

whereabouts all along, thanks to a GPS (global positioning satellite) system picking up the suspect's mobile phone transmissions. Not only did this allow the police to triangulate the phone's location to within a few metres, but they were reportedly able to activate the phone even when it was switched off. In addition, the police alerted credit card companies so that an alarm was automatically triggered when the suspect used his credit card to buy airline tickets. Meanwhile, police in his home town were examining his personal computer where they found downloaded child pornography, and his criminal records which revealed that he had previously been charged with molesting a 12-year-old child in the US. In Wigan, Shevaun's computer was also examined, and it was discovered that, unbeknown to her parents, she had been in communication with the American for over a year. Perhaps most bizarrely, it was reported that the former marine had planned the abduction with military precision. Forensic analysis of his computer apparently revealed that his rendezvous and escape with Shevaun 'smacked of special forces "in-hit-out" tactics' (2003).

These are just two examples demonstrating that surveillance is far from a unitary technology and hasn't always relied on social media. They happen to be two high-profile criminal cases, but even when we confine our discussion to the mundane monitoring of 'ordinary' citizens by government agencies, as discussed previously in relation to the NSA and GCHQ, we are in fact referring to a nexus of computers, telecommunications and people. Taken together, these networks are said to constitute a '*carceral society*' (Foucault, 1977), whereby more and more aspects of life are becoming subject to the kind of disciplinary power that we usually associate with the prison. Moreover, these systems of discipline and domination are driven by a common set of motives and desires on the part of those who instigate and operate them. In a slight modification of Haggerty and Ericson's (2000) typology, these rationales for surveillance will be further explored in this chapter under the following headings: *control of the body*, governance and governmentality, *security* and *cybersurveillance*, *profit*, and *voyeurism* and entertainment.

Control of the body

A great deal of surveillance is directed towards monitoring, codifying and controlling the human body. Surveillance of specifically targeted groups can be achieved via an interface of technology and corporeality that can range from direct physical contact between flesh and technological device, to more oblique or covert methods of producing information (Haggerty and Ericson, 2000). The former would include the various forms of 'electronic tagging' that are now commonplace, such as securing an electronic tag round newborn babies' wrists or ankles in hospital which not only contains personal information about the child and its medical condition, but also triggers an

alarm if the infant is moved beyond a secure area. The electronic monitoring of offenders and those on probation, and the use of microchips inserted under the skin of pets to monitor their whereabouts, are also examples of the diversity of applications which exploit the flesh-technology-information amalgam. Less direct forms of surveillance that rely on distanced monitoring of corporeality include the computer monitoring of keystrokes to assess output and efficiency in offices and the visual surveillance of shop workers' body language to ensure that they are conveying the customer service ethos of their employer.

When it comes to techniques of identification, body surveillance extends beyond individuals and discrete groups to entire populations. In this respect, identity verification is achieved by means of 'biometrics', which are identification techniques based on physical attributes – fingerprints, palm scans, retina identification, body fluids and so on. In the global surveillance society, one is no longer identified by what one has (for example, a passport or credit card), or by what one knows (for example, a personal identification number or PIN), but increasingly by what one is – a collection of unique body parts (Aas, 2005). Ironically we have returned to the anthropometric preoccupations of the positivist school of criminology with their measurements of the body, skull and so on – albeit in a more sophisticated guise. There is, then, nothing intrinsically new about the 'informization of the body' (van der Ploeg, 2003: 58). Primitive forms of biometric identification have existed for centuries, and advancements in photography and fingerprinting at the end of the 19th century coincided with the centralization and bureaucratization of administration and record-keeping. In fact, fingerprinting is a good example of a form of surveillance that has lost a great deal of its stigma through familiarity and diversity of use. Once used uniquely by law enforcement agents to identify suspected criminals, with all the negative connotations that such an application would evoke, the use of fingerprinting has expanded to include privileged cardholders, frequent flyers, club members and library users (van der Ploeg, 2003). What is new is that forensics has 'lost' its body (Aas, 2005). Again, to take the example of forensic crime investigations, traditional fingerprinting is being superseded by 'genetic fingerprinting', otherwise known as DNA testing. Many criminal cases that had been consigned to police files years or even decades ago have been belatedly solved by recourse to DNA tests on items of clothing, weapons or other items touched by a suspect and which have been stored by investigators. But despite the fact that DNA provides a unique identifier that cannot be transferred between individuals, no system is foolproof. Even if an effective form of everyday personal identification incorporating DNA could be found, as with other technological advancements it is likely that the professional criminal and terrorist would remain one step ahead of the police (Jewkes, 2003a, 2003b). DNA can be cloned, 'planted' or, in the case of suicide bombers and terrorist 'martyrs', rendered irrelevant.

Governance and governmentality

A salient theme in the criminological literature on surveillance has been its contextualization within an 'actuarial' discourse. In other words, surveillance occupies a central role in a broad strategy of social control that has moved from being 'reactive' (that is, only activated when rules are violated) towards one that is 'proactive' (that is, tries to predict rule violations before they happen). Visual surveillance systems are thus seen as just one element within a raft of risk-calculating crime control strategies which also embrace risk assessments of 'dangerousness' in relation to prisoners and those on probation, a national register for sex offenders and the notification of communities about paedophiles in their midst, community safety partnerships undertaking local crime audits, and attempts to 'design out' crime in architecture and town planning (O'Malley, 2001; Stenson, 2001). Not only do surveillance systems underpin correctional policies, then; they have created a new mode of governance. The 'rehabilitative ideal' with its promise of 'treating' the sickness that causes individuals to offend, and its evocation of a benevolent state concerned to eradicate poverty, deprivation and hardship, dominated criminological discourse throughout much of the 20th century (McCahill and Norris, 2002). But in recent years, as concerns about crime and the perceived failures of the criminal justice system have intensified, those in power have retreated from any pretence of liberalism and adopted the language of authoritarian populism, using phrases like 'prison works', 'zero tolerance' and 'tough on crime' (Stenson, 2001).

The new discourse of governance is also reflected in the re-emergence of 'Classical' criminological theories that view crime as opportunistic and 'normal'; in other words, requiring no particular maladjustment on the part of the offender. The salience of these theoretical perspectives in recent years has been accompanied by a shift from policies directed at the individual offender to those aimed at 'criminogenic situations' including car parks, city centres at night, run-down neighbourhoods, poorly lit streets, subways, schools and colleges, shopping centres and football stadia. While one objective of the new *governmentality* is to develop methods of situational crime control, a related aim is to single out those who do not 'belong' in these environments and take pre-emptive action to exclude them. Thus, rather than attempting to tolerate, understand and rehabilitate the different and the dangerous, there has been an ideological shift towards the less expensive and simpler task of displacing them from particular locations and from opportunities to obtain goods and services; of restricting mobility and behaviour; and of managing them rather than changing them. These shifting attitudes are increasingly being seen not simply as attempts to govern crime but also to involve 'government through crime'; a new 'governmentality' (Simon, 1997). According to Stenson, it is targeted disproportionately at poor whites and ethnic minorities who are being

guardian.co.uk
DNA-assisted convictions
give the impression that DNA is a miracle
ACPO has admitted that only 33,000 of the 4.9 million crimes the police
recorded in 2009 were solved as a result of a match on the national DNA data-
base, a statistic that prompted one MP to describe as 'negligible' the rate of
DNA detections ([http://www.guardian.co.uk/politics/2010/jan/05/dna-data-
base-crime-police-vaz](http://www.guardian.co.uk/politics/2010/jan/05/dna-data-base-crime-police-vaz)).

Security and 'cybersurveillance'

There are two aspects of security commonly discussed in the criminological literature on surveillance: personal safety against crime (e.g. from assault by a stranger) and security against an act of terror. In relation to the former, one of the outcomes of the processes of governance and capitalism outlined above is that, as urban space has become progressively fragmented and fortified, the population that inhabits that space become subject to feelings of insecurity and paranoia. Despite the unwanted and undesirable being left in the spaces between the controlled urban spaces, there is a tendency for those who occupy the newly privatized public realm to nonetheless demonize them (Graham and Clarke, 2002). As discussed elsewhere in this volume, when difference and diversity are not tolerated, far less celebrated, the inclination to regard some people as 'other' and fear them as a result becomes more pronounced. In such a climate, visible surveillance technologies may further increase public anxieties and contribute to the image of public spaces as dangerous places. Paradoxically, the solution most frequently put forward to counter the public insecurity that is, in part, generated by the prevalence of surveillance systems is to introduce yet more surveillance systems. Hence, a greater level of exclusion is created and a 'fortress mentality' of segregation and ghettoization is reinforced. For example, personal and home security devices, including do-it-yourself CCTV systems, are increasingly commonplace in urban and rural areas alike. Architects and planners in Britain are following the American

Romanian... when he and his wife... of Iraq, Saddam Hussein, both created a culture of enforced eavesdropping that effectively amounted to a total surveillance society, with secret police mandated to employ rudimentary forms of torture to ensure that self-imposed censorship was upheld. But the Internet has taken whispering campaigns to a new and potentially dangerous level - described by Valier as 'transnational vengeful networks' (2004: 103) - as the man mistaken for child killer Jon Venables found when a Facebook page was created urging vigilantes to kill him. Moreover, the monitoring of communications by governments in the West might be seen as no more lawful, for all its high-tech gloss and covert methods, than the practices of Ceausescu and Saddam. As communications intelligence has moved its operations from narcotics trafficking, money laundering and terrorism to intercepting 'ordinary citizens' personal and commercial telex messages, mobile phone communications, e-mails and Internet traffic, notions of what is 'acceptable' in the interests of security are once again under scrutiny.

Profit

One of the most significant drives behind the expansion of surveillance comes from the companies who manufacture the hardware and software, many of which were once suppliers of military equipment, but have adapted to a changing global market. As the technology becomes more sophisticated, the commercial market for surveillance equipment sets to grow even further, with manufacturers of biometric access controls and facial recognition software among the most profitable. CCTV systems are themselves big business: in the period of rapid expansion of CCTV in the 1990s the UK Government invested 75 per cent of its crime prevention budget in CCTV schemes and in the 10 years to 2002 committed over a quarter of a billion pounds of public money to its expansion through the City Challenge Competition and Crime Reduction Programmes (Norris, 2003). In total around £500 million has been invested in CCTV in the UK, which makes it the single most heavily-funded

crime prevention measure operating outside the criminal justice system (Welsh and Farrington, 2008). Sadly, its impact on offending has been described as 'modest'; it is only in car parks that it has had any significant effect (ibid.). But while car thefts and break-ins may have declined as a result of CCTV, motorists are likely to be victimized (or criminalized, depending on your point of view) by other kinds of camera. According to one insurance company, 2 million drivers are caught speeding each year on roads (an increase of 328 per cent over a decade) and the fines generated from these cameras exceed £114 million every year (www.swiftcover.com/about/press/speed_cameras_cost/).

The desire for profit has interesting social implications. When Foucault (1977) developed his vision of surveillance as a form of hierarchical social control, he emphasized the power that panoptic surveillance techniques had over the masses, stating that surveillance did more than observe and monitor people. For Foucault, panoptic surveillance targets the soul, disciplining the working populace into a form of self-regulation designed to meet the requirements of the developing factory system (Haggerty and Ericson, 2000). However, Bauman (1992) argues that surveillance is becoming less about discipline and repression, and more to do with classifying individuals according to their conspicuous wealth and consumption patterns, seducing those deemed 'desirable' into the market economy. With the advent of networks of computers 'data mining' has become operational through the extraction of information about individual citizens and can be used to classify high and low value customers for corporations, in just the same way that it can be used to assess and rank 'high' or 'low' risk groups in relation to criminal behaviour (Coleman and Norris, 2000). There are three potential outcomes of this process. First, surveillance can be used to construct and monitor consumption patterns in order that detailed consumer profiles can be put together. Second, these profiles can then be used to predict future behaviour or consumption habits, lure customers to a rival organization, or even encourage people to buy items they may not otherwise have purchased, on the basis that they fit in with a pre-existing aspect of their lives. This increases potential profits for corporations based on knowledge of consumer behaviour in the name of 'efficiency' (Coleman and McCahill, 2010). Third, surveillance can be used to differentiate between populations, limiting the movements of some on the basis of their identity profiles, consumption habits or spending power. The meeting of certain criteria by desirable (i.e. relatively affluent) consumers might then determine anything from preferential credit ratings to rapid movement through customs and airports (Haggerty and Ericson, 2000).

These processes combine to create what Gandy (1993) terms the 'panoptic sort'; a situation in which *all* individuals are continuously identified, assessed and sorted into hierarchies which are then used to manage and control their access to goods and services. Furthermore, they have taken place against a backdrop of changes which have resulted in the supremacy of conspicuous

ments of post-modern purity'. These analogies recall the work of anthropologist Mary Douglas, who argues that the elimination of 'dirt' is a positive effort to organize the environment; dirt invites social control because it is perceived as a threat to order. There has also been, in recent years, a more literal manifestation of this idea, with restrictions in many city centres on litter dropping, alcohol consumption, smoking and traffic. McCahill further notes that in the city centre shopping mall he observed, banned activities included walking a dog, pushing a bicycle, eating, sitting on the floor and lying down. When CCTV operatives observed these kinds of behaviours, a patrol guard would be deployed to request that the miscreant 'position their body in a way conducive to the commercial image of the mall' (McCahill, 2002: 128). In this respect, the flawed consumers who come under surveillance in shopping malls are, quite simply, 'matter out of place' (Douglas, 1966: 2).

Voyeurism and entertainment

While many commentators argue that recent developments in systems of surveillance and social control have augmented an intensification of panopticism (where the few observe the many), an emerging theme in the sociological and criminological literature on surveillance has been that of '*synopticism*', where the many observe the few (Mathiesen, 1997). Synopticism has been accelerated by the proliferation of mobile phone cameras, which have led to a number of instances where members of the public have filmed events that were not 'meant' to be seen, or have simply arrived on the scene before journalists, and either posted the footage online or sold it to national television networks for broadcast around the world. For some, this is the essence of synopticism's appeal: 'surveillance footage represents one of the crudest satisfactions of the scopophilic drive, a sense of power at being privileged to see that which was meant to remain unseen: the point at which the private ... goes public' (Dovey, 1996: 127).

In fact, the drive is not only to look, but to be looked at. In the 21st century, to be watched elicits a positive as well as a negative response, a synoptic development which suggests that CCTV, video and webcam footage is as much about entertainment as it is control. The popularity of social networking sites such as Facebook, Instagram, Snapchat, LinkedIn and Twitter are testament to the desire to see and be seen. In addition, the 'reality TV' genre that surveillance,