

Crime and the Surveillance Culture

CHAPTER CONTENTS

NSA, GCHQ and the new age of surveillance	222
Panopticism	224
The surveillant assemblage	226
Control of the body	228
Governance and governmentality	230
Security and 'cybersurveillance'	232
Profit	236
Voyeurism and entertainment	239
From the panopticon to surveillant assemblage and back again	242
'Big Brother' or 'Brave New World'?: some concluding thoughts	243
Summary	248
Study questions	248
Further reading	249

OVERVIEW

Chapter 8 provides:

- An overview of recent revelations concerning the covert surveillance and spying activities of government agencies in the US and UK over their own citizens and the citizens of numerous other countries
- A consideration of the dominance of the panopticon as a metaphor for contemporary surveillance techniques.
- A discussion of the extent to which surveillance technologies and systems are linked to form carceral networks of disciplinary power.
- An exploration of the institutional rationales and motivations that have led to a dramatic expansion of surveillance over the last two decades.
- An analysis of the ways in which media and popular culture have helped us to conceptualize various forms of surveillance through their representation in newspapers, television, films, music, art and so on, and how the 'viewer society' that traditional and 'new' media have given rise to, synthesize panoptic and synoptic models of surveillance.

KEY TERMS

- | | |
|------------------------------|--------------------------|
| ■ carceral society | ■ profit |
| ■ control of the body | ■ security |
| ■ cybersurveillance | ■ surveillant assemblage |
| ■ governmentality | ■ synopticism |
| ■ panopticon and panopticism | ■ voyeurism |

NSA, GCHQ and the new age of surveillance

Vodafone reveals existence of secret wires that allow state surveillance

Vodafone, one of the world's largest mobile phone groups, has revealed the existence of secret wires that allow government agencies to listen to all conversations on its networks, saying they are widely used in some of the 29 countries in which it operates in Europe and beyond.

(*Guardian*, 6 June 2014)

Everyone is under surveillance now, says whistleblower Edward Snowden
People's privacy is violated without any suspicion of wrongdoing, former National Security Agency contractor claims.

✓
The US intelligence whistleblower Edward Snowden has warned that entire populations, rather than just individuals, now live under constant surveillance.

"It's no longer based on the traditional practice of targeted taps based on some individual suspicion of wrongdoing," he said. "It covers phone calls, emails, texts, search history, what you buy, who your friends are, where you go, who you love."

(*Guardian*, 3 May 2014)

Over the last 30 years, Western societies have experienced a rapid growth in the use of surveillance, to the extent where most citizens have come to take for granted that they are observed, monitored, classified and controlled in almost every aspect of their public lives. Such has been the volume of news about state surveillance and counter-surveillance in the form of whistle blowing by activists, military personnel, computer experts and former security employees, that such stories seem to have been circulating for a very long time. Indeed, it might appear scarcely believable that WikiLeaks, the online organisation that publishes 'secret', sensitive and classified information, only came to many people's attention in 2010 when the extent of war crimes committed by coalition troops in Afghanistan was published. Nonetheless, revelations such as those reported by the *Guardian* above, are shocking for the level of personal, intimate intrusion they claim is occurring. The disclosure by Vodafone that government agencies have been using its network to snoop on the conversations of its customers, represents the first time such an organization has publicly admitted both to initial complicity in surveillance and subsequent resistance to governments' demands for access to user data (*Guardian*, 6 June 2014).

The *Guardian* has been at the forefront of bringing revelations about the US's National Security Agency (NSA) surveillance activities to a global audience. In June 2013, Edward Snowden, a former systems administrator for the Central Intelligence Agency (CIA) and Defense Intelligence Agency (DIA), and then a contractor working for an intelligence and security company in Hawaii, allegedly downloaded 1.5 million secret files about the NSA's covert and highly controversial practices, before flying to Hong Kong to meet journalists. He then flew on to Moscow where he has been granted asylum while, in his absence, the US Department of Justice charged him with violating the Espionage Act, an offence punishable by 30 years in custody. Among Snowden's revelations were that the NSA, together with the British Intelligence Agency at GCHQ, collected the phone records of millions of citizens, accessed and collected data from Google and Facebook accounts via a program called Prism, mined personal data from smartphone apps such as 'Angry Birds', hacked computers, intercepted phone and internet communications (including those of foreign politicians attending G20 meetings), carried out offensive cyber-attacks and infected more

than 50,000 computer networks worldwide with malware designed to steal sensitive information, shared raw intelligence data with Israel in an information-sharing agreement, bugged offices of the European Union, spied on at least 38 foreign embassies using a variety of electronic surveillance methods, tapped the private phone of German Chancellor Angela Merkel, sifted through vast amounts of email and text communications of its own citizens and those of many other countries, and harvested millions of faces from web images for use in a previously undisclosed facial recognition database (www.businessinsider.com/snowden-leaks-timeline-2014-6). While these examples are fairly wide-ranging, they merely represent the tip of the iceberg (see website above for a full list of 'Everything we've learned in one year of unprecedented top-secret leaks'). Snowden's fate remains uncertain but, while the US Government have branded him a traitor and criminal, his alter-ego as patriot and hero have been underlined by his appointment, in February 2014, as Rector of Glasgow University.

At the time of writing, the scale of the US and UK Governments' surveillance programmes is still unfolding with new revelations being reported on a near-daily basis. A decade ago most academic scholarship in the field of surveillance was concerned with closed circuit television (CCTV), and experts could scarcely have envisaged how pervasive and invasive surveillance was actually becoming. Nonetheless, CCTV continues to ignite heated debate, perhaps largely because it was introduced on a rapid and grand scale in the UK with little or no public discussion. With the oft-cited estimation that the average person living and working in a major city could be filmed up to 300 times a day, surveillance became a cornerstone of the literature on 'target hardening', 'defensible space' and victimization. Some studies examined whether visual surveillance technologies such as CCTV were effective in cutting crime or whether they simply displace it to surrounding areas (with contradictory findings). Others focused on the capacity for visual surveillance systems to reduce public fears about personal safety. On the basis that these issues are dealt with at length in other books (for example Coleman and McCahill, 2010), this chapter will take a different approach and will discuss some of the key motivations behind the rapid expansion of surveillance and its potential for social classification and social control. The chapter will also attempt to blend voices from criminology with those of the most prominent writers in the fields of sociology and cultural studies. But first let us consider the primary motif that unites debates about surveillance across all academic disciplines: the Panopticon.

Panopticism

In the popular consciousness, many forms of surveillance are dominated by the figure of 'Big Brother', George Orwell's creation of an all-seeing, all-knowing,

invisible super-power. In academic discussions of surveillance, however, the dominant metaphor has been that of the *panopticon*, an image that lends itself especially well to discussions of surveillance technologies which allow some individuals to monitor the behaviour of others. The panopticon, developed by 18th-century reformer Jeremy Bentham, was an architectural design that could be used for prisons, schools, factories, workhouses and any other social institutions that required the management of large groups of people by a small number of individuals with authority over them. While Bentham's vision was essentially a benign one, the panopticon became a motif for punitive prison regimes, and although it is often written that Bentham's model was never realized, several prisons have been and continue to be constructed according to the broad principles of *panopticism*. In brief, Bentham's design consisted of a circular building with individual cells built around its entire circumference, and a central watchtower in which the activities of the prisoners could be constantly watched. A system of lighting that illuminated the cells but kept the inspection tower in darkness made it possible for just one person to monitor many inmates, each of whom knew they were under surveillance, but did not know exactly when. They were therefore obliged to behave as if they were being monitored at all times, and conformity and passivity were assured. The mental state of being seen without being able to see the watcher induced a fear that eliminated the need for visible deterrents or overt force.

Writing about the plague at the end of the 17th century, Foucault (1977) describes how certain areas of a town were cordoned off and kept under continuous vigil with guards inspecting every part of the town to ensure that no-one escaped to spread the disease further. Consequently, like the inmates in Bentham's prison, the town's population were not simply observed; the surveillance of them was designed to act as a deterrent, a caution to encourage them to behave in a certain way. Thus, for Foucault, Bentham's architectural design was not only a blueprint for future surveillance technologies which would allow a small, unseen few to observe the lives of the masses, it was also a means of dispersing control over a conforming, docile population.

The panopticon was subsequently appropriated by others following Foucault's example, who took the ideological concept behind the design and used it to demonstrate the potential of new communication and information technologies. Most notably, Stan Cohen (1985) has considered numerous manifestations of surveillance, including community penalties, neighbourhood watch, private security, and the use of public surveillance cameras, and argued that they have enabled the 'dispersal' of social control. Among the consequences of dispersal are the move to informal, private and communal controls which 'widen the net' of the formal system by bringing about 'an increase in the total number of deviants getting into the system in the first place' (Cohen, 1985: 44). At the same time there is a 'thinning of the mesh' which increases 'the overall level of intervention, with old and new deviants being subject to

levels of intervention (including traditional institutionalization) which they might not have previously received' (ibid.). In short, surveillance has a tendency to disperse and become operative in a wide range of social settings not merely found *within* the criminal justice state but also *alongside* it, and to subject a large number of individuals and groups to criminalization or being labelled as deviants who formerly would not have been (cf. Coleman and McCahill, 2010).

The surveillant assemblage

The pertinence of the panoptic model is obvious in relation to the widespread surveillance of private data and communications by governments as revealed by Ed Snowden. Panopticism has also been evoked to explain the insidious presence of CCTV although, as Norris and Armstrong (1999) demonstrate, the panoptic effects of CCTV systems are limited. Three shortcomings are highlighted. First, CCTV systems that operate in public spaces, such as streets, are impossible to monitor continuously and it is relatively easy for those intent on behaving deviantly to disguise their appearance or move outside of the camera's gaze. Second, even when deviance is observed, the ability to mobilize a rapid response is constrained. In most cases, CCTV operators themselves are not authorized to deal with incidents, and neither are they in a position to demand swift intervention by the police. Third, the disciplinary power of CCTV is only complete when one-way total surveillance is combined with additional information about the individual being monitored. Norris (2003) suggests that despite the massive expansion of CCTV surveillance in Britain, its operators' inability to routinely link a person's image to any more detailed knowledge or information about them, places a severe limitation on CCTV as a Panopticon; such surveillance is, as Haggerty and Ericson note, 'often a mile wide but only an inch deep' (2000: 618). To put it in its simplest terms, there is not much the police can do with a recorded image of an offence that has already taken place unless further data can be gathered about the offender – name, whereabouts, address, previous convictions and so on – hence the use that the police make of television programmes like *Crimewatch UK* in appealing to the public to 'fill in the blanks'.

However, depth, or intensity, of surveillance can also be achieved via the connection of different technologies (for example, digitized CCTV systems and computer databases) and institutions (such as the police and private security companies). In the second decade of the 21st century, social media profiles have become one of the primary sources of information about both offenders and victims and few criminal cases are reported without recourse

to the self-revelations posted by the individual concerned on Facebook and Twitter. Haggerty and Ericson refer to this convergence of once discrete surveillance systems as a '*surveillant assemblage*' and argue that we have witnessed the 'disappearance of disappearance' (2000: 619). This raises the interesting question of whether our electronic identities have taken precedence over our 'real' identities. Once information (be it visual or textual) about a person is entered onto a linked surveillance system, their identity is 'fixed' even if it is 'false'. In much the same way as a person's legal identity is constructed from a mass of facts taken from the beginning to the end of life – birth certificate, passport, employment histories, medical and dental records, criminal record, post mortem, and so on – a cumulative mass of documents that captures and fixes them (Finch, 2003, 2007; cf. Foucault, 1977), so an individual can be captured in a web of non-documentary, visual surveillance.

Writing well before the advent of social media, Mark Poster was prophetic when he noted that, increasingly, in any major serious crime investigation both the victim(s) and the suspect will have their movements, consumption patterns, reading tastes, personal contacts, sexual histories and various other aspects of their private lives compiled into a detailed 'dossier that reflects the history of his [sic.] deviation from the norm' (Poster, 1990: 91). But even before the ubiquitous Facebook was invented, information was coalesced and then made public knowledge via the mainstream media. For example, following the murder of *Crimewatch* UK presenter Jill Dando on the doorstep of her London home in April 1999, it was revealed that 14,000 emails were examined, 486 names in her Filofax were investigated, and 2,400 statements were taken. Stories about Dando's relationship with her fiancé and several of her previous boyfriends appeared in the tabloid press. Further depth of knowledge was achieved by means of additional layers of surveillance. For example, after CCTV footage showed a blue Range Rover speeding south of the murder scene shortly after the killing, 1,200 cars were traced (the result of which was that seven months later the murder team arrested a man on suspicion of the theft of such a vehicle). In the week following her death, police released CCTV footage of her shopping in Hammersmith on the morning of her murder, and also revealed that their 'prime suspect' had made his getaway on a number 74 bus, speaking on a mobile phone before disembarking at Putney Bridge. A year after her murder, on 25 May 2000, Barry George (who ultimately was found not guilty of the crime and was released from prison after eight years) was arrested following a period of intensive surveillance of his home.

Another early example that illustrates the depth of information which can be achieved when fragments of data are coalesced is the police hunt for 12-year-old Shevaun Pennington, who disappeared with a 31-year-old American in July 2003 after 'meeting' him in an Internet chat room. Following Shevaun's safe return home it was reported that, despite her family's pleas for information about their missing child and her abductor, the police had known their