. Young offenders need to be removed from the ambit of the new Ministry of Justice and placed with the Department for Education and Skills. They should be treated as excluded children first and offenders last. As 'Every Child Matters' states, it is important that: 'being healthy, staying safe, enjoying and achieving, making a contribution and achieving economic well-being should not be denied to the young offender population'. Will Prime Minister Brown be strong enough to question the current fascination with surveillance, rather than the welfare of young people?

Dr Anthony Goodman is Principal Lecturer in Criminology at Middlesex University.

References

- BBC News (2007) *Police chief's Orwellian fears* <http://news.bbc.co.uk/1/hi/uk/6673579.stm>
- Cohen, S. (1979) 'How can we balance justice, guilt and tolerance? 'Community control a new utopia.' 'Some modest and unrealistic proposals.' *New Society*.
- Gray, E., Taylor, E., Roberts, C., Merrington, S., Fernandez, R. and Moore, R. (2005) *Intensive Supervision and Surveillance Programme. The final report*. London: Youth Justice Board.
- Home Office (1997) *No more excuses*. London: Home Office.
- Merrington, S. and Stanley, S. (2004) 'What works? Revisiting the evidence in England and Wales', *Probation Journal* 51(1): 7-20.
- YJB (2007) Youth Justice System: ISSP. <http://www.yjb.gov.uk/en-gb/yjs/SentencesOrdersandAgreements/IntensiveSupervisionAndSurveillanceProgramme/>.

'Drawing the line' and 'applying the brakes': an interview with Richard Thomas, the UK's Information Commissioner

The Information Commissioners Office (ICO) was set up on 30 January 2001 when the Freedom of Information Act came in to promote and protect access to official information. In this interview Enver Solomon of CCJS and Kevin Stenson, guest editor of CJM, ask him how he sees the future of surveillance and information collection, particularly in regards to its impact on the criminal justice system.

Kevin Stenson: In November last year you published a report (Report on the Surveillance Society' available at: www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf) in which you said that fears that we were 'sleep walking into a surveillance society' have become a reality. What kind of surveillance, in particular, most concerns you?

Richard Thomas : The most worrying types of surveillance are hidden surveillance. As you may know I'm also the Commissioner for Freedom of Information and so transparency is a very important drive generally but, if people know what is going on, then that is less threatening. Let me give you a

is and what it's there for, and there are ways and means by which that can be done; not necessarily a label on every camera. We've thought about other ways of communicating the information but we think it's important that there should be only covert surveillance in the most exceptional circumstances and where it can be justified.

Our report painted the picture of life in 2006, which was a very comprehensive survey of different types of surveillance, and then it rolled forward to 2016, 10 years ahead. Now, interestingly, we're only, what, seven months on since our report was published, and already there are so-called 'spies in the sky'. We predicted that by 2012, for the Olympics, we might start seeing spies in the sky for the sake of good public order. Here we are in summer 2007 and Liverpool police now have a hovering camera to keep good order in the city of Liverpool. Scarborough has cameras in the streets now with loudspeakers attached to them, and the Home Office recently announced a programme to roll out more cameras with loudspeakers, saying for instance 'you in the checked shirt, you're not behaving properly; pick up that cigarette' or asking someone to stop misbehaving in a particular way. I'm not saying you can never ever use a microphone, but to pick

We predicted that by 2012, for the Olympics, we might start seeing spies in the sky for the sake of good public order. Here we are in summer 2007 and Liverpool police now have a hovering camera to keep good order in the city of Liverpool.

few examples of that. In the workplace we have an Employment Code of Practice for Data Protection in the Workplace and there are many ways in which employers can monitor the activities of their staff. For example looking at email traffic, internet usage, kit in lorries and cabs of cars. We take a very hard line on that, saying that the employer should tell the employees they are being monitored so that no-one is caught by surprise. That's one example. We talk about CCTV and I'm sure we'll say more about that in a moment, but the technology now exists for very small cameras to be hidden away. One can foresee a scenario where you could have micro CCTV cameras in every lamppost. The current code of practice for CCTV is that it requires clear labelling as to who runs the camera, what its purpose

up conversations I think would be objectionable, with the exception of the most narrowly defined circumstances, and the only circumstance I can think of at the moment are the microphones you get on tube trains where you can talk to the driver.

Enver Solomon: In terms of hidden surveillance then, the police have argued that the only unseen surveillance they might carry out is 'proportionate' and that there are appropriate and sufficient safeguards in place. Do you think that any surveillance of that nature is indeed proportionate and that there are, in your view, satisfactory safeguards in place?

Richard Thomas: Well, first of all you have to recognise, in terms of cameras, that we are probably

the most watched country in the world. You've got the figures: 4.2 million cameras at least, one for every 14 citizens, and some people estimate around 300 times a day you can be on camera somewhere. And I think I also recognise that they're extremely popular with the general public and that, quite understandably perhaps, MPs would say that most of their constituents would like to see more cameras, not fewer. We also recognise that there can be beneficial effects in the prevention and detection of crime, but I think these need more serious debate. There has been a certain amount of research done within the Home Office as to the efficacy of cameras. I don't claim to be an expert on this because I think it's fair to say the jury is still out in terms of the role of cameras in the prevention of crime and there's some evidence that it tends to displace it rather than prevent it altogether. In terms of detection I think probably one can see the arguments being rather stronger. Clearly, if criminal activity has taken place and is caught on camera, one recognises that. I think what I would say is that, if there's a clear need in a particular situation for a camera - say in a particular street where a great deal of drug dealing

positive and negative mistaken identity, believing you're individual A, he's individual A, and in fact they're B, or missing someone because you think you've got an accurate check. There are risks of inaccurate information; there are risks of out of date information, there are risks of improper access to that information and there are risks with security breaches, which is becoming one of the hot topics at the moment.

Now we move on to sharing, because if there are risks associated with the collection in one environment, those risks can be multiplied more and more as the information is shared from one database to another or more, and more people have access to it. For example: let's say that there's a mistake about somebody incorrectly associated with a conviction, incorrectly under suspicion, mistakes about their age, mistakes about their race, all sorts of factual or judgemental mistakes being made; if that information moves on to another organisation, even if it's corrected in the first organisation, there's no guarantee that it's going to be corrected in the second organisation, and we have seen examples - in the area of social services, child protection, education,

We need to be more discriminating, more focused as to the purposes, the benefits, the raison d'être for every piece of surveillance, whether it's in the street or in shopping centres, cameras in stations and so on, before it's actually deployed.

is going on; if you know that people are likely to be victims of drunken loutish behaviour, that assaults can take place, if you know that women are at risk in a particular park, then I have no difficulty at all, nor do I think anybody else does, but not just an indiscriminate roll-out of cameras.

What I am saying is we need to be more discriminating, more focused as to the purposes, the benefits, the raison d'être for every piece of surveillance, whether it's in the street or in shopping centres, cameras in stations and so on, before it's actually deployed. And then there's another whole set of questions about, if you are going to deploy it, well you may as well make sure it works, because many of the cameras are not recording images which can legitimately be used in evidence or in courts of law and so on, so what is the point of that?

Kevin Stenson: Moving on to information sharing and particularly in relation to targeted early intervention programmes for children and families who are considered to be at risk of offending: do you think it's legitimate to bring together data in order to establish who might be the criminals or problem families of the future?

Richard Thomas: I think there are various risks associated with excessive collection of information and, just to run through some of those, risks of both

in the criminal justice field - where information has been incorrect, has been retained too long and has not been put right, even when the problem's been discovered. And yet another example: if you've got one database from which it can leak out inappropriately, if that information is shared across other organisations, well that increases the risk of security breaches.

Enver Solomon: So, if you're bringing data together across different datasets to try and determine who might be more likely to offend there are dangers with that?

Richard Thomas: The short answer is yes there are dangers, and there might be relevance but there are dangers.

Enver Solomon: Do the benefits outweigh the dangers?

Richard Thomas: Well, I think you'd have to look at that case by case. I think we are moving to more and more intelligence-based policing and, if that proves to be effective in both deterring and detecting crime, then there are going to be some benefits in that. But one of the risks which we associate with

Continued on next page



Three hundred times a day you are on a camera somewhere

the excessive use of high technology to process information, is where profiling gets out of hand. Now I think everyone is familiar in the private sector with the way in which profiling is used for commercial advantage as a general proposition, without any great harm or risk. If internet book companies know our preferences for marketing purposes, they may know what sort of books you like to read; if travel companies know your last six holidays, well they can begin to work out what sort of holidays you might like. That causes maybe irritation from time to time and some people don't like too many mailshots or too much marketing material; by and large there's a good solution which is the waste bin. But when it comes to using similar techniques in the law enforcement, child welfare and education world, I think we've got to tread carefully. People say we can feed in lots of characteristics, lots of factors, and we can predict families at risk, children at risk; we can predict even people who may be the criminals of the future. I think this is technology which needs to be used with the very greatest of care. I wouldn't be hostile to using it in a very structured and cautious way where it can protect children from being abused or where some sort of intervention is required with a family to, if you like, help them back on the straight and narrow, but it is very easy to make false conclusions or misleading judgements, which can actually go to the heart of people's life chances for the future. And so, if these techniques are going to be used, and there are already signs that they're starting to be at least thought about, then I think there needs to be the very tightest control framework around them.

Kevin Stenson: To what extent do you think that surveillance and methods of greater improved information sharing should rightfully and legitimately change the nature of a democratic society like ours?

Richard Thomas: Well, I think technology is the thing I keep coming back to because we've now got a situation where, as the price of technology reduces, as the potential of technology increases, we have almost unlimited capacity now to collect unimaginable amounts of information about individuals, to process that in ways which were unthought of 10 years ago, and to hold it forever. Storage can go on forever. And I think that's got absolutely vast implications for the sort of society we want to live in. And these are the questions which we are currently asking. We're saying we need to have a debate about where we want to draw some boundary lines. I have no doubt that all the boundary lines need to be drawn. You could, in theory, say, by planting cameras inside everyone's bedroom, everyone's living room, everyone's kitchen, you know, we can really deal with terrorism and crime, but I think everybody would say that's wholly and utterly unacceptable, so that's clearly a line drawn there. But where do you draw the line? Do you have cameras in every high street, every side street, every narrow street, and every village? And with satellite monitoring, it's not that difficult to monitor the entire country. And so I like to think, but I'm not that optimistic, that Data Protection with its basic framework has the answers, but I think actually it doesn't by itself. I think we can pose the questions: we can say is this a purpose too far, is this an activity where the legitimate functions of preventing terrorism or fighting serious crime, or even minor crime, involves excessive use of data?

Kevin Stenson: Finally, you did at the beginning of this interview present a fairly dystopian picture of spies in the sky-style surveillance. Do you really think that we are moving in that particular direction?

Richard Thomas: I think we're moving in the direction of more and more surveillance but I'm not convinced that we're moving to a destination of a dystopian society as you paint it. I think it's part of my organisation's role to apply the brakes somewhat, to slow down, to make people stop and think before we just go there mindlessly. The report we published last year is very explicit; we're not suggesting that there are evil or sinister powers out there trying to create a Big Brother Orwellian society – an all-seeing all-knowing state – but we may get to a point where we look back and say how the hell did we get here; and if we are slowing things down, if we're raising a debate. I think the view we took was, if we don't do it, no-one else is going to do it. And already I think it's entering into the political mainstream. I don't want to get political about this but I think it has been said that a lot of these things, which can be seen as an attack on civil liberties, or at least undermining civil liberties, have happened over the last 10, 20, 30 years, without any proper awareness of the issues, let alone proper debate. I'm an optimist in life; I don't think we're going to that sort of chilling society that you project; I think we are indicating that's where we could end up if we don't apply the brakes more vigorously, but we're not saying we will end up there. ■

Risky or at risk? Young people, surveillance and security

Surveillance strategies need to focus more on young people as victims rather than potential criminals write **Denise Martin, Caroline Chatwin and David Porteous.**

Most of us experience some form of surveillance in our daily life, whether it is the CCTV camera in the shop where we buy our morning paper, the identify card we use to enter the workplace, or the software that monitors our PC to protect it from fraud. But not all forms of monitoring should be accepted uncritically. As Lyon (2001:4) suggests, there is more than one side to surveillance as it has the 'capacity to reinforce social and economic divisions, to channel choices and to direct desires, and even at its sharp end to constrain and control'. It is these different faces of surveillance that this article will discuss with a particular focus on the experiences of young people. Using a recent (unpublished) research study on crime and victimisation in an East London borough, it will argue that surveillance has varying consequences for young people, and that surveillance techniques

categorical surveillance which is five times the rate for the over 30s'. This was further confirmed by the East London research where young people saw themselves labelled as criminals. One school which participated in the research was located in close proximity to a major supermarket chain. Pupils indicated that they were refused entry to the store prior to, during and immediately after the school day. Identification was by means of a school uniform and security guards chased anyone out who dared enter the store.

School security strategies also illustrate a strong awareness of risk. All of the schools attended by the young people interviewed had CCTV cameras as well as a seconded police officer who patrols the grounds. Other policies include random knife searches and 'lock down', whereby at the end of the school day, sliding doors which give access

Young people's victimisation is endemic across spatial boundaries and the places where they are likely to be subject to surveillance are the very places where they become victims of crime.

reflect a view of them as a 'risky' group rather than a group at risk. This perception fails to recognise the reality and consequences of crime for young people. Nevertheless, despite these tensions, some young people view surveillance as necessary for their own protection.

Young people are often regarded as a group which is likely to engage in criminality, a notion reinforced by New Labour, which has eagerly pursued an agenda engaging with anti-social and disobedient youth (Muncie, 2004). This agenda corresponds with developments within the wider criminal justice system whereby whole groups of the population are being categorised as suspect, and behaviour previously defined as just problematic is criminalised (Hudson 2003). The upshot of this is these groups are monitored and possibly excluded from 'respectable areas'. For young people even hanging out on the street or at the shopping centre becomes 'deviant' activity. This has been confirmed by Norris and Armstrong (1999:114), whose research into targeted CCTV surveillance found that 'youth is treated as suspicious merely because it is youth. Thus two-thirds of teenagers were subject to

to corridors are secured and only staff with swipe cards are allowed passage. When young people were questioned about the effectiveness of these strategies it was clear that they saw them as monitoring rather than prevention tools. One group of boys described how, just yards from the school, they had been subject to a knife attack, but had not received any help until they had managed to return to the front reception desk. Another interviewee recalled being beaten by a group of boys in the playground. 'No-one came to stop it', he said, until eventually some other pupils intervened.

The categorisation of young people as a risky group ignores the reality of young people's experiences as victims of crime. Pain (2003: 165) suggests that young people's victimisation is endemic across spatial boundaries and that the places where they are likely to be subject to surveillance are the very places where they become victims of crime. This view was echoed by our interviewees who described a number of incidents occurring around the periphery of the school or on the journey home.

Continued on next page



One boy had been mugged twice on the journey home, another reported being beaten up by a gang on a bus, others described conflagrations involving large groups of outsiders waiting outside the school gates at the end of the day. Moreover, it was reported that risks to their safety were sometimes magnified rather than reduced by school security measures. For example, a couple of girls reported how they were made to leave one of the schools through a rear exit which was dark in winter and could be particularly intimidating if you stayed late for any reason, as there were fewer people around. A number of young people also questioned the extent to which they were taken seriously as potential or actual victims. One of the most severe incidents reported was an attempted rape, which occurred just outside the aforementioned supermarket. The victim managed to reach the store and report the crime but after they called the police she was left sitting on a bench alone for almost an hour until they arrived.

As Hudson (2003) emphasises, once identified as a 'risky' group your rights as a victim diminish. This was confirmed by some young people who believed there was little point in reporting incidents when nothing was going to get done. Some young people had a negative view of authorities like the police as they 'moved them on' when they were in groups, possibly sending them to even more dangerous, unmonitored places. It should be noted that the schools involved did take bullying within the school seriously and young people who had been a victim of crime outside of school also reported their satisfaction with the school support.

Although some young people were indifferent to forms of surveillance such as the school police officer and CCTV cameras, others believed that increasing forms of surveillance were required in order to deal with crime. For example, a number of young people suggested extending the use of surveillance cameras to quieter streets whilst the most commonly cited suggestion for improving safety was an increased police presence. Many students also cited strategies such as not being out after dark or not walking home alone as ways they had found to improve their safety. Their actions suggest that while there may be a general call for increased surveillance to make an area safer, surveillance may not, in practice, be enough and other strategies need to be implemented.

In examining the experience of young people and surveillance a contradictory picture emerges. On one hand young people are viewed as a potential threat that requires monitoring, whether this includes cameras and security in schools or exclusion from consumer sites. On the other, the potential threat to them in some of the spaces they occupy is ignored, leading to a high level of victimisation that can have severe consequences for those involved. This needs to be further recognised by official bodies if the victimisation of young people is to be properly dealt with. Despite the discriminatory nature of surveillance, that some young people believed it offered them the best protection from future victimisation is a matter for further and continuing scrutiny.

Dr Denise Martin, Dr Caroline Chatwin and David Porteous are based at the Criminology Department, Middlesex University.

References

- Hudson, B. (2003) *Justice in the Risk Society*, London: Sage.
- Lyon, D. (2001) *Surveillance Society*, Buckingham: Open University Press.
- Muncie, J. (2004) *Youth and Crime*, London: Sage.
- Norris, C. and Armstrong G. (1999) *The Maximum Surveillance Society*, Oxford: Berg.
- Pain, R. (2003) 'Youth, age and the representation of fear', *Capital & Class*, Summer 2003 Issue 80, p151-171.

Balance, scrutiny and identity cards in the UK

Cheryl A Edwardes, Ian Hosein and Edgar A Whitley contend that the government's argument that ID cards are for the 'greater good' needs to be scrutinized and balanced against the needs of the individual.

Our often bruising experiences researching the introduction of the UK Identity Cards Act (see Whitley *et al.* 2007) has provided a unique insight into ongoing debates about political theory and the legislative process. In particular, our research into the identity cards scheme raises important questions about the relationship between balance and scrutiny which we explore in this article.

Writing in 1690, the political philosopher John Locke suggested that 'in well-ordered common-wealths, where the good of the whole is so considered ... the legislative power is put into the hands of divers persons ... [who] have by themselves ... a power to make laws, which when they have done, being separated again, they are themselves subject to the laws they have made; which is a new and near tie upon them, to take care, that they make them for the public good' (Locke 1690). He was arguing that when government acts in the interests of 'the public good', effective mechanisms for independent scrutiny should be put in place to ensure that its powers are used with caution and consideration.

Notable philosophers since Locke have echoed these sentiments. Jean-Jacques Rousseau envisaged a legislator with a 'great soul' proposing laws conducive to the common good and believed purity of motive was only guaranteed if the adoption of the proposed laws depended upon the approval of those to be bound by them (Rousseau 1762). John Stuart Mill, considering representative government in 1861, paired a small body of crown-appointed men legislating for the common good with 'skilled labour and special study and experience', with a body publicly elected to "watch and control the government [and] throw the light of publicity on its acts" (Mill 1861).

Almost a century later, Karl Popper advocated the establishment of a group of social engineers mandated by a universal 'agreement about existing evils and the means of combating them' to 'incrementally improve society'. These engineers would have no need for the use of 'passion and violence in executing' their social reforms (Popper 1945).

These thinkers agree that political actions should be motivated by the common good and agree upon the necessity of ensuring that actions taken in the

name of the common good are just that, typically by some form of independent scrutiny. All, however, define the common good differently. Locke believes it is safety and physical well-being, for Rousseau it is liberty, Mill thinks it is happiness and Popper the eradication of social ills. The diversity of these interpretations and definitions of the 'common good' emphasises that the common good is a notion that can be easily adopted by governments as they justify their own political or ideological aims'.

Identity cards and the common good

The build up to the introduction of identity cards in the UK has been focused on the common good. Concerns about civil liberties and older notions of British values and culture were set aside by government ministers, as they advanced the concept of the common good. On the day the Identity Cards Bill was given its second reading in Parliament, the then new Home Secretary, Charles Clarke, wrote passionately in the Times, saying:

'I claim that the ID Cards Bill that I am introducing today is a profoundly civil libertarian measure because it promotes the most fundamental civil liberty in our society, which is the right to live free from crime and fear' (Clarke 2004).

This view relies heavily upon communitarian philosophy and implicitly moves the debate from scrutiny to one of balance. Its leading thinker is Amitai Etzioni who, in his influential book, *The Limits of Privacy* (1999) argued that we must heed the needs of the many instead of over-emphasising the interests of the few.

'Although we cherish privacy in a free society, we also value other goods. (...) To begin a new dialogue about privacy, I [ask] if you would like to know whether the person entrusted with your child care is a convicted child molester. I further ask: Would you want to know whether the staff of a nursing home in which your mother now lives has criminal records that include abusing the elderly? (...) Addressing such concerns raises the question of if and when we are justified in implementing measures that diminish privacy in the service of the common good.'

In calling for 'balance' and the 'common good' politicians believe that their ideas are firmly

Continued on next page

founded in political theory and that they also have the benefit of a monopoly on the legislative process. Although such a position might imply that balance is distinct from scrutiny, even Etzioni recognised that any balancing scheme must be carefully regulated. As a result he qualifies the ‘balancing act’ and demands that the need for intervention be properly documented, that non-infringing alternatives be considered, the effect of any intervention is minimised and that undesirable side effects are properly managed.

In the case of the Identity Cards Scheme the Government has shown little restraint in its policy and technology design. For instance, the purpose of the Scheme continually shifted as the government moved from preventing benefit fraud, to tackling terrorism, then to preventing identity fraud, without ever fully understanding the nature of these problems to begin with. Moreover, the most invasive design was chosen: under the Scheme, all UK residents and citizens will be fingerprinted, and these fingerprints will be available for comparison with those left at scenes of crime (Blair 2007).

Balance and Scrutiny?

Whilst the arguments for balance and the ‘common good’ run throughout the Scheme, questions of scrutiny are less clear. Indeed a policy process that resulted in a scheme of this sort leads us to doubt whether Parliament was truly able to scrutinise it in the first place. Moreover, recent events associated with the UK Identity Cards Scheme suggest that while Government is happy for the Scheme to have a potentially large impact on the scrutiny of the actions of individuals, it is less open to the idea of scrutiny of the Scheme itself.

Since 2000, ‘Gateway Reviews’ undertaken by the Office of Government Commerce (OGC) have been set up to ensure that the procurement of large government IT projects deliver value for money. These independent reviews are intended to check that the plans for a project are sufficiently developed. In the case of the Identity Cards Scheme, the Government repeatedly asserted that the Scheme had passed its various Gateway Reviews but refused to disclose the contents of the reviews.

The Information Commissioner, who regulates the Freedom of Information Act (FoIA), disagreed with the Government and concluded that, especially in the case of such an important scheme, the Gateway Reviews should be made public. Rather than accepting this decision, the government took the case to an Information Tribunal. In May 2007 the Tribunal concurred with the Commissioner. However, at the time of writing, the OGC had still not disclosed the content of these reviews. On May 30 2007 the OGC announced that they would appeal the case to the High Court to prevent disclosure. Two days later *Computer Weekly*, one of the leading newspapers for the IT industry, uncovered orders to OGC staff to destroy internal reports ‘and all supporting documents’ (Collins 2007). The Tories and Liberal Democrats condemned this move as an attempt to further hide the details of the ID scheme, and other contentious IT projects.

The Government has argued that there were legitimate reasons behind their actions suggesting that the effectiveness of the Gateway Reviews would be diminished if participants knew that they might be made public at some later date. However, at the Information Tribunal, we learned that the Government briefed participants of the Gateway Reviews saying that there was ‘little risk of [Gateway Reviews] being disclosed under

FoIA or other means’, i.e. the normal expectation was that independent scrutiny of this aspect was unlikely to happen. This is despite the fact that Freedom of Information legislation is intended to provide a mechanism for such scrutiny to take place if required; instead the government insists on keeping the results hidden.

Perhaps we are seeing a massive shift in the view of decision-makers who not only believe that the balance in favour of the common good must be served, but that this must be done with minimal scrutiny. Such a trend appears not to be limited to the UK as the US Secretary of Homeland Security recently presented a similar view, when he tried to convince the European Parliament that it should stop interfering with US anti-terrorism policy and permit the US to accumulate travellers’ data from EU sources with limited oversight:

‘You must ask yourself this question—whether you would be satisfied to be constrained by slow-moving processes if the consequence would be to allow an attack to go forward that would kill thousands of people or perhaps millions of people, including one’s own children’.

The arguments made by authors from Locke onwards involve checks and balances; yes there is the common good that must be balanced against the rights of the individual but in addition, claims made on behalf of the common good must be subject to independent scrutiny. In the case of the ID Cards Scheme this appears not to be happening.

For more information about the LSE Identity Project, please visit our website <http://identityproject.lse.ac.uk>.

Cheryl A. Edwardes, Ian Hosein and Edgar A. Whitley are part of the *Information Systems and Innovation Group, Department of Management, London School of Economics and Political Science*. <http://is.lse.ac.uk>.

References

- Blair, T. (2007) ‘PM’s response to ID cards petition,’ 19 February 2007. Available at <http://www.pm.gov.uk/output/Page10987.asp>.
- Clarke, C. (2004) ‘ID cards defend the ultimate civil liberty,’ *The Times*, 20 December, 2004.
- Collins, T. (2007) ‘Civil servants told to destroy reports on risky IT projects’, *Computer Weekly*, 1 June, 2007.
- Etzioni, A. (1999) *The limits of privacy*, Basic Books: New York.
- Locke, J. (1690) *Second treatise on Civil Government*.
- Mill, J. S. (1861) *Representative Government*.
- Popper, K. R. (1945) *The open society and its enemies: Volume 1 The spell of Plato*.
- Rousseau, J-J. (1762) *The social contract or principles of political right*.
- Whitley, E. A., Hosein, I. R., Angell, I. O. and Davies, S. (2007) ‘Reflections on the academic policy analysis process and the UK Identity Cards Scheme,’ *The information society*, 23, 1, 51-58.

Open-Street CCTV Canadian Style

Randy Lippert describes how Canada is moving towards increased CCTV presence.

Introduced by local police to watch streets in the downtown bar district, the first open-street closed circuit television (CCTV) program in Canada appeared in Sherbrooke, a small Quebec city in 1992. In the 15 years since, small scale, open-street CCTV programs have slowly emerged in city centres across the country. Rather than a federal or provincial government initiative, the 16 or so current programs have resulted from varied local police, municipal government, and business improvement association funding arrangements, along with private security marketing (see Brown and Lippert, 2007) initiatives in which cameras or services are 'donated'.

Most often cameras are introduced in downtown retail strips near a concentration of bars to target criminal and 'anti-social' conduct, especially during early morning closing times. As in post-industrial cities in the UK (Hobbs et al., 2003), many Canadian open-street CCTV programs have appeared with the growth of night-time, retail alcohol establishments in downtown 'entertainment' areas. Although

Section 7 requires secure storage of collected CCTV images from 48 to 72 hours before deletion unless retrieved for law enforcement purposes. Compliance with section 7 is plainly evident in working programs, but adherence to section 4 is dubious and tends to go unmonitored. A third guideline – section 6 – requires posting signs at the perimeter of cameras' gaze (or distributing pamphlets) indicating to the public why their personal information is being collected. They are not required to include information about how to file a privacy complaint.

Since deterrence is often used to justify CCTV programs, why only a rudimentary sign or pamphlet is required, rather than additional means, is unclear (and ironic since privacy commissions were created to confront the rise of new communication technologies that can disseminate information widely and inexpensively). This lack of public communication about CCTV and privacy law helps explain why since 2001 the Ontario commission has received only one complaint about open-street CCTV.

CCTV cameras are increasingly monitored by private security firms that fall under provincial licensing regimes, but so far no public discussion has taken place about a need for operators to be trained on human rights or privacy issues in order to obtain licenses.

urban revitalisation and the threat of terrorism are occasionally used to justify the introduction of CCTV, more often police and other advocates cite a widely publicised, violent incident that occurred in an area and the need to deter similar acts as justification.

There are currently no legal provisions prohibiting police or governments from establishing open-street CCTV in Canada. Regulation remains limited to efforts of the federal and provincial privacy commissions, although open-street CCTV falls under their mandate only in so far as cameras collect personal information. The commissions' annual operating budgets are but a few million dollars annually and therefore tiny in relation to their mandates' scope, which in Ontario entails administering two Acts governing both privacy protection and freedom of information. Nevertheless, Ontario's privacy commission published *Guidelines for Using Video Surveillance Cameras in Public Places* in 2001 (IPC, 2001). Three guidelines are noteworthy. Section 4 places responsibility squarely on police and municipal officials to show that less intrusive means of policing are unworkable so they can justify each camera via verifiable crime incident reports.

In some instances police services are distancing themselves from direct involvement in open-street CCTV – when it does come to the public's attention – due to its 'Big Brother' image and the burden of funding ever-changing technology while – at the same time – retaining easy access to CCTV images to pursue criminal prosecutions. CCTV cameras are increasingly monitored by private security firms that fall under provincial licensing regimes, but so far no public discussion has taken place about a need for operators to be trained on human rights or privacy issues in order to obtain licenses.

The most publicized Canadian open-street CCTV system to date is operated by the Royal Canadian Mounted Police (RCMP) in the small resort city of Kelowna, British Columbia (BC). One CCTV camera linked to the local detachment was set up in a park in 1999 and then another to watch an outdoor downtown bus transit area to monitor the drug trade. Following complaint from the provincial privacy commissioner in 2001, the federal privacy commissioner ordered the RCMP to cease 24-hour recording. A month earlier

Continued on next page

the federal commissioner had successfully halted a privately-run open-street camera operation in Yellowknife, Northwest Territories (NWT) (an operation which – like the RCMP itself – fell under federal jurisdiction) on privacy grounds. This time the RCMP ceased 24-hour recording, bringing the operation into technical compliance, but continued 24-hour monitoring. In 2002 the federal commissioner then took the RCMP to British Columbia Supreme Court to try to halt operations by invoking Section 8 of Canada’s Charter of Rights and Freedoms, claiming open-street CCTV constituted an ‘unreasonable search’. Following national publicity, in 2003 the court ruled the commissioner lacked legal standing to initiate the action. Since replaced (he was ironically charged by the RCMP on an unrelated criminal matter), the new federal commissioner has not taken up the legal fight and Kelowna’s program has expanded to new locations. Other than, most notably, in Brockville, Ontario and Vancouver - where local public resistance halted open-street CCTV plans - serious legal barriers and organised public resistance to its introduction in new locations is relatively rare and otherwise ineffective in Canada.

Among provincial privacy commissions, Quebec’s (Commission d’accès à l’information du Québec) regulations in relation to open-street CCTV implementation are the most restrictive or at least enforced, and in 1992 actually halted the Sherbrooke program citing privacy concerns as the reason. This commission requires crime reduction be evaluated to justify continuance in lieu of alternative methods such as foot patrols. Consistent with this requirement, an ongoing independent evaluation using a quasi-experimental method in downtown Montreal is currently underway. An early study in Sudbury, Ontario using a before-and-after design conducted by consultants for local police in 2000 (KPMG, 2000) has been widely cited – typically coupled with selective UK examples - as evidence of crime reduction effectiveness to justify new CCTV programs. Outside these instances, there are no other independent evaluations of open-street CCTV or studies that seriously consider displacement or other methodological issues in Canada. This is undoubtedly because there is no monetary incentive, legal requirement, or political advantage to conduct them, with anecdotal evidence usually cited as program justification instead.

Open-street CCTV, its regulation, and its evaluation, are all embryonic in Canada. In its present state open-street CCTV in Canada resembles more the Australian experience (see Sutton and Wilson 2004) than that of the UK. However, recently a major open-street CCTV pilot project was launched by police in Toronto. In receiving a two million dollar provincial government grant and in promising an independent evaluation, this program may be a sign that Canada is beginning to move toward the UK model.



Photo: Steve Ball

Canada is following the UK's example

Randy Lippert is associate professor of criminology, University of Windsor, Ontario, Canada. He is studying open-street CCTV in three Canadian cities.

References

Brown, J. and R. Lippert (2007) ‘Private Security’s Purchase: Imaginings of a Security Patrol in a Canadian Residential Neighbourhood’ *Canadian Journal of Criminology and Criminal Justice* (In Press).

Hobbs, D., Hadfield, P., Lister, S., and Winlow S. (2003) *Bouncers: Violence and Governance in the Night-time Economy*. New York: Oxford University Press.

KPMG (2000) Evaluation of the Lion’s Eye in the Sky Video Monitoring Project. <http://www.police.sudbury.on.ca/publications/reports/KPMG.pdf>.

Information and Privacy Commissioner (IPC) (2001) *Guidelines for Using Video Surveillance Cameras in Public Places*. Toronto: Information and Privacy Commissioner/Ontario.

Sutton, A. and Wilson, D. (2004) ‘Open-Street CCTV in Australia: The Politics of Resistance and Expansion’, *Surveillance and Society* 2(2/3): 310-22.

The architecture of surveillance

Richard Jones writes about the politics and design of surveillance systems and compares the views of leading theorists.

Surveillance studies are today in good health, and raising a questioning voice in the face of what appears to be the roll-out of a never-ending stream of new surveillance technologies. While the ‘greats’ such as Marx, Weber and Foucault continue to exercise their influence over theoretical approaches, new directions are also apparent. David Lyon’s careful sociology continues to inform (see pp 4). Several researchers have revealed the social realities of CCTV system operation and workplace surveillance. Themes of current theoretical interest include the state, identity systems, and the regulation of, as Lyon puts it, the two key areas of ‘travel and transaction’; the surveillance of ‘mobilities’ generally; the nature of ‘privacy’; state-commerce relationships; and the politics of surveillance. Here, I will concentrate on just one small issue related to some of these themes, namely how surveillance systems can be designed to emphasise different political values — the theoretical implication of which is that technological system design is more of a political activity than it first appears, and hence bears closer scrutiny.

In his book, *Code*, the American lawyer and Internet theorist Larry Lessig (2006) argues that the internet is regulable not only through law, but also by market forces, social norms, and by what he terms ‘architecture’. By this last term, he means the physical or virtual properties of a system, suggesting that in a given system these properties enable and constrain users’ behaviour in certain ways. The system design, Lessig argues, typically expresses or supports certain political values. For example, a computer network could be designed to protect users’ anonymity, or alternatively it could be designed to permit easy identification of users by others. Elsewhere, I have argued that Lessig’s model has interesting parallels with the more clearly criminological work of Anthony Bottoms on compliance; and with R.V. Clarke and colleagues’ development of situational crime prevention typologies. I have also shown how a model synthesised from these approaches can be applied to fields as disparate as cybercrime, punishment, and policing (see, for example, Jones 2007). Much of this work focuses on physical or virtual constraints. Can the notion of ‘architecture’ also be applied to the study of surveillance systems, seemingly designed more to watch rather than constrain — and if so, what if anything does this tell us?

In fact, architecture accounts not just for

what users can and can’t do within a given system, but also for what administrators can and can’t know or do about those users. (I use the term ‘administrators’ to refer to anyone from a CCTV scheme operator, through to state security services; and ‘users’ to refer to the end users of physical or virtual spaces.) In other words, the term ‘architecture’ relates to the overall operating properties of a given system. These properties typically cast a (political) relation between users and administrators, and different technological designs can support different political values. An online discussion board system might for example be designed to promote user anonymity (‘privacy’) or instead be designed to enable identification of discussants (‘security’).

There are a number of dimensions to surveillance architecture that are of interest from a privacy perspective. One is whether the system design enables users to tell whether they’re being monitored or not: the visibility or invisibility of the surveillance system. (Perhaps this is a spectrum, running from the overt surveillance of visible observation by a police officer, for example; through what Michel Foucault termed the ‘visible and unverifiable’ surveillance of the Panopticon (or, today, an unconcealed CCTV camera: you can see it’s there, but can’t tell if you’re being watched); to covert surveillance.) A second is whether the technology simply ‘monitors’ activity as it happens, or whether it additionally or instead stores a ‘searchable’ record (Lessig, 2006: 202). One of the privacy challenges of ‘digital surveillance’ lies in the capabilities enabled by database search. A third (and related) dimension, and perhaps the most obvious, is the degree to which the surveillance system design protects or intrudes upon users’ anonymity. Rotenberg (2001), following others, distinguishes between ‘Privacy Enhancing Technologies’ (PETs) and ‘Privacy Intrusive Technologies’ (PITs). PETs can include ‘[e]ncryption, anonymous web-browsing, filtering devices... privacy-preference tools and the like’, and can offer some degree of privacy, though they are no panacea (Ball et al., 2006: 83-84). The point to note here, however, is simply that not all surveillance is similarly intrusive.

Lessig coins the term ‘digital surveillance’ to describe a ‘very specific kind of surveillance’, in ‘which some form of human activity is analysed by a computer according to some specified rule’

Continued on next page

(Lessig 2006: 209; see also Graham and Wood 2003), an area that David Lyon and others have explored in detail (see for example Lyon 2002). A challenge for 'friends of privacy' in respect of digital surveillance is to establish what exactly it is about discrete, automated, computerised surveillance that remains objectionable. Lessig suggests three possibilities: such searches offend a person's dignity; they are intrusive; or they represent insufficient limits on government power over individuals.

In some respects Lessig's work echoes Packer's earlier account of two opposing models of the criminal process. Indeed, in his famous book *The Limits of the Criminal Sanction*, Herbert Packer (1969) discusses the electronic surveillance of the time in the context of considering competing 'Due Process' and 'Crime Control' ideologies during the initial phases of the criminal process. Although written before the emergence of 'digital surveillance' technologies, and focusing on the then 'war on organised crime' (which today we might transpose to the 'war on terror'), arguably many of the basic issues relating to surveillance remain the same. Packer recognises that surveillance technologies 'pose increasingly difficult problems for the criminal process as pressure from law enforcement for license to enlist these devices in the investigation of crime meets counterpressure from people who see the doom of individual freedom in a wholesale intrusion by government into the private lives of its citizens' (1969: 195).

In the case of electronic surveillance, the 'Crime Control Model' expresses strong support for its use by law enforcement officials, maintaining that while abuses may sometimes occur this is a price worth paying, and that in general, 'Law-abiding citizens have nothing to fear' (1969: 195-196). The 'Due Process Model' on the other hand, argues that 'The right of privacy... cannot be forced to give way to the asserted exigencies of law enforcement'. Moreover, knowledge of unchecked surveillance 'would certainly inhibit the free expression of thoughts and feelings that makes life in our society worth living' (1969: 196-197).

A distinctive feature of Packer's book was his role-play of the two competing positions, on the issues at each stage of the criminal process, showing how the respective positions taken express not merely the prioritising of due process over crime control goals (or vice versa), but also express a wider political ideological stance, turning ultimately on the relationship between individual and state. Introducing Packer's model into the surveillance and privacy debates is helpful then, I think, because it helps us locate these debates within a still deeper political antagonism, namely between Due Process and Crime Control values. From this perspective, privacy concerns surrounding surveillance become more clearly related to debates elsewhere in criminal justice, such as about prisoners' human rights. Indeed ultimately Packer's thesis is about

competing political views on law, and specifically about legal protections afforded to individuals as against the state. Lastly, Packer's model is useful in suggesting a framework characterising the ideologies expressed in the designs of intrusive surveillance technologies (such as 'backscatter' x-ray body scanners) and in the pro-privacy objections to such technologies.

In conclusion, my argument here is that Lessig's and Packer's models are useful in helping us distinguish between surveillance systems in terms of the political values embedded therein. Of course, this is not the end of the matter, and how the system operators actually use the systems clearly remains of crucial importance. However, system design is likely to influence system use at some level, and further exploration of the properties, features and uses of surveillance systems may help us cast further light on this still often hidden area.

Dr Richard Jones is based at Edinburgh Law School, University of Edinburgh.

References

- Ball, K. *et al.* (2006) *A Report on the Surveillance Society*. Surveillance Studies Network.
- Graham, S. and Wood, D. (2003) 'Digitizing surveillance', *Critical Social Policy*. Vol. 23(2): 227-248.
- Jones, R. (2007) 'The Architecture of Policing' in A. Henry and D.J. Smith (eds) *Transformations of Policing*. Aldershot: Ashgate.
- Lessig, L. (2006) *Code version 2.0*. New York: Basic Books.
- Lyon, D. (2002), *Surveillance as Social Sorting*. London: Routledge.
- Packer, H. (1969) *The Limits of the Criminal Sanction*. London: OUP
- Rotenberg, M. (2001) 'Fair Information Practices and the Architecture of Privacy', *Stanford Technology Law Review* 1.

Electronic monitoring, commercial surveillance and the 'malfunctioning subject'

Craig Paterson looks at the implications of electronic monitoring for modern society.

Between 14,000 and 15,000 people are now subject to a variety of forms of electronic monitoring (EM) across England and Wales. First used in 1989, those subject to EM-based programmes include bailees, adult and juvenile offenders, prisoners under early release restrictions, terrorist suspects, individuals subject to immigration controls and, potentially in the near future, the elderly and those who refuse to pay child support. Growth in EM has been driven by a fascination with the potential of new technologies to deliver 'techno-managerialist' solutions to complex social problems. This techno-centric view of the use of EM has meant that the wider implications of its development have often been missed. EM represents the movement of commercial surveillance technology into people's homes, the extension of societal controls and the potential for commercial personnel to make disciplinary, normalising judgements about the

do they present?' have remained unanswered.

Although international debate has concentrated upon the types of offenders that *should* be made subject to EM, a familiar pattern has been adopted towards offender targeting in England and Wales. This focuses upon the 'usual suspects' and targets of crime control methods – in general, those individuals living in the most deprived areas of the country. The development of commercial crime control technologies supplements the already intensive focus upon these individuals and groups who are deemed to be 'malfunctioning' and is reinforced through, Anti-Social Behaviour Orders (ASBOs), Acceptable Behaviour Contracts, Exclusion and Dispersal Orders, the proliferation of CCTV, biometrics and even identity cards as further weapons in the sovereign battle for control over disorderly neighbourhoods and, in particular, disorderly youth.

The development of commercial crime control technologies supplements the already intensive focus upon these individuals and groups who are deemed to be 'malfunctioning'.

behaviour of 'malfunctioning' subjects: those deemed by authorities to manifest limited ability to regulate their conduct and who require additional control. There is a historical parallel here with the extension of social work governance of family life (Donzelot, 1980).

The growth of the EM of offenders in England and Wales has taken place despite a lack of conclusive evidence that it 'works' in protecting the public, reducing re-offending or changing behaviour in the long-term (Mair, 2005). In part, this explains the diverse use of EM technologies in the criminal justice system and the lack of a coherent Home Office policy concerning its most effective use. This is not a unique set of circumstances. Debates on the introduction of crime control technologies such as CCTV, biometrics and identity cards have borne considerable resemblance. While the salient ideological and political discourse in these discussions has revolved around issues of surveillance, security and control, more practical questions such as, '*what can these technologies actually achieve?'*' and, '*what indirect consequences*

This view is supported by evidence collected in research conducted with Group 4 Securicor, an EM service provider. Analysis of EM statistics in Greater Manchester found that the areas experiencing high levels of juvenile nuisance were similar to those with high numbers of offenders subject to EM. The Intensive Supervision and Surveillance Programmes (ISSP) and Intensive Change and Control Programmes (ICCP) that incorporate EM for persistent juvenile and young offenders, were developed to counter growing concern about 'youth nuisance' in the area. This was further confirmed by Manchester's top position in the league table of local authorities issuing ASBOs, with 1237 issued between 1 April 1999 and 31 December 2005, of which 51 per cent were issued to 10-17 year olds (Home Office, 2007). Previous research has shown that 74 per cent of ASBOs were used against those aged twenty-one or under (Campbell, 2002).

Although using the language of enhanced security and public protection to justify growth in

Continued on next page

the use of EM, this technology has in reality served to expand regulatory systems of social control for those deemed to be 'malfunctioning'. The extension of surveillance into domestic space was acknowledged by Group 4 Securicor as providing a distinct separation between their service and traditional community penalties:

'What other community service order can give them absolute proof of compliance? Otherwise, it's just speculation. Little Johnny reported to the police at eight o'clock on a Friday night as he was supposed to do, but where was he at half past ten? Nobody knows...But we do now'.

(EM Manager)

The implication here is that traditional community penalties did not provide sufficient levels of public protection and security due to inadequate surveillance. The current thinking sets in place a process through which increasingly intensive and intrusive forms of surveillance can be justified in the name of enhancing security:

'I can see a whole range of community service orders based on satellite tracking. They (central government) will want to know the whereabouts of individuals, particularly those guilty of less acceptable crimes. They will want to know the whereabouts of paedophiles, sex offenders and the like 24 hours a day.'

(EM Manager)

The broad, and often unclear, use of the concept of 'security' has the potential to render the term redundant, just as with earlier conceptions of social control (Cohen, 1985). And the conflation of security rhetoric in political debate about the control of young people and the control of terrorism is particularly invidious. How does a surveillant technology that locates the whereabouts of an individual actually enhance security and public protection, when there is no immediate means to enforce violations? Instead, it seems that the politicisation of 'technocorrections' generates a chimera of control which disguises the messy reality of everyday life that exists beneath the surveillance gaze.

The EM of offenders represents just one section of the expanding industry in 'technocorrections' that incorporates elements of the private security, military and telecommunications industries. The surveillance capacity generated by these industries has diverted attention away from the role of human agency in the implementation of surveillance technologies. Surveillance studies encourage an understanding of EM as a form of socio-technical interaction extending the focus of previously public surveillance technologies (for example, CCTV) into the domestic sphere. EM curfew orders seek to remove disorderly groups and individuals from public space and to encourage structure in often unstructured lives. Demand for the control of offenders also emanates out of communities and helps to create a contested political struggle over the regulation of local populations and territories. The use of EM curfew orders in addition to other social management strategies asserts the interests of 'respectable' members of the community ahead of those deemed to be troublesome, whose freedom to roam is limited. EM must therefore be understood as a component of the extensive crime control machinery available to the state, commercial organisations and local community groups to target specific populations through routine, formal and informal surveillance.

The recent shift in the use of EM technologies beyond crime control has taken place with practically no public debate about the use of regulatory surveillance and the indirect consequences for new populations deemed to be 'malfunctioning'. This is

partly because surveillance encounters are now seen as the norm in the society that we live in (Ball and Wood, 2006). This means it is necessary to imagine the future so that we can make decisions about how much intrusive surveillance is acceptable. In the United States, EM technologies are already used to monitor the whereabouts of elderly victims of dementia and also for sex offenders who have completed their sentence but who are still considered to present a threat to the public. This presents two new avenues for development in the commercial surveillance industry. While monitoring the whereabouts of the elderly has long been identified as a target market for the EM industry, monitoring offenders after release represents a further extension in the net of social control through lifelong surveillance.

Craig Paterson is a Senior Lecturer in Criminology at Sheffield Hallam University.

References

- Ball, K. and Wood, D. (2006) *A Report on the Surveillance Society for the Information Commissioner by the Surveillance Studies Network*. http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_summary_06.pdf.
- Campbell, S. (2002) *A Review of Anti-Social Behaviour Orders: Home Office Research Series 236*. London: Home Office.
- Cohen, S. (1985) *Visions of Social Control*. Cambridge: Polity.
- Donzelot, J. (1980) *The Policing of Families*. London: Hutchinson.
- Home Office (2007) *Anti-Social Behaviour Orders – Statistics*, www.crimereduction.gov.uk/asbos2.htm.
- Mair, G. (2005) 'Electronic monitoring in England and Wales: evidence-based or not?' *Criminal Justice*. 5 (3):257-77.

Securing the Neurocity

David Murakami Wood warns that cities could be transformed beyond recognition by hi-tech surveillance if protocols are not put in place.

The most highly developed cities are on the brink of an enormous and potentially fundamental transformation. Described as 'pervasive' or 'ubiquitous computing', 'ubiquitous media', or 'ambient intelligence', the 'combining of virtual and material worlds', or the emergence of an 'Internet of things', this transformation provides a basic neural infrastructure for the city in addition to the physical infrastructures of transport, sewerage, electricity and so on, with which we are familiar (Graham and Murakami Wood, 2006). Urban designer, Dana Cuff argues that these systems: 'challenge some of our fundamental ideas about the subjectivity, visibility, space, and the distinction between public and private... [and] reformulate our conception of the civic realm' (43). The Neurocity is coming.

Surveillance and the Neurocity

The UK, with more than 4.2 million CCTV cameras, has become a 'model' for the implementation of urban security by other nation states. Britain was particularly significant in implementing not just CCTV itself, but also new automated recognition technologies. Automatic number plate recording (ANPR) cameras were installed in the City of London in 1997, as part of a process which transformed the Square Mile into the most surveyed public space in the world (Coaffee, 2004). The ANPR technology was subsequently extended from February 2003 for use in the Congestion Charging scheme, which is now being extended nationwide with the ANPR system operational by 2008 (Norris, 2006).

The creation and connection of databases is not simply a commercial obsession but is also a key strategy of UK police forces with new databases of DNA samples.

The relationship between surveillance, space and people continues to be transformed with the advance of multiple biometric technologies such as facial and iris recognition, based on software algorithms, some of which can be linked into the new digital CCTV (Intona and Wood, 2004). At the same time, the surveillance of individuals has gone hand in hand with the amassing of huge amounts of personal information in databases. This is a step-change from the world of the paper file: computer databases allow greater integration and automated algorithmic operations to be performed effectively in real-time,



Photo: Julie Grogan

Our cities could change completely with hi-tech surveillance.

and without the bodily subject necessarily knowing (Graham and Wood, 2003). Large divisions remain between real bodies, movement and behaviour, and databases. However three trends could all change these divisions very rapidly.

Firstly, the creation of personal information profiles combining different sources of data with algorithmic analysis to look for particular patterns

that might indicate a potential danger or profit opportunity which can be pre-empted, are becoming more common. The creation and connection of databases is not simply a commercial obsession but is also a key strategy of UK police forces with new databases of DNA samples (and new powers to fill them), digital facial images and more all linked through an expanded and more capable Police National Computer (PNC), potentially linked in real time to the hand-held 'tablet' PCs of officers on the streets.

Continued on next page

Secondly, conventional surveillance technologies are becoming more *mobile* by being combined with robotics or with remote control aviation technologies to make Unmanned Aerial Vehicles (UAVs). These have been in use by the US military for some years

and situations not necessarily linked or operating with the same rationale. Whether by multiple friendly watchers, little sisters or by Big Brothers however, we are increasingly leaving our traces for others to follow, we are increasingly known in many different

Whether by multiple friendly watchers, little sisters or by Big Brothers, we are increasingly leaving our traces for others to follow, we are increasingly known in many different and unexpected ways.

- currently the best-known example is the 'Predator' reconnaissance drone aircraft used in Iraq. However, in Los Angeles, still the laboratory for urban control, police are already experimenting with small remote controlled spy planes called 'SkySeer'. Many uses have been suggested in the UK.

Thirdly, 'pervasive computing' will allow the creation of almost invisible networked forms of automated surveillance. Already Radio-Frequency Identification (RFID) tags are becoming common, and are already embedded in goods, animals and most recently human volunteers (Murakami Wood 2007 forthcoming). But this is already outdated: so-called 'smart dust' has been developed in several university and corporate research laboratories, notably at Berkeley, and now marketed through Dust Networks which offers 'self-organising wireless technology' based on networks of tiny 'motes' made up of millimetre-sized packages of sensor, computing and communication devices which according to their website, will 'extend monitoring and control deeper into the physical world'.

This network of fixed or mobile devices, able to locate, communicate with each other, with people, and with databases in real time, provides the potential for the emergence of the 'Neurocity'. 'Neurocities' will work by new spatial 'rules' which, not surprisingly, resemble the highly-structured protocols (Galloway, 2004) by which distributed computer communication architectures function. However this does not offer us much protection. Haggerty and Ericson claim that the new surveillance results in the progressive 'disappearance of disappearance', with the anonymity previously afforded by the city increasingly elusive. However this trend is reinforced by the increasing use of pervasive computing and surveillance technologies for social networking and even 'whole life logging': people, and especially younger people, increasingly want to be exposed to others. This makes concepts based on rights, such as privacy, increasingly difficult to sustain as a basis for organising opposition, or even simply debate.

However, the Neurocity need not be the totalitarian society of George Orwell's Airstrip One, with one omniscient controller. Bruno Latour has described the current order as *oligoptic*, that is made up of multiple surveillant actants with very detailed specific knowledge of very confined areas. We move constantly between different highly surveyed spaces

and unexpected ways.

We need to be far more knowingly involved in shaping the protocols which will determine the room for manoeuvre we will have in the future Neurocity, otherwise we might wake to not just a surveillance society but to cities that will soon be more aware than we are.



Dr David Murakami Wood, is based at the Global Urban Research Unit (GURU) at Newcastle University,

References

Coaffee, J. (2004) 'Rings of steel, rings of concrete and rings of confidence: designing out terrorism in central London pre and post 9/11', *International Journal of Urban and Regional Research*, Vol. 28.1, 201-11.

Graham, S. and Murakami Wood, D. (2006) 'Software-sorted Cities.' Expert Report in Murakami Wood, D. *et al.*

Graham, S. and Wood, D. (2003) 'Digitising Surveillance: Categorisation, Space, Inequality', *Critical Social Policy*, 23(2): 227-248.

Murakami Wood, D. (forthcoming, 2007) 'Towards Spatial Protocol: The Topologies of the Pervasive Surveillance Society', commissioned for a special issue of *Social and Cultural Geography*.

Murakami Wood, D. (ed.), Ball, K., Graham, S., Lyon, D., Norris, C., and Raab, C. (2006, revised and reissued 2007) *A Report on the Surveillance Society*, Wilmslow, UK: Office of the Information Commissioner / Surveillance Studies Network.

Norris, C. (2006) 'Criminal Justice.' Expert Report in Murakami Wood, D. *et al.*

Stolen identities

Jennifer Whitson and Kevin D Haggerty argue that companies' zest for customer data and the huge growth in e-commerce is exacerbating the problem of identity theft.

The thwarting of identity theft preoccupies most modern institutions. And while identity theft is a criminal act, the most common responses to this crime fall outside of the legal system.

At the most general level, identity thieves manipulate someone's personal information to secure some benefit. They can acquire this data from dumpsters, customer service representatives, trojan horse computer programs and by stealing computers or hacking into corporate databases. Victimization ranges from the single instance credit card fraud to more elaborate, extended uses of a person's documentary identity.

Commonly recognised as the most rapidly rising crime in both North America and the United Kingdom, the latest Home Office estimate is that identity theft costs the UK economy £1.7 billion per year, while in the United States, the Bureau of Justice Statistics estimate that in the second half of 2004, over 3.6 million households learned that they had been victims of identity theft (Bureau of Justice Statistics, 2006; Home Office Identity Fraud Steering Committee, 2006).

information. In the case of American Express, for example, this can include access to a client's credit report and highly codified data on their lifestyle and consumption patterns. Such information purportedly allows major financial institutions to differentiate in real time between legitimate and suspicious transactions. In a trend that mimics the increased use of profiling in criminal justice, private institutions use such data to subject consumers to heightened scrutiny on the basis of their relationship to statistical consumption profiles.

By simply carrying out routine daily activities, an individual also potentially exposes their personal data to identity thieves. Increasing awareness of these risks has pushed target hardening and 'responsibilisation initiatives' to the forefront of measures to counter identity theft. The specific measures that are advocated are constantly evolving, but some of the more familiar responsibilisation strategies involve encouraging individuals to keep personal information private. They are reminded to carry a minimum amount of credit cards and identifying information. Passwords should be added to bank accounts, credit

In a trend that mimics the increased use of profiling in criminal justice, private institutions use such data to subject consumers to heightened scrutiny on the basis of their relationship to statistical consumption profiles.

Identity theft is related to wider changes in communication systems. As commerce has become increasingly informational, it depends ever more on reliable data which is used to avoid risk and maximize profits. Pervasive identity theft can increase the costs of verifying data and dealing with customers. It also risks undermining the public trust in the informational systems which are the cornerstone of e-commerce. Attuned to these dangers, institutions have responded to identity theft in four different ways: (1) making data collection more secure (2) disseminating consumer protection information, (3) offering new services and products, and (4) changing institutional security practices and technologies.

Government, law enforcement and corporations compile and analyse data on instances of identity theft in order to predict future trends, educate the public and lobby for legal reforms. The information is also used in forms of 'dataveillance', as institutions try to pinpoint and prevent identity theft as it is occurring. To facilitate this data monitoring, institutions require access to more and more of a consumer's personal

cards and telephone accounts and these should be changed regularly. Consumers are encouraged to monitor their billing cycles and scrutinise bank and credit card statements as soon as they arrive. Creditors should be contacted immediately if bills are late or if documents contain errors. All items containing personal information should be stored in a safe (ideally locked) location. The iconic technology in this regard is the paper shredder. A generalised program of shredding is encouraged, encompassing receipts, copies of credit applications, insurance forms, medical statements, credit offers and magazine mailing stickers.

Such responsibilisation measures are augmented by anti-crime products and services such as safes, computer locks, firewalls and encryption software. Even household locks and alarms are being re-coded to foil identity thieves based on the awareness that burglars are now really seeking personal information. New services are marketed to reduce the impact of

Continued on next page

identity theft, including American Express's 'fraud protection guarantee' which ensures cardholders will not be liable for fraudulent charges or deductibles if victimized by identity thieves. Nonetheless, American Express still aggressively markets two types of insurance against identity theft, and cardholders are encouraged to purchase both to ensure maximum protection. Similar services are available from other financial companies, credit bureaus and insurance companies.

Responsibilisation efforts designed to reduce crime risks through personalised and market-based initiatives are often criticized for ignoring the social and institutional structures that facilitate crime. This is nowhere more apparent than in identity theft. Rather than identity theft being the result of the public being sloppy or irresponsible with their personal data, research suggests that most identity theft results from information lost through the careless data management practices of major institutions. More than 50 per cent of stolen identities involve thefts by employees or people impersonating employees. Other research has noted that up to 70 per cent of identity theft can be traced to leaks that occur within organizations (Collins and Hoffman, 2004: 6; Jewkes, 2002). While some companies are now attuned to the potential public relations nightmare that can result from lax data handling practices, the informational security of the major institutions that compile and hold vast quantities of the public's personal data have consistently been found to be wanting. Not only have these institutions been slow to respond to identity theft, but many have actively fought measures designed to reduce such crimes as they would necessitate costly upgrades to security technologies or practices that might harm their profit margin. This situation results in companies calculating the costs of upgrading security protocols versus the costs of not doing so, and occasionally gambling with their customer's private information (Sullivan, 2004).

Rather than contemplate measures to reduce our reliance on these proliferating informational identities, ever more detailed documentary identities are instead being entrenched, combined and triangulated to establish a person's true identity. Following this logic, personal information needs to be more detailed than in the past — an assumption that encourages the development of new forms of official documentation and further scrutiny of a person's informational profile. In the process informational security measures are poised to become more elaborate and intrusive as they simultaneously reproduce the institutional reliance on personal information that has ultimately made identity theft possible.

Kevin D Haggerty is Editor of *The Canadian Journal of Sociology*, Professor of Criminology and Sociology, University of Alberta, Canada.

References

- Bureau of Justice Statistics. (2006) 3.6 million U.S. households learned they were identity theft victims during a six-month period in 2004. <http://www.ojp.usdoj.gov/bjs/pub/press/it04pr.htm>.
- Collins, J. M., and Hoffman, S. K. (2004) *Identity theft victims' assistance guide: The process of healing*. New York: Looseleaf Law.
- Home Office Identity Fraud Steering Committee. (2006) Identity theft: Don't become a victim. <http://www.identity-theft.org.uk/>.
- Jewkes, Y. (2002) Policing the net: Crime, regulation and surveillance in cyberspace. In Y. Jewkes (Ed.), *Dot.Cons: Crime, deviance and identity on the internet* (pp. 15-35). Cullompton: Willan.
- Sullivan, B. (2004) *Your evil twin: Behind the identity theft epidemic*. New Jersey: Wiley.

Jennifer Whitson is a PhD Candidate in the Department of Sociology and Anthropology at Carleton University, Canada.

Dilemmas of privacy and surveillance: challenges of technological change

Nigel Gilbert looks at future advances in electronic data collection and surveillance and urges engineers and government to work together to maintain the public's trust.

Increasing amounts of electronic data about individuals are being collected as we go about our daily lives. This is beneficial when it means, for example, easier access to medical records at the time and place they are needed, better personal security against theft and violence, and more precisely targeted supermarket special offers. But these benefits come at a cost; there is always a trade off between data collection and preserving our privacy. In a recent report, a Royal Academy of Engineering working group argues that one can have security, convenience *and* privacy – if good engineering principles are followed. The report, *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (available electronically at <http://www.raeng.org.uk>), raises a number of issues which government, privacy specialists and the public need to consider.

Identification and authentication

For many electronic transactions a name or identity is not needed; just an assurance that one can pay or is eligible for the service. In short, authentication (do you have the right to perform some activity?), not identification (who are you?), should be all that is required. Services for travel and shopping can be designed to maintain privacy by allowing people to buy goods and use public transport anonymously. It should be possible to sign up for a loyalty card without having to register it to a particular individual

and the like should be required to make copies of personal credit ratings available annually without charge, as is now the case in the United States.

Planning for failure

Another issue considered in the Report is that in the future there will be even more databases holding sensitive personal information. As government moves to providing more electronic services and constructs the National Identity Register, databases will be created that hold information crucial for accessing essential services such as health care and social security. But complex databases and IT networks can suffer from mechanical failure or software bugs. Human error can lead to personal data being lost or stolen. If the system breaks down, as a result of accident or sabotage, it is possible that millions could be inconvenienced or even have their lives put in danger.

The Report calls for the Government and corporations to take action to prepare for such failures, managing the risks in a planned and considered way. It also proposes that individuals who are affected by foreseeable disasters should be entitled to receive compensation.

Surveillance cameras

The report also investigates the changes in camera surveillance. CCTV cameras are increasing in resolution, record in colour and generate digital

Evidence from Home Office and other research is that cameras are poor at preventing crime, although they can be used to identify criminals after the event.

and consumers should be able to decide what information is gathered about them. The same is true for many other services where information is collected, often without good reason, or for reasons that appeal to the organisation collecting the data, but which give no benefit to the consumer.

The Royal Academy of Engineering Report suggests that the government could regulate this and other matters through a 'digital charter' that would clarify how personal information may be shared, the rights that individuals have to check and correct their data, and their right to opt out of having their data stored by businesses and the state. One of its practical recommendations is that credit agencies

images that could be stored for a very long time. And predicted improvements in automatic number plate recognition, recognition of individual's faces and faster methods of searching images mean that it may become possible to search back in time through vast amounts of digital data to find out where people were and what they were doing. The UK has the highest density of surveillance cameras per head of population in the world. Often, these cameras are installed in the belief that they will reduce crime, but the evidence from the Home Office's and other research is that cameras are poor at preventing crime,

Continued on next page

although they can be used to identify criminals after the event. The report calls for greater control over the proliferation of camera surveillance and for more research into how public spaces can be monitored without undermining an individual's privacy.

A reasonable expectation of privacy

At present, legal decisions on privacy often hinge on what constitutes a 'reasonable expectation of privacy', and courts have to make a fine judgement between the principles of Article 8 of the European Convention on Human Rights (Right to respect for private and family life) and Article 10 (Right to freedom of expression). Specifying what privacy is reasonable to expect will become harder as, for example, many

at present. The Report calls for more experiments in, for example, permitting the public to see what surveillance cameras are viewing and recording; more transparency about what digital data is being collected by organisations; and more explanations of what is being done with that data.

Anticipating the future

We already have a good idea about what technologies will be on the market in the next 10 years, because that is the minimum time it takes from invention through to mass market penetration. The report looks at likely developments and classifies them according to their implications for privacy and surveillance. It suggests some areas where current

The watched should be able to see what the watchers are watching.

more people carry mobile phones incorporating high-resolution cameras and it becomes easy for amateur photographers to distribute their work on the internet. There needs to be a more stringent public consensus about what degree of privacy is reasonable, and tougher penalties for those who offend against data protection legislation.

Profiling

One of the most important uses to which digital data is put is profiling: large databases are 'mined' to build up profiles of common patterns of behaviour. For example, a database of all transactions carried out in a store might be used to identify a number of typical purchasing profiles, ranging from 'young family' to 'older woman living alone'. Customers can be assigned to one of these profiles and appropriate special offers targeted at them. Such profiling has advantages if the offers are to the benefit of the customer, but there is a danger that it can simply reinforce disadvantage and cement prejudice. Profiling is never completely accurate and becomes particularly problematic when people are wrongly classified. Citizens can find themselves stigmatised as bad credit risks or as criminals, without their knowledge, and without any recourse just because their data matches a profile. The Report recommends that businesses that make offers to customers on the basis of profiles should be required to divulge that they have used profiling and it recommends that unfair profiling should be outlawed.

Trust and surveillance

The success of business and the acceptability of democratic governments depends heavily on maintaining public trust. Studies of what enhances trust often mention the idea of 'reciprocity': that there needs to be an effective channel of communication between organisations and their publics and that the 'watched should be able to see what the watchers are watching'. However, this is often not possible

and foreseeable technologies will probably need regulation and where new technologies need to be developed. For example, we should be examining ways of monitoring public spaces that minimise the impact on privacy. We should be devising secure ways of providing goods and services electronically that do not require identification. And we might think about ways of protecting personal information by adapting the digital rights management technology used to protect music and films.

Engineers' knowledge and experience can help to 'design in privacy' into new IT developments. But first, the engineering professions, the Government and corporations must recognise that they put at risk the trust of citizens and customers if they do not treat these issues seriously.

Nigel Gilbert is Professor of Sociology, University of Surrey.

Enver Solomon writes on recent developments in criminal justice.

Prolific and Other Priority Offender Programme

A focus on so called 'prolific and other priority' offenders has been a key part of the government's approach to criminal justice in recent years. It is based on the government's belief that a small number of offenders are responsible for a disproportionate amount of all crime. Since September 2004 prolific and other priority offender (PPO) programmes have been established across England and Wales prioritising and directing considerable resources to these offenders. The Home Office recently published an evaluation of the programmes which highlighted a number of key findings.

- **Offending and reconviction** – The evaluation found that there had been a 43 per cent reduction in the offending of the entire PPO cohort when comparing the total number of convictions in the 17 months before and following the PPO programme. It also found that there had been a reduction in the rate of their offending after starting the programme. However, the evaluation concluded that the specific impact of the PPO programme on re-offending as distinct from other interventions and factors that may also have influenced offending levels amongst PPOs, was limited. It concluded: 'it is not possible to state the extent to which the reduction in offending observed in the PPO cohort is solely attributable to the PPO intervention'.
- **Offenders views and experience** – The majority of offenders were largely positive about the programme. They considered the programme to be more demanding and stringent than their previous criminal justice experiences. The majority also valued the additional support and interventions received as part of the programme.
- **Practitioners' views** – Overall, staff were positive about the scheme and its objective to both 'catch and convict and rehabilitate and resettlement' offenders.

The evaluation is available at www.homeoffice.gov.uk/rds/pdfs/07/rdsolr0807.pdf. A critique of the government's PPO strategy is provided in *Crime, persistent offenders and the justice gap* by Richard Garside, the director of CCJS, published by the Crime and Society Foundation at CCJS. It is available at www.crimeandsociety.org.uk/briefings/jgap.html.

Ministry of Justice

On 9 May the new Ministry of Justice came into operation. The Ministry takes over responsibility for the National Offender Management Service and sentencing policy from the Home Office. Policing, drugs, anti-social behaviour, the prolific and other priority offender strategy and overall crime reduction policy all remain in the Home Office.

It is interesting to note that although NOMS and sentencing policy moves to the new Ministry of Justice the Home Secretary will continue to play a major role. A statement outlining the organisational changes said: 'In order to maintain the Government's clear focus on public protection and crime reduction, the Home

Secretary will continue to have a core role in decision-making in this area, reflecting his responsibilities for crime reduction.'

At the same time a new all powerful cabinet committee on Crime and Criminal Justice, chaired by the Prime Minister is being created. It will play a pivotal role in determining future policy, as was highlighted by the government: 'The new Secretary of State for Justice will work with the Home Secretary, the Attorney General and other ministers to ensure flexible and effective responses to different types of crime, from anti-social behaviour, to serious and organised criminality, including through the expansion of summary powers. Government policy in this area will, in future, be decided by a new Cabinet Committee on Crime and the Criminal Justice System, chaired by the Prime Minister.'

To mark the launch of the new Ministry of Justice, two publications were unveiled. The first, *Justice – a new approach* by the first Secretary of State for Justice, Lord Falconer, is available at www.justice.gov.uk/docs/Justice-a-new-approach.pdf. The report states boldly: 'The Ministry of Justice is a new institution with a new approach. We are neither the ministry of prisons, nor are we the ministry for judges or lawyers. The new Ministry of Justice starts life from a simple premise – the justice system is here to serve the public. We must give the public the system it deserves'.

A second report, *Penal policy – a background paper* sets out the government's latest approach to tackling the continuing rise in prison numbers. The report sets out a series of policy proposals including:

- The Sentencing Guidelines Council to review whether guidelines currently 'fully reflect the principles set out in the Criminal Justice Act 2003' and to review how it currently functions.
- New arrangements to allow for 'non-dangerous prisoners' to be recalled to custody for a term of no more than 28 days.
- Plans for Suspended Sentence Orders to apply only to indictable offences, including either way offences, but not to summary (less serious) offences as is currently the case.
- Plans to test 'higher intensity community orders' as an alternative to custody for offenders who might otherwise get a short prison sentence of less than 12 months.

The report is available at www.justice.gov.uk/docs/Penal-Policy-Final.pdf.

Protection of Children from Sex Offenders

In June the Home Office published the conclusions of a wide-ranging review of the protection of children from sex offenders. The review sets out a number of new initiatives including:

Disclosure – There will be a duty on Multi-Agency Public Protection Authorities (MAPPAs) to consider the disclosure of information on offenders in every case. The presumption will be that the authorities will disclose information if they consider that a particular offender presents a 'risk of serious harm' to children. A pilot will also be established to provide a process for members of the public to register with the police child protection concerns relating to a named individual. If that individual is a convicted child sex offender and is considered a risk to the public, there is a presumption that the information will be disclosed to the relevant member of the public.

Treatment programmes – The Home Office intends to develop the use of greater drug treatment in combination with psychological treatment. It is also planning to provide more treatment opportunities for non convicted individuals concerned about their sexual thoughts or behaviour. Finally there are plans to look at the possibility of joining up prison and probation treatment programmes so that there is a continuation from custody into the community.

Technology – The use of satellite tagging and tracking to monitor high risk sex offenders is to be reviewed and compulsory polygraph (lie detector) tests for sex offenders are to be piloted.

Public information and raising public awareness – A community awareness programme is to be piloted to provide child protection advice and develop information to give parents and carers the necessary knowledge to help safeguard children. At the same time public awareness of how sex offenders are managed is to be enhanced by providing accessible, widely available information and ensuring the effective communication of the work of MAPPAs.

The full report, *Review of the protection of children from sex offenders*, is available at www.homeoffice.gov.uk/documents/chid-sex-offender-review-130607.

POSTGRADUATE CRIMINOLOGY AT MIDDLESEX UNIVERSITY, LONDON

- MA Criminology: Crime, Conflict and Control
- MSc Criminology with Forensic Psychology
- MA Youth Justice, Community Safety and Applied Criminology

Apply now to start next September, based at our Enfield campus in north London. Benefit from:

- The opportunity to attend three-day Common Study Sessions at other European universities
- The option to undertake an internship with a criminal justice agency or to undertake work based learning
- Close links with researchers at the Crime and Conflict Research Centre
- May be studied full-time (one year) or part-time (two years)
- Excellent career opportunities in the criminal justice sector.



**Middlesex
University**

Admissions Enquiries:

020 8411 5555

email: admissions@mdx.ac.uk

IT'S YOUR WORLD.

**WHAT WILL
YOU CHANGE?**

www.mdx.ac.uk

The Una Padel Award

The Annual Award Scheme from the Centre for Crime and Justice Studies

Through our work we come across a range of organisations and people working in the criminal and social justice sector. We are often struck by the dedication and commendable work that is carried out daily across the country. Often practitioners and organisations go unrecognised in terms of raising awareness about their work and achievements to a wider audience.

Una Padel, our director until 2006, was a tireless campaigner for social justice and penal reform. She was an inspiration to us and others and held practitioners and innovative work in the field in very high regard.

The Una Padel Award is launched to give recognition to outstanding and inspiring organisational and individual contribution in the field of criminal justice. It is also an opportunity to ensure that Una Padel's dedication, work and commitment continue to encourage and inspire practitioners in the field.

We are looking to reward unrecognised commitment, determination and potential. We welcome your nominations for people or organisations that you have come across in your work that have made a real contribution and change in areas of preventative work with excluded and disaffected young people, offenders, victims, prisoners and their families and other people at risk.

Selection of award winners

CCJS have invited a judging panel made up of CCJS staff and key people in the criminal justice sector, to select the award winners this year.

The award winners will be formally announced and presented with their award at the Centre's AGM in November/December 2007.

If you would like to receive further information or have some ideas of who to nominate please contact Julie Grogan at CCJS. Tel: 0207 848 1688. ccjs.enq@kcl.ac.uk for full details of the Una Padel Award and an application pack or visit our website: www.kcl.ac.uk/ccjs

About the Centre for Crime and Justice Studies

We are an independent charity at King's College London that informs and educates about all aspects of crime and criminal justice. We provide information, produce research and carry out policy analysis to encourage and facilitate understanding of the complex nature of issues concerning crime.

The Centre has a long and distinguished history and in this our 75th Anniversary we are continuing to both broaden our appeal and challenge assumptions about the way discussions around criminal justice are framed at present.

0207 848 1688 ccjs.enq@kcl.ac.uk

FORTHCOMING HOME AFFAIRS CONFERENCES

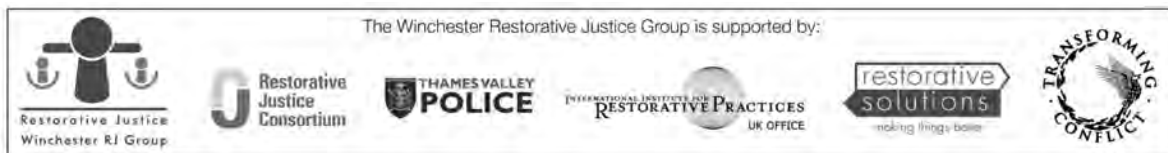
SEPTEMBER

2nd Annual Conference: Successful Employment and Resettlement of Ex-Offenders **Thursday 27th September 2007, Central London**

With contributions from leading Government figures, criminal justice agencies, employers, housing agencies and the voluntary sector, this important national conference will set out how to develop programmes that will impact positively on ex-offenders and help them re-build their lives.

OCTOBER

Fourth International Winchester Restorative Justice Conference **Restorative Justice: When, Where and How it Works** **Wednesday 10th – Thursday 11th October 2007, Winchester Guildhall, Winchester SO23**



Bringing together leading experts from across the world as well as the UK, the conference will provide a key opportunity for delegates at all levels of knowledge of restorative approaches to learn how to apply and implement these principles to achieve real change in attitudes and behaviour.

Conference website: www.neilstewartassociates.com/rj2007

Annual Tackling Anti-Social Behaviour Conference **Wednesday 17th October 2007, Central London**

Bringing together representatives from local authorities, the police, probation youth offending teams, town centre managers and the Home Office, the conference will consider what action can be taken to tackle anti-social behaviour at a local level including how to minimise the effects of drugs and alcohol misuse, housing for troublesome families, and the Neighbourhood Policing Programme.

4th Annual Conference: Vulnerable and Intimidated Victims and Witnesses **Wednesday 31st October 2007, Central London**

Bringing together representatives from groups that provide care and assistance for victims and witnesses, the courts, the police and probation service, the Witness Service, voluntary organisations, social services and other key stakeholders, this national one-day conference will explore how to provide better support for vulnerable and intimidated victims and witnesses.

NOVEMBER

Annual Youth Justice Convention 2007 **Tuesday 13th – Wednesday 14th November, Bournemouth International Centre**



This is the leading policy and networking event for all those committed to tackling youth crime. This year, the Convention programme will explore the relationship between protecting the public, protecting vulnerable young people and reducing the risk of re-offending in all aspects of the youth justice system.

View the speaker line up and register online: www.neilstewartassociates.com/yjc07

6th Annual Domestic Violence Conference **November 2007, Central London**

For further information on any of these conferences please contact **Sarah Spencer** on **020 7324 4359** or email sarah.spencer@neilstewartassociates.co.uk
View forthcoming conferences on our website: www.neilstewartassociates.com

CENTRE FOR CRIME AND JUSTICE STUDIES

Join us!

The Centre for Crime and Justice Studies at King's College London is an independent charity that informs and educates about all aspects of crime and criminal justice.

Our mission is to promote just and effective responses to crime and related harms by informing and educating through critical analysis, research and public debate.

Membership Benefits:

- Free subscription to our quarterly magazine Criminal Justice Matters, plus PDF copies, which provides expert up to date comment and analysis.
- Reduced rate subscription to the British Journal of Criminology, one of the world's leading journals in its field.
- Advance notice of our policy briefing papers.
- Discounts on publications.
- Free subscription to our quarterly CCJS bulletin with news of events and criminal justice developments.
- Access to our information service.
- Discounts, advance information and booking for our conferences.
- Priority booking for our free lecture seminar series and 'meet the speaker' receptions.

For membership details please contact Sylvia Kusi-Appouh at CCJS on 0207 848 1688, sylvia.kusi-appouh@kcl.ac.uk or complete the details below and send us your cheque today to CCJS, King's College London, Strand, WC2R 2LS.

Membership/CJM Application Form (Please complete in Block Capitals)

Full Name (including title)

Address

..... Post Code

Day Tel No.

Email address:

Occupation/Profession.....

I wish to become a member. Please circle subscription applicable

Payable by *Direct Debit* (Please ask us for form)

	UK	Rest of Europe	Rest of World
Ordinary	35	38	42
Student	25		

Credit/Debit Card Or by *Sterling Cheque*: Cheques payable to CCJS please

Ordinary	40	42	46
Full-time Student	30	32	38

(Copy of student card attached please)

Please send me CJM only for the next year

I enclose £25.00 UK

£35.00 Rest of Europe

£40.00 Rest of world airmail

<input type="checkbox"/>
<input type="checkbox"/>
<input type="checkbox"/>

Organisational Membership Rate

Charitable and voluntary sector	50
Public bodies, universities and statutory sector	100
Private companies and corporate sector	150

Cheques or BACS payments only

Signature Date

Notes for Contributors

- Each quarterly issue of CJM focuses on a special area of criminological interest. CJM 69 will cover '**Prevention**' and CJM 70 will cover '**Political Economy**'. Contributors are advised to discuss their ideas with Enver Solomon or Rebecca Roberts before submission. Please ring the office or email: enver.solomon@kcl.ac.uk or rebecca.roberts@kcl.ac.uk
- Articles (max length: 1200 words) should be jargon free, with no more than six references, and written to appeal to a well-informed, but not necessarily academic audience. Photos or illustrations are particularly welcomed. Publication, even of invited articles, cannot be guaranteed and we reserve the right to edit where necessary. Articles, letters and reviews can only be accepted on this basis.
- Editorial policy for CJM is determined by the editorial board, which is in turn accountable to, and appointed by, the council of the Centre. The views expressed by contributors are their own and are not necessarily the views of the Centre.
- CJM is sent free to all members of the Centre and additionally to a growing number of independent subscribers, both nationally and internationally. Advertising is welcomed. Please contact Julie Grogan on 020 7848 1688.

CRIMINAL JUSTICE MATTERS ISSN: 0962 7251
Number Sixty Eight, Summer 2007 Copyright 2007 CCJS.

Criminal Justice Matters is published by the Centre for Crime & Justice Studies,
School of Law, King's College London, Strand, London WC2R 2LS. Tel: 020 7848 1688 Fax: 020 7848 1689
E-mail: ccjs.enq@kcl.ac.uk Web-site: www.kcl.ac.uk/ccjs Registered Charity No. 251588

Editorial Board: Enver Solomon and Rebecca Roberts (Editors), Rob Allen, Hazel Croall,
Peter Francis, Penny Fraser, Barry Loveday, Rob Mawby, Andrew Sanders, Kevin Stenson, David Wall
Copy Editor: Diana Ruthven

Director: Richard Garside

Deputy Director: Enver Solomon;

Office Manager: Julie Grogan

Research Director: Roger Grimshaw

Membership & Events Co-ordinator: Sylvia Kusi-Appouh

Project Officer: Sunita Patel

Project Officer: Zoë Davies

Acting Director, Crime and Society Project: Will McMahon;

Senior Associate, Crime and Society Project, Sean Roberts;

Research and Policy Associate, Crime and Society Project, Rebecca Roberts;

Administrator, Crime and Society Project, Ed Brenton

Typesetting and production: Amberwood Graphics; Printing: Anglebury Press Ltd.

Unless otherwise indicated, photographs are illustrative only and their use in no way suggests any criminal association or involvement on the part of the subjects.

RECENT PUBLICATIONS

CENTRE FOR CRIME AND JUSTICE STUDIES

Law-abiding majority? The everyday crimes of the middle classes

Profedssor Susanne Karstedt and Dr Stephen Farrall

A briefing paper that explores the amount of law breaking committed by middle class life. It presents research based on a survey of nearly two thousand people in England and Wales.

Free

Knife Crime: Ineffective reactions to a distracting problem? - A review of evidence and policy

Chris Eades

A policy briefing paper report providing a comprehensive review of evidence and policy on knife crime.

Only available to download in pdf format

Ten years of criminal justice under Labour: an independent audit

Enver Solomon, Chris Eades, Richard Garside and Max Rutherford

A wide ranging independent assessment of the government's record on law and order looking at the progress of the criminal justice system since 1997 against many key targets.

£20.00

Debating Youth Justice: From punishment to problem solving?

Zoë Davies and Will McMahon (eds)

A collection of critical essays by leading experts from the UK and abroad analysing the youth justice system and responses to youth crime and anti-social behaviour in England and Wales.

£20.00

The use and impact of the Community Order and the Suspended Sentence Order

George Mair, Stuart Taylor and Noel Cross

The first independent examination of the new Community Order and Suspended Sentence Order introduced in the 2003 Criminal Justice Act.

£15.00

Community Sentences Digest

Enver Solomon and Max Rutherford

Invaluable comprehensive information and analysis about community sentences, their use and trends and the offenders who serve them.

£20.00

The use of the Community Order and the Suspended Sentence Order for young adults

Stephen Stanley

An analysis of how the new community sentences in the Criminal Justice Act 2003 are being used for young adult offenders.

£15.00

Poverty and disadvantage among prisoners' families

Rose Smith, Roger Grimshaw, Renee Romeo and Martin Knapp

Joseph Rowntree-funded research into poverty and disadvantage among prisoners' families based on interviews with family members and an evaluation of service provision. Available online only.

Welfare and punishment

Professor David Downes and Dr Kirstine Hansen

Published by the Crime and Society Foundation project at CCJS this report explores the relationship between welfare expenditure and levels of punishment. It presents research on welfare spending and imprisonment rates across 18 countries, including the UK.

Free.

Does criminal justice work? The 'Right for the wrong reasons' debate

Richard Garside and Will McMahon (eds)

In 2006 the Crime and Society Foundation project at CCJS published online *Right for the wrong reasons* and sought responses to the argument. *Does criminal justice work? The 'Right for the wrong reasons' debate* incorporates responses from a number of political, public policy and academic commentators.

£15.00

All the reports are available to download from the CCJS website www.kcl.ac.uk/ccjs or from the Crime and Society Foundation website www.crimeandsociety.org.uk.

Hard copies are available at the full price.

For all CCJS members there is a 25 per cent discount.

To order a copy of any of these publications or enquire about CCJS membership please e-mail ccjs.enq@kcl.ac.uk.

CENTRE FOR CRIME AND JUSTICE STUDIES

School of Law, King's College London, Strand, London WC2R 2LS. Tel: 020 7848 1688 Fax: 020 7848 1689

E-mail: ccjs.enq@kcl.ac.uk Web-site: <http://www.kcl.ac.uk/ccjs> Registered Charity No. 251588