High-Tech Solutions to Low-Tech Crimes? Crime and terror in the surveillance assemblage

Yvonne Jewkes describes anti-crime surveillance systems in political context.

On March 11th 2004 an al-Qaeda terrorist attack on Madrid left 202 people dead as 10 bombs were detonated simultaneously on four packed commuter trains. The explosives, hidden in sports bags and backpacks, were detonated by mobile phones with their alarms set to go off at 7.39 AM. Like the earlier al-Qaeda attack on the USA in 2001, the Madrid attack was a combination of low-tech planning (the terrorists were traced back to the shop where they had bought the mobile phones in their own names) and high-tech policing. The grim reality facing governments today is that terrorists belong to a special, though in many ways quite ordinary, class of criminal. They rarely have prior convictions, thus background checks are seldom revealing (Stalder and Lyon, 2003). They communicate with each other in barely coded messages. And for those willing to kill themselves in an attack, the most sophisticated law enforcement systems are not going to make a difference.

The panopticon

The effort to combat terrorism with technology has been stepped up since 9/11, but there is broad public concern that surveillance strategies designed to identify potential terrorists are being employed in more insidious ways to spy on the population at large, with the result that civil liberties are being undermined and personal privacy is a thing of the past. In academic discussions, the dominant metaphor has been that of the panopticon, Bentham's architectural design for any social institution (most famously, a prison) that requires the management of large groups of people by a small number of individuals with authority over them. The beauty of the design, from the point of the authorities, was that the watched knew they were under surveillance, but did not know exactly when, and were therefore obliged to behave as if they were being monitored at all times, assuring conformity and passivity. 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.

The panopticon is increasingly used as a metaphor for technological innovations including CCTV, internet service providers, ID cards, store loyalty cards, DNA databases, encryption, fingerprinting, hand geometry, eye scans, voice recognition, and digitised face recognition, among many others. It is via these advances in technology that the disciplinary gaze might be said to be stretching beyond the confines of closed and controlled environments such as the prison or the factory to encompass society as a whole (Foucault, 1977).

'Surveillant assemblage'

Yet the panoptic effects of digital systems are limited by the fact that, in contemporary manifestations, the disciplinary power of the panopticon is only complete when one-way total surveillance is combined with additional information about the individual being monitored. For example, 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 the panoptic value of the technology (Norris, 2003). Such surveillance is 'often a mile wide but only an inch deep' (Haggerty and Ericson, 2000). Depth, or intensity, of surveillance is thus achieved via the connection of different technologies (for example, digitised CCTV systems and computer databases), institutions (such as the police and private security companies) and people (individuals, groups and communities). Haggerty and Ericson (2000) refer to this coalescence of once discrete surveillance systems as a 'surveillant assemblage'.

Increasingly, in *any* major crime investigation fragments of data will be coalesced and both victim and 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 file that chronicles their deviation from the 'norm'. For example, following 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, it was revealed that, despite her family's pleas for information about their missing child and her abductor, the police had known their whereabouts all along, thanks to a GPS (Global Positioning Satellite) system that could pick 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 (Jewkes, 2004).

Systems of discipline and domination

This example demonstrates that surveillance is far from a unitary technology. Taken together, these networks of people and institutions are often said to constitute a 'carceral society' whereby the alliance of formerly discrete technologies into a surveillant assemblage is designed to create systems of discipline and domination (Foucault, 1977).

This bleak assessment has become of increased salience since 9/11. One of the developments causing concern to civil liberties groups in the aftermath of the attacks on the World Trade Center and the Pentagon is the passing of the *USA PATRIOT Act (The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act)*. A 342-page document which many in Congress profess not to have read, the Act gives federal officials greater authority to track and intercept communications both for law enforcement and foreign intelligence-gathering purposes. The provisions made in the Act are esoteric and wide-ranging: among other things, it requires DNA samples of convicted terrorists to be held on a database of 'violent convicts', gives the FBI powers to covertly obtain the transaction records for bookshops and libraries, internet service providers, telephone companies, casinos, travel agents and car dealers, and extends the 'foreign student monitoring program' to include flying, language and vocational schools. The Act has met with opposition from communities and legal officials, with some US District Courts ruling sections of it unlawful. Its critics claim it creates new crimes, new penalties and new procedures for use against American and non-American citizens. Under the guise of fighting terrorists, some believe that the primary purpose of Patriot is to perpetuate public fear within an atmosphere in which anything other than staunch support for the war on Iraq is considered unpatriotic and dangerous.

In the wake of 9/11, the climate of political and public acceptability has become more favourable to the idea of surveillance. For example, many governments – our own included – are trying to gain public support for mandatory 'smart' ID cards. But many criminologists and cultural commentators remain deeply apprehensive and, although surveillance has many and varied (and indeed benign) applications, it is state surveillance that remains of greatest concern. While current fears about terrorism may have mollified the general public into accepting a greater degree of surveillance (and there is no convincing evidence that this is the case), many political commentators, human rights campaigners and civil liberties organisations have expressed extreme disquiet about the licence that governments take in unstable times. For example, there was a political furore in 2002 when the British Home Secretary announced plans to permit every local authority and a number of other public bodies access to phone, email and internet data; powers that previously had been uniquely held by the police, M15, M16, GCHQ, Customs and Excise and the Inland Revenue. The fact that the Government was forced to withdraw the plan in favour of one that allows for the retention of data by internet service providers may do little to allay the fears of those who believe that Britain is already the most surveilled country in Europe, and that – in matters of security – where America leads, Britain will follow. ■

***Yvonne Jewkes** is Senior Lecturer and Director of Studies in Criminology at the University of Hull.*

References continued on page 43