Criminal Justice

London, Thousand Oaks
and New Delhi.
1466–8025(200108) 1:3;
Vol. 1(3): 251–276; 018478

Someone to watch over us:
Back to the panopticon?

RICHARD FOX
Monash University, Melbourne, Australia

Abstract

Are we becoming a surveillance society? Sophisticated devices and techniques have greatly enhanced the capacity of government to intrude into the lives of citizens. Many of the new forms of surveillance are well suited to the networked society. Technology now allows the compilation, storage, matching, analysis and dissemination of personal data at high speed and low cost. But the private sector is also involved. Simply by participating in modern commerce, individuals are significantly eroding their own privacy. While there may be broad public support for the preventive role of many forms of overt surveillance, there are also serious weaknesses in the legislative frameworks within which the monitoring of citizens by overt and covert means takes place. There are concerns about accountability, fairness and the effects on the privacy rights of those who may be unwittingly caught up in the process. The new forms of surveillance are evocative of the old in the use of surveillance as an exercise of power and discipline.

Key Words

• Australia • policing • privacy • surveillance • technology

Fears and anxieties about electronic surveillance, and critiques of or resistance to it, arise from—among other things—specific aspects of its panoptic character. Opponents of the 'new surveillance' deplore the fact that it depends upon categories, that no knowledge of the individual is required,

> that it is increasingly instrumental, that areas of personal life once thought to be inviolably private are invaded, and that it effectively erodes personal and democratic freedoms.
>
> (Lyon, 1994: 77)

1984 and all that

In 1983, the Australian Law Reform Commission released the report on its seven-year inquiry into privacy in Australia (Australian Law Reform Commission [ALRC], 1983). It deliberately did so on the brink of the year George Orwell had selected to set his famous book *Nineteen Eighty-Four*. Though the book was parody, it became symbolic of the manner in which the combination of authoritarian government, extensive bureaucracy and intrusive technology could be used to systematically undermine personal freedom and individual privacy.

The report was prescient in warning that privacy was already endangered in Australia and was more likely to be so because of:

- growing official powers to intrude into the lives and property of citizens;
- new business activities involving collection of data on individuals and surveillance of their practices and behaviour;
- new information technology in which the advantages of computerization could also be turned into a source of concentrated information and power in the hands of a few and in ways that were less subject to restraint than in the past; and
- the weakening of national boundaries and of sovereignty.

The Commission recorded that the speed with which technological advances were permitting intrusions into private life was not being matched by the efforts of law makers to provide some form of restraint and redress. Although the three-volume report did not use the word 'Internet', it particularly drew attention to the significance of the threats to privacy posed by new forms of telecommunication technology which facilitated cross-border exchange of information with far fewer checks and controls than the limited ones possible under fragmented domestic laws (Privacy Commissioner, 1994; Lyon and Zureik, 1996).

The image presented by the Australian Law Reform Commission to highlight its concern about the future of privacy was the world of *Nineteen Eighty-Four*. There privacy had been shattered by the ubiquitous two-way television screens monitored by a brutal central government. In enunciating this fear, the Commission was echoing warnings of those who, a decade before, had noted the intensification of surveillance in the community and had prophesied that the only limits to realization of a total surveillance society were those set by the capacities of the available surveillance technology (Rule, 1973).

Those capacities now exceed what Orwell thought necessary for his imagined surveillance society. This article explores the extent to which the

Australian Law Reform Commission predictions are being fulfilled and the degree to which privacy claims remain a barrier to over-surveillance in this new millennium.

Globalized threats

Both Orwell and the Australian Law Reform Commission foresaw that cross-border threats would be inimical to privacy interests, but the Commission was better at identifying the nature of the menace. For Orwell it was Oceania's permanent state of war with its global neighbours. Centralization of power and total surveillance was the strategic response of the state to its internal and external enemies. The Australian Law Reform Commission saw the combination of globalization and technological advances in data collection as the danger.

The Internet has since emerged as an expedient and uninhibited form of global communication. It promotes freedom of expression as a human right while disparaging any countervailing rights of privacy, and confidentiality. It is largely a law-free zone.[1] There is no global authority controlling it, no world-wide legislative regime formulating privacy, censorship, or criminal law standards binding on it (McCarthy, 1997) and no global police to respond to unlawful behaviour committed via it.[2] The Internet allows offences to be committed effortlessly by an offender in one part of the world against victims in another (McDonald, 1997; Grabosky, 1998a; Grabosky and Smith, 1998). Old forms of crime such as theft (Mann and Sutton, 1998) and fraud (Office of Strategic Crime Assessments (Australia), 1995; Smith et al., 1999; Australasian Centre for Policing Research, 2000; Grabosky et al., 2001),[3] pornography (Rimm, 1995; Ali and Biskup, 1996; Wallace and Mangan, 1996; Forde and Patterson, 1998) and incitement and new species not previously criminal such as cyber-terrorism (Flemming and Stohl, 2000), cyber-vandalism and cyber-stalking (Ogilvie, 2000) are taking advantage both of the global scope of the Internet and of weaknesses in the extraterritorial reach of the local criminal law. Standard forms of investigation do not work well in cyber-space, nor do conventional powers of search, seizure and arrest (Grabosky, 1998a; Minister for Justice and Customs (Australia), 2000).[4] The ready availability of powerful forms of cryptography compounds the problem by facilitating concealment of unlawful activities (Baker and Hurst, 1998). The Internet now offers a new and rich environment for crime. This in turn has generated demands for greater use of surveillance as a strategy for controlling unlawful activity that transcends jurisdictional boundaries.

Typical of international recognition of the growing tension between privacy interests and law enforcement objectives in a surveillance environment is the 1998 report on covert policing and human rights standards commissioned by the British section of the International Commission of Jurists (JUSTICE) (Colvin, 1998). It reported that police, customs and

other law enforcement agencies in the United Kingdom and elsewhere were turning to more proactive intelligence-led policing methods which involved reliance on modern surveillance devices to strengthen the hand of investigators. It identified four catalysts for the move in this direction: the growth of organized, sophisticated and serious transnational crime; a belief that proactive policing was more effective than reactive responses to such crime; the ready availability of low-cost technology which permitted massive amounts of data to be gathered, stored, matched, analysed and disseminated rapidly to others; and a need to supply such intelligence to other national and international policing and security agencies responding to similar types of crime (Colvin, 1998).

The report noted how little public debate had taken place on either the proper limits on such activities, or the legal framework for regulating them. The impact on the privacy rights of innocent individuals who might be swept up in surveillance operations was also neglected. Nor had there been adequate coverage of the extent to which the use of covert surveillance could be seen as subverting the rights of defendants to a fair trial (in Australia, see Bronitt, 1996, 1997).

It concluded that existing legislative and procedural frameworks in relation to those activities no longer provided the safeguards necessary to meet international standards of fairness and accountability. Since rights to privacy and a fair trial were included in the *European Convention on Human Rights* which was incorporated into British law under the *Human Rights Act 1998* (UK), these matters were being brought into sharp relief as police tried to respond effectively to new forms of complex crime while still aiming to maintain the confidence of the public and the courts in the fairness of the use of advanced surveillance systems (Uglow, 1999).

It must be stressed that the growth in surveillance under discussion in this article is occurring on a number of fronts, not all of which are the result of global threats (other examples are given in McBride, 1997). Ironically, some of the pressure for greater local use of surveillance has come from investigations into the police themselves. The Wood Royal Commission into the New South Wales police established in 1994 to investigate police corruption and later extended to report on police protection of paedophiles, called for a significant expansion of surveillance powers. These were seen as an alternative to police investigative practices which themselves were prone to corruption. The Commission's recommendations supported greater use of telephone interception, interception of computer communications, covert video surveillance and concealed listening devices (Wood, 1997).

Nor need the growth in surveillance be related to serious crime. Detection and prosecution of summary offences, particularly those arising out of the use of motor vehicles, has been the focus of much technical innovation. What these offences lack in gravity they make up for in frequency. The revenue benefit of installing automated monitoring systems which achieve high detection rates and contribute to the efficient collection of the

resultant fines has been enthusiastically embraced by government (Fox, 1995).

Advances in surveillance

As government continues to promote the application of modern technology to all aspects of the justice system (Parliament of Victoria, Law Reform Committee, 1999), it is understandable that policing agencies will follow suit (Congress, Office of Technology Assessment, 1995; Colvin, 1998; Grabosky, 1998b; Marx, 1988; Clarke, 2000a). Increased miniaturization of surveillance devices and other forms of sense-enhancing technology now allows investigators to capture evidence of suspicious activities from afar. They may select from apparatus such as the following.

Eavesdropping devices

These are designed to overhear and record private conversations or to intercept and store digital transmission of messages by techniques involving use of:

- Telecommunication interception and recording devices including ones which record the keying of telephone numbers.[5]
- Concealed miniature microphones and radio transmitters.
- Long-range microphones.
- Laser or microwave devices which can amplify window vibrations and convert them to audible sounds.
- Scanning of satellite transmissions by sophisticated computer software programs which search for key terms in phone calls, faxes, telexes, Internet messages and other electronic communications and computerized data irrespective of their local, national or international origins.[6]

Optical devices

These are devices which visually monitor activity. They include:

- Continuously monitored closed circuit television (CCTV) at fixed locations to observe and record events in high-risk areas.
- Lightweight compact and miniaturized TV cameras for video surveillance as an adjunct to individual criminal investigations.
- Traffic cameras coupled with radar or laser beams to measure and record vehicle speed and capture digital or film-based images of the offending and the recorded speed. Film in traffic cameras is being replaced by digital imaging which allows almost instantaneous transmission of images to a central location for evaluation and the issuing of penalty notices.
- Red-light cameras to record violations at traffic-light controlled intersections.

- Bus-lane cameras to identify vehicles travelling in restricted traffic lanes on the highway.
- Satellite-based imaging to locate illicit drug crops and other crime scenes.

CCTV is nowadays the most common form of both overt and covert surveillance affecting ordinary citizens. Already the efficacy of such devices has been extended by relying on infrared and light-intensifying devices so as to produce high-resolution digital images in low- and night-light situations. What was first used for security purposes in commercial settings to guard the perimeter areas of office buildings and factories, or to detect cheating and to resolve betting disputes in casinos (Manning, 1996), has become routine as a means of monitoring the use by the public of private spaces such as shopping malls and plazas, or in entertainment precincts, where higher crime rates prevail. Modestly priced video security systems are now available as standard fittings for new homes and apartments and are appearing in schools to deter vandalism, illicit drug use and schoolyard violence.

Digital imaging can now be augmented by recognition software which can automatically read vehicle registration plates, or can match faces or identify persons through other biometric characteristics.[7] Cameras can scan the faces in the crowd to compare the images with those of known trouble makers stored on a pictorial database. Databases of football 'hooligans' are being compiled, as well as ones on demonstrators, bank robbers and suspected illegal immigrants (Colvin, 1998; Fay, 1998; Williams and Johnstone, 2000).

Locational devices

These are contrivances that signal the location or track the movement of objects or individuals. A simple locational device is the mobile or cellular phone (Werdegar, 1998). More precise and sophisticated global positioning units linked to satellite navigation systems are now so modestly priced they can readily be adapted for inclusion in objects whose movements have to be monitored centrally and from a distance. Other locational devices include:

- *Beepers* which when attached to an object of interest (e.g. a consignment of illicit drugs) allows the object to be tracked as it is transferred from place to place.
- *Electronic vehicle tracking devices*. The 'e-tag' which is the recommended electronic device for installation in all vehicles using certain tollways in Australia is, in essence, an identifying and tracking device as well as one which records the fee to be charged for each use of the tollway (Whorlow and Compton, 1995).
- *Personal electronic tags*. These are electronic tags lawfully strapped to an offender's wrist or leg to monitor the person's compliance with bail conditions, a curfew order, probation, or a sentence of home detention (Fox, 1987; Lyon, 1994; Whitfield, 1997; Enos et al., 1999). Soon these

> 'tags' will be able to be given a miniaturized global positioning capability allowing the location of their wearer to be tracked precisely at all times. Such conditionally released persons may then be permitted to roam more freely in the community. Further miniaturization might make it feasible to implant locational micro-chips in an offender's body for the duration of the court order.

Policing the Internet

Attempts have been made to engage in routine surveillance of Internet communications by focusing on traffic passing through the computers of local Internet Service Providers (ISP). The United States has been lobbying hard for international agreements and harmonized national laws to make it possible to intercept legally any communication without delay and with minimal technical hindrance in the interest of combating serious crime.

United States federal legislation already calls for telecommunications agencies to ensure that their services are amenable to interception by law enforcement agencies (US, 1994).[8] Efforts are still being made to restrict public access to high-level cryptography programs so that communications cannot be wholly immune from lawful interception (Organisation for Economic Co-operation and Development (OECD), 1997). The UK government has now enacted legislation (UK, 2000)[9] which would require companies to install equipment to allow authorities to intercept and decode e-mail messages carried on their networks.[10] Intrusion can also be achieved in other more subtle ways.[11]

In November 1995, a memorandum of understanding was signed between 15 European Union member states (and later Australia, Canada and the United States) (EU JHA-Council, 1995) committing the signatories to facilitate surveillance by law enforcement agencies (including the security services) by meeting certain minimum requirements. These were designed to allow real-time access by authorized agencies to actual communications and call-associated data. Thus if a mobile phone is being used by a suspect, information on its geographical location must be supplied; and where compression or encryption is used by the ISP, the information must be supplied to the law enforcement agencies in a decoded form. Other aspects refer to keeping those targeted in ignorance of the interception and allowing for rapid responses in urgent cases.[12]

Building databases

It is not merely surveillance that threatens privacy interests, it is also the uses to which the information gathered can be put. The storage, retrieval and processing of information has been vastly improved. Extraordinarily large databases can be assembled and trawled to extract useful information or patterns. The Australian Transactions Reports and Analysis Centre (AUSTRAC)[13] relies on sophisticated software to spot anomalous patterns of financial activity indicative of suspect transactions and possible money

laundering within some 7 million financial transactions reported to it each year (AUSTRAC, 2000). The surveillance of populations in general, or of particularly targeted individuals, through analysis of the data trails generated by their activities has been described as 'data matching', 'data linkage' or 'dataveillance' (Clarke, 2000b). It allows separately collected and organized information to be compared and matched to allow the extraction of new knowledge about persons and their activities (Greenleaf, 1991).

The databases need not contain data that have been acquired by covert means. Nor need they be compiled by government. Databases are also assembled by private sector interests. The information is usually obtained in the course of a commercial transaction, but the consensual element is not always evident. A survey of the privacy performance of Australia's top 100 websites conducted at the request of the Australian federal government in 2000 indicated that although 72 per cent of the sites investigated collected personal information, only about 50 per cent had formulated a privacy policy. Less than 30 per cent informed users that specific information on them was being collected. Furthermore, 43 per cent of the websites which collected personal information did so without the user actively providing it (Williams, 2000). Failure to clearly spell out the possible further use of personal information for purposes different from those for which it was originally collected was also noted.

Interfaces also exist between centralized police databases and ones needed for service delivery or risk management in other areas of government such as mental health, social welfare and child protection (Ericson and Haggerty, 1997), or between the private and public sectors in areas such as insurance fraud. For both, risk minimization is the objective (O'Malley, 1999). Such an approach shifts attention from potential victims to potential offenders who, because of their 'profile', come under some form of 'categorical suspicion'. It is this preventive function of surveillance and data sharing that makes it so attractive to risk managers. But the consequences for those wrongly categorized as a risk, or whose label is maintained though no longer valid, are significant once the 'profile' is loaded into databases that never forget.

Data matching depends on consistent identification of people. Crime control would be facilitated if a compulsory personal identification system for all citizens was in place. In 1987 the Australian public rejected a proposed universal *Australia Card* (Greenleaf, 1987; Davies, 1992), but that victory was later undermined by the quasi-compulsory nature of tax-file numbers, Medicare numbers, the 100 point proof of identity required by law for opening bank accounts and the Australian business numbers essential for goods and services tax purposes. These identifiers allow data matching and profiling for revenue protection, public security and other purposes. New state and federal laws setting up DNA databases and authorizing the collection of samples from suspects[14] are yet another step

towards compiling unique identifiers for all citizens, or at least those who fall under 'categorical suspicion'.

Private sector surveillance

The privatization, corporatization and outsourcing of criminal justice functions is already well developed in Australia. There are private security firms, private prisons, outsourced community-based correctional services, privately run drug-offender rehabilitation centres and drink-driver retraining programmes (Victoria, Parliament, Public Accounts and Estimates Committee, 2000). Now private commercial interests which regard personal records as valuable commodities have begun to pose threats to individual privacy as surveillance enters the consumer sphere in ways which parallel those of government.

First, surveillance itself is a function which governments have been willing to assign to the private sector. For instance, in the state of Victoria the setting up and maintenance of traffic and red light cameras is being moved into the hands of private corporations (Victoria, Auditor-General, 2000, para. 3.4). Another instance is the practice of requiring banks and other financial institutions to report suspicious transactions to government, under financial transactions reporting legislation which is designed to deter money laundering, tax avoidance and serious crime (Commonwealth, 1988). The monitoring obligations which may fall upon financial institutions under federal and state laws concerned with the confiscation of proceeds of crime are similar.[15] Likewise, legislation mandating the reporting of suspected cases of child abuse by health and educational professionals is a surveillance function allocated to the private-sector in the interest of crime prevention.[16] Many government agencies have the power to demand that private sector entities disclose the personal or financial information of third parties in order to enforce the agencies' special statutory mandates. The Australian Tax Office and the Department of Social Security are obvious examples.

Second, quite apart from any such co-optation by government, the private sector has its own good reasons for keeping an eye on those with whom it does business. By gathering information about prospective customers and building files and profiles of them, business aims to reduce fraud and other fiscal risks as well as differentiating consumer preferences in pursuit of fresh markets. Industry has made good use of data on their customers gleaned from the information supplied by them in the course of routine electronic commerce (Rosen, 2000). It is also willing to exchange that information with other businesses via credit reference associations and the like as part of risk management. A person's bad record in one context is likely adversely to affect access to service in another both locally and globally. Though in Australia many aspects of that process are the subject of guidelines under the Privacy Act 1988 (Cth), the basic approach has

been to rely on industry self-regulation with minimal accountability to government.

Third, while private police have less scope lawfully to undertake covert physical surveillance of citizens than public police acting under warrant (Shearing and Stenning, 1987), private electronic surveillance of citizens by way of closed circuit television cameras is now common (Norris et al., 1998). As described above, CCTV is now almost a standard feature in commercial settings to deter property offences or disorder. The most rapid recent expansion of surveillance technology can be found in road traffic management which increasingly straddles both the public and private sectors. Operators of modern tollways on which fees are collected electronically, have access to information on users' names, addresses, dates of birth, drivers' licence numbers, car registrations and credit cards. It is almost impossible to travel on such roads without significant disclosure of personal identity. The ability of such systems to identify vehicles and persons and track their movements led the New South Wales Privacy Committee to warn that while these technologies may offer great benefits in terms of traffic flow and other efficiencies, there were significant unresolved privacy concerns (Privacy Committee of New South Wales, 1996–7).

Video surveillance in the workplace has become an issue as well. At the end of 1996 the New South Wales Privacy Committee recommended that the Listening Devices Act 1984 (NSW) be amended to include a definition of covert video surveillance and a prohibition on its use for measuring work performance, or in areas such as toilets, showers and changing rooms (Privacy Committee of New South Wales, 1995). Guidelines were also issued on the use of video surveillance in the workplace.[17]

The counter-claim of privacy

Why prioritize privacy?

Generally the resistance to over-surveillance is framed in the language of privacy. The rise of surveillance as an instrument of social regulation is said to be signalling the death of privacy (Whitaker, 1999; Garfinkel, 2000). It is claimed that privacy is an essential component of human dignity and a near-universal personal need (Bok, 1983). A significant degree of privacy is said to be necessary to satisfy each human's need for psychological and physical space within which intimate communications with others may take place and in order to maintain a sense of personal autonomy and worth.

Westin, in his pioneering work, defined it as 'the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others' (Westin, 1967: 12). However, the Australian Law Reform Commission in its *Privacy* report acknowledged that the concept was more complex and involved a

collection of related interests and expectations, rather than a single coherent idea (ALRC, 1983; Michael, 1994).[18]

Though claims to privacy as a fundamental human need have been given standing as a legal right in international instruments such as the European Convention on Human Rights 1950 and the International Covenant on Civil and Political Rights 1966 that recognition is qualified. It is accepted that interference with privacy can be justified in the interests of national security, public safety or the prevention of crime. But even these qualifications on privacy imply the observance of certain further basic rights of the subject including appropriate legal authorization and proof that there is a real need to use the power to invade privacy.

In arguing that the citizen's desire to be free from surveillance is a privacy interest, the New South Wales Law Reform Commission 1997 Issues Paper on *Surveillance* makes the point that there is no necessary connection between surveillance and the collection of information: 'In essence, privacy involves keeping oneself and one's affairs removed from public view or knowledge, even if the information so protected is itself not intrinsically sensitive' (New South Wales Law Reform Commission, 1997: 13).

The argument is that surveillance is intrusive and an erosion of privacy regardless of any information-collecting purpose. To regulate the use of personal information under data protection laws such as the *Privacy Act 1988* (Cth) does not address the more fundamental issue of surveillance and its authorization.

The principal argument for resisting expanded surveillance powers on privacy grounds, particularly where the individual is offered no choice about being observed or being the subject of a data file, is that widespread routine surveillance creates an abiding sense of communal unease in which awareness of such scrutiny tends to chill the exercise of accepted civic rights, such as freedom of movement, association, assembly and speech. Surveillance of citizens inhibits full participation in democratic society.

Doubt has also been expressed about the efficacy of some of the surveillance devices in deterring crime. Often they do no more than displace the offending to some other location.[19] The likelihood of 'function creep' is also relevant. Previously authorized arrangements for routine electronic surveillance of the public are now being applied to purposes and targets beyond those envisaged at the time of installation. Thus CCTV traffic-monitoring cameras have come to be used to keep an eye on street drug activities and other crime 'hot spots'. And what were originally intended for crime control can be readily redeployed against political protestors or trade unionists in industrial disputes. Their recorded participation in lawful agitation may result in them being labelled for future attention, and the risk of wrong or misleading information being used as the basis for unjustified decisions increases as the surveillance net expands.

Then there is the 'overkill' argument:

> [Surveillance] can also distort the relationship between citizens and police by producing an asymmetry of knowledge and consequent imbalances of power. Reliance on surveillance techniques for law enforcement inevitably results in a situation of overkill. Surveillance is usually justified as a means of detecting organised crime and crime such as drug dealing and paedophilia which supposedly involve extensive networks. These targets are sufficiently aware of the techniques being used to take countervailing action. This results in calls for even more intrusive surveillance with the development of something of an arms race between police and professional criminals and the privacy of the majority being sacrificed in the process.
>
> (New South Wales Privacy Committee, 1996–7: 15)

It is the accumulation of the various forms of surveillance and control that is seen as most threatening to individual privacy and freedom. It is not surprising that these moves in law enforcement are being accompanied by demands for better definition of the means of controlling potential misuse of the monitoring powers and a clearer enunciation of those civil liberties and human rights standards that are relied upon to counter-balance the view that, in fighting crime, the ends can always justify the means (Kirby, 1998). As the means by which privacy can be invaded proliferate, the importance of defining what are the legitimate expectations of privacy increases even though those expectations must allow for the public interest in surveillance when it is a necessary and proportionate response to serious crime.

Updating the controls

The 1998 JUSTICE report on surveillance, covert policing and human rights standards in the United Kingdom revealed that, in that country, some of the surveillance methods in use were completely outside any system of legal regulation. And even when there was some legal framework for their control, it failed tests of necessity and proportionality. The report called for a single regulatory system with separate codes of practice to cover the various types of surveillance activity.[20] The objective was to lessen the risk that major surveillance operations would be held to be unlawful by a court in the course of a trial and the evidence thus collected rendered inadmissible. It was hoped that such an approach would serve the public interest in permitting effective prosecution while still maintaining confidence in relation to what the police may lawfully do and their accountability in exercising such powers (Colvin, 1998).

Creation of a single regulatory system of this nature for Australia is complicated by the fact that constitutionally the country is a federation with power divided between the federal government and six politically autonomous states. The legal landscape here in relation to surveillance is chaotic. Until the 1970s the use of listening devices was unrestricted by law in Australia. Regulation of the various possible forms of surveillance of citizens and the relationship between laws permitting surveillance and

those supporting privacy is largely, but not wholly a matter of state law. However the federal government can regulate surveillance involving the telecommunications system through its constitutional power over telephonic and like services (Commonwealth 1900, s.51(5)) and has done so by placing restrictions on the use of telephone intercepts except as permitted under the Telecommunications (Interception) Act 1979 (Cth). Non-listening devices used in relation to commonwealth drug offences are governed by provisions in the Customs Act 1901 (Cth) while the Australian Federal Police have to look to the Australian Federal Police Act 1979 (Cth) in relation to serious non-narcotic crimes.

Recently the Telecommunications (Interception) Act 1979 (Cth) and the Australian Security Intelligence Organisation Act 1979 (Cth) were amended to extend their reach and to include forms of visual surveillance and tracking (Commonwealth, 2000; Waters, 1997). There are also relevant provisions at a state level. However it is to be noted that the restrictions on installation, use and maintenance of surveillance or tracking devices contained in the Surveillance Devices Act 1999 (Vic) and the requirement that a warrant be obtained to authorize the use of such devices, are declared not to apply to nominated federal officers in the performance of their duties as employees of the Australian Competition and Consumer Commission, the Australian Security Intelligence Organisation, the Australian Federal Police or in the enforcement of the Customs Act 1901 (Cth), or the Migration Act 1958 (Cth).

The surveillance functions associated with traffic management and motoring offences, and those undertaken by state and territorial police are governed by separate legislation in each state and territory.[21] So too is the licensing of private security and investigation agents or others who might install security alarm and surveillance systems.[22]

The competing interest in privacy is ordinarily a matter of state jurisdiction.[23] However, because the topic has been the subject of international agreements, the federal government has been able to legislate in that area in the exercise of its external affairs power (Commonwealth 1900, s.51(29)). The main function of the federal Privacy Act 1988 (Cth) is to protect personal information which is collected by federal government departments or agencies rather than impose a central regulatory system controlling surveillance. The Federal Privacy Commissioner has been asked to assist the private sector to develop appropriate forms of privacy protection through voluntary self-regulation in accordance with the privacy principles set out in the legislation and, in March 2000, the federal Attorney-General released the Privacy Commissioner's e-mail guidelines relating to the use of e-mail and web browsing in the workplace. These call for organizations to devise clear policies so that users logging on to a computer system are given notice of which activities are not permitted and who can access the content of their e-mail and web-browsing activities. These guidelines complement the government's Privacy Amendment (Private Sector) Act 2000 (Cth) which will require website operators who collect personal information on-

line to take reasonable steps to ensure that users know who is collecting their information and how it is used, stored and disclosed. Though the government considers this Act to be the most significant development in Australian privacy laws since the passage of the Privacy Act 1988 (Cth), its basic approach remains one of self-regulation. Furthermore, like most privacy legislation, the federal legislation contains significant exemptions for law enforcement agencies acting in the course of their duties.

There is no Australian equivalent of the United Kingdom's *Regulation of Investigatory Powers Act 2000* which makes provision for the interception of communications, the carrying out of surveillance, the use of covert human intelligence sources and the acquisition of the means by which electronic data protected by encryption or passwords may be decrypted or accessed. It also provides for the establishment of a tribunal with jurisdiction in relation to those matters including matters arising out of surveillance by the security service, the secret intelligence service and like agencies (Akdeniz et al., 2001).

Surveillance as social control

Is Big Brother dead?

A number of observers have commented on how the development of the modern state seems bound up with the growth of surveillance as a major mechanism of social control (Foucault, 1978; Giddens, 1987; Marx, 1988). Even though surveillance has long been a means of regulating communities (McMullan, 1998), the social control implications are the ones which seem to evoke most anxiety.

The nightmare presented by the Australian Law Reform Commission was that of Orwell's Oceania in *Nineteen Eighty-Four* where there was no escape from the watchful eyes of 'Big Brother'. Yet it is an image which seems to be no longer current despite the fact that the ubiquitous two-way tele-screen of *Nineteen Eighty-Four* may now be making a belated appearance in households in the guise of a combined high-definition digital TV and Internet monitor with interactive capability. While citizens are now subject to various forms of close surveillance, the bureaucratic and coercive elements of Orwell's imagination are less visible. Orwell's model assumed that the threat to privacy and freedom came from a brutal central government, but, as the Australian Law Reform Commission anticipated, the boundaries and sovereignty of national states are being eroded by global forces while transnational corporations grow in strength and influence.

The involvement of the corporate world in surveillance is driven by an interest in assessing and manipulating markets and reducing risk. Their special contribution is the private forms of 'dataveillance' to which their customers voluntarily submit when surrendering personal information as a condition of obtaining the convenience of computerized and automated financial transactions and other services offered to consumers. These same

citizens also appear willing to submit to public safety surveillance in the form of CCTV and other event-recording devices in public places for crime control and traffic management. Despite the data-matching possibilities of these innovations and the risks of error and abuse, the public seems to regard the current level of surveillance as essentially benign. This perception is reinforced by the assumption that as the monitoring is fragmented, decentralized and distributed between the public and private sectors, there is no ground to fear that behind it lurks an oppressive 'Big Brother' who is orchestrating the surveillance and whose objective is to crush citizens into conformity.

Back to the panopticon?

The alternative view put by a number of commentators is that the latest forms of surveillance are more akin to Bentham's utoptian idea of a 'panopticon' than Orwell's dystopian 'Big Brother' (Lyon, 1994: 57; Reeve, 1998: 69; Whitaker, 1999: 32). 'Panopticon'[24] is the name coined by Jeremy Bentham, in 1787 (Bentham, 1995) for his proposed plan for a semi-circular prison designed to keep each prisoner under supervision from a central location at all times:

> Prisoners, who in the original plan would be in individual cells, were open to the gaze of the guards, or 'inspectors', but the same was not true of the view the other way. By a carefully contrived system of lighting and the use of wooden blinds, officials would be invisible to the inmates.
>
> (Lyon, 1994: 62–3)

The objective of the panopticon was not simply to punish, but also to maintain discipline, a point enlarged by Foucault, in the 1970s. The latter saw the panopticon as a metaphor for the state's means of maintaining social discipline through surveillance of its citizens (Foucault, 1978). By subjecting them to scrutiny, whether in or outside formal institutions, the state could exercise power to produce a high level of civic compliance with a minimal need for direct coercion. Whatever the actual degree and constancy of scrutiny, the aim was to produce the impression of constant observation by officialdom, thus promoting self-discipline in those subject to surveillance.

Nowadays the machinery for monitoring citizens in their various activities is vast. The 'panoptic principle' does not need the context of a prison, nor the agencies of criminal justice, to advance social discipline (Shearing and Stenning, 1985: 335, describing its application to Disney World). It is applicable to all administrative arms of the state concerned with gathering information specific to their particular responsibilities, especially as it bears upon revenue collection and expenditure. Data on citizens are not only required to ensure compliance with relevant laws, eligibility criteria and performance standards, but also as a means of informing government of its own needs and strategies: 'The ability of the administrative state to administer rests on its extensive knowledge about the society and the

knowledge of where and when deviations from compliance occur' (Whitaker, 1999: 43).

Citizens are already well aware that major databases of personal information have been compiled which include them in order to record their financial standing or to maximize compliance with taxation and social security laws, access to medical benefits, the control of borders and the regulation of industries and the professions.

To maintain collections of data on consumers of public or private services, particularly on those individuals or groups who attract suspicion, is seen as more cost-effective in inducing conformity through deterrence or proactive intervention than through conventional reactive and punitive responses. The surveillance assists in the identification of risks through use of data matching, statistical probabilities and profiling, and their containment by excluding potential rule breakers from opportunities to engage in non-compliant behaviour (Ericson and Haggerty, 1997; Hughes, 1998; O'Malley, 1998, 1999).

In Bentham's panopticon those under surveillance submitted to it because of the coercion of the prison itself. Nowadays much monitoring of citizens by the private sector occurs as the result of 'participatory surveillance'. It is 'participatory' to the extent that citizens are willing to abandon elements of their privacy in order to gain access to highly desired private sector services, or because it is otherwise in their interests to do so. To this extent surveillance must be recognized as having an enabling as well as a constraining character.

In designing his panopticon, Bentham assumed state-centred surveillance power as did Orwell. But the modern distribution of power points to a transition from the centralized *surveillance state* modelled on former eastern bloc states, to a more capitalist *surveillance society* in which both the public and private sectors are engaged in keeping an eye on citizens for their own separate purposes (Hume and Adams, 1996; Staples, 1997; Whitaker, 1999).

Almost without notice, the panopticon has been revived under different proprietors and in a largely electronic form. While the consequences have not been as apocalyptic as feared by Orwell, these developments still remain largely unregulated and must themselves be kept under surveillance.

Conclusion

At one time the concept of 'surveillance' was confined narrowly to policing or spying. Now it encompasses the numerous other settings in which personal data are being collected by the governmental and private sectors as part of their crime prevention, revenue-raising, risk management, resource allocation and marketing objectives. The systematic collection of such data has been expedited by advances in computerization and tele-

communications which allow personal information to be stored, retrieved, matched, processed and disseminated with rapidity and at low cost. These processes have made surveillance as much a global, as a national or local phenomenon. The growth in public and private surveillance does not, in itself, signal a slide into tyranny, but as Justice Michael Kirby of the High Court of Australia has advised:

> It is highly desirable that in every jurisdiction legislators, governments, academics and the community generally should be debating the social implications of the new technology including the Internet. Such debates need to be supplemented by international initiatives which seek to devise principles as global as the technology itself. Otherwise, we will persist with a legal patchwork of dubious effectiveness and more and more business and other communications will take place in extra- and supra-jurisdictional space.
>
> (Kirby, 1998: 331)

He has also called for a second generation of information privacy principles in harmony with the development of the new technology to be drawn up without delay. The growing appreciation of the extent of surveillance is as much driven by legal interest in privacy rights as it is the product of the work of criminologists, or the activism of those organized to resist its spread. While it is true that civil liberties groups have expressed some interest in the topic, there is not the same awareness of the impact of database proliferation in areas not directly falling within the ambit of criminal justice. Moreover the privacy lobby has been unable to compete with the blandishments of technology in the enthusiasm for surveillance as a weapon against organized, sophisticated and transnational crime. Yet the New South Wales Privacy Committee, in its 1996–7 *Annual Report* cautioned that when politicians engage in a bidding war to prove who is 'toughest' on crime:

> Their proposed solutions often involve an increase in systems of personal surveillance which bears down hardest on the most vulnerable and powerless groups; the young, the disadvantaged and members of ethnic or national minorities, indeed the very people most likely to be victims of crime.
>
> (New South Wales Privacy Committee, 1996–7: 4)

The year George Orwell predicted would be the one in which most of the world would be living under a totalitarian rule which enforced its malevolent power by total surveillance of its citizens has long since passed. But the technological capacity to do what he described has been attained, and the image of a modern state with agencies possessed of an armoury of surveillance devices to record the present and remember the past remains compelling. Recent events in Europe and the South Pacific show how easy it is for totalitarian forces to assume power. But even within more stable democratic frameworks, there seems to be a growing willingness to rely on mass surveillance as a means of exerting disciplinary authority under the panopticon principles of Bentham (Rule, 1973; Davies, 1992, 1996; Lyon, 1994; Shapiro, 1999).

Though seemingly more consensual, more diffuse and thus more benign than the Orwellian prospect, the existence of any large-scale panopticon-style surveillance must be recognized as creating a new power relationship between the watchers and the watched. The latter are now more obviously in a position of subordination and uncertainty (Norris et al., 1998: 5–6):

> Not only does it facilitate the power of the watchers over the watched by enabling swift intervention to displays of non-conformity but through the promotion of habituated anticipatory conformity. . . . Surveillance therefore involves not only being watched but watching over one's self.

Social control is thus being achieved by conditioning to conformity as well as by the deterrent effect of potential exposure. More pointed interventionist and exclusionary strategies through the criminal justice system, or other means, are still being kept in reserve, but the surveillance record strengthens them immeasurably by offering the evidence to justify such action if required.

It is proper for criminologists to enquire what form the surveillance society is taking, but it is far too late for them to ask whether someone is watching over us: 'Unnoticed by the public, and overlooked by social and political commentators, the surveillance society sneaked under our guard, and has been implemented' (Clarke, 2000b: 14).

Notes

Based on a paper presented at the 15th Annual Conference of the Australian and New Zealand Society of Criminology, the University of Melbourne, Australia, 21–3 February 2001.

1 That it should continue to be so has been advocated by writers such as Duff and Gardiner (1996).
2 For developments in this area in the public sector see: www.cybercrime.gov and in the private sector: www.cybercrimes.net/international/lawenforcement.html.
3 The Internet facilitates fraud by making identity theft easy. The pilfering of personal information and credit card numbers from websites for use in fraudulent activities is becoming endemic.
4 See generally Casey (2000) and also the Australian Federal Police e-crime link resource at www.afp.gov.au/ecrime/index.htm.
5 Legislation seeking to regulate such 'bugging' is to be found in each of the states, e.g. Queensland (1971); New South Wales (1984); Northern Territory (1990); South Australia (1972); Tasmania (1991); Victoria (1999); and Western Australia (1978) as well as the Commonwealth (1979). The *Telecommunications (Interception) Act 1979* (Cth) prohibits the interception of 'a communication passing over a telecommunications system', except as allowed for under the provisions of that Act.
6 The Intelsat system is used for most global telecommunications. Communications relayed by Intelsat are shadowed and open to interception by a

widespread network of listening posts and tracking stations. This is the UKUSA network, a product of agreements between the United States National Security Agency (NSA) and the British Government Communications Headquarters (GCHQ) and junior partners which include Canada, Australia and New Zealand. See Richelson and Ball (1990), Hager (1996) and Whitaker (1999).

7 Such as the unique features of a person's iris scanned by cameras located at eye-level at automatic teller machines.

8 The FBI has expressed anxiety that as foreign companies (often with substantial foreign government ownership) buy controlling interests in US telecommunications companies, 'There may be no practical way to conduct lawful surveillance effectively and securely if the facilities that process US communications are located outside the United States'—FBI General Counsel Larry Parkinson (Greene, 2000).

9 *Regulation of Investigatory Powers Act 2000* (UK), s.12 Maintenance of interception capability.

10 The United States Justice Department has recently released a report on the technical aspects of an e-mail monitoring system called 'Carnivore' which gathers information from Internet service providers about the on-line messages sent and received by criminal suspects. It stores all evidence captured according to criteria set by the FBI, to a removable disk: www.msnbc.com/news/457153.asp. The full text of the report is to be found at www.usdoj.gov/jmd/publications/carniv_entry.htm. The Council of Europe, *Draft Convention on Cybercrime* (second revision, 2 October 2000) proposes the compulsory installation by service providers of similar eavesdropping facilities for the convenience of government.

11 See Lewis (2000) describing readily available software programs such as *Spector, eBlaster, Cyber Snoop* and the *007 Stealth Activity Recorder* that, once installed on a target computer, can secretly record all transactions which appear on the computer screen including password keystrokes. Originally designed to allow parents to spy on their children's computer usage, they are now being applied in a similar fashion in many other domestic and work situations.

12 For Australian background see Bushell (1999) and Dancer (1999).

13 Operating under the *Financial Transactions Reports Act 1988* (Cth).

14 For example *Crimes Act 1914* (Cth), s.23YO; *Crimes Act 1958* (Vic), s.464ZFD.

15 The main Acts are Commonwealth (1901, 1987, 1989 1979); Australian Capital Territory (1991); Queensland (1989); NSW (1997); NT (1988); SA (1996); Tasmania (1993); Victoria (1997); WA (1988).

16 For example *Children and Young Persons Act 1989* (Vic), s.64.

17 See now *Workplace Video Surveillance Act 1998* (NSW).

18 Michael (1994: 1): 'Of all the human rights in the international catalogue, privacy is perhaps the most difficult to circumscribe and define. . . the problem of the definition and scope of this fundamental human right has bedevilled decades of debate upon the subject. . .'

19 The New South Wales Privacy Committee (1995–6: 23) reported that an evaluation of CCTV cameras in Sydney had failed to demonstrate that they

had made a substantial and quantifiable impact on crime rates. Rather it suggested that some of the criminal activity was being displaced to neighbouring streets. In response to this, the New South Wales police service issued guidelines in 1996 for limiting the use of CCTV as a crime prevention strategy by local councils. The advice was that they should only be used as a measure of last resort where it could be demonstrated that other less privacy-invasive strategies had failed to preserve a reasonable measure of public safety. The guidelines specifically warned that CCTV should not be introduced in public places primarily as a means of enforcing regulations and by-laws. They indicated that, wherever possible, priority should be given to preserving the rights and freedom of citizens, including the right to be free from unwarranted surveillance by government and law enforcement agencies when visiting public places. See also New South Wales Law Reform Commission (1997); Painter and Tilley (1999).

20 For example *Intrusive Surveillance Code of Practice*, issued under *Police Act 1997* (UK), s.101(3), at http://www.homeoffice.gov.uk/oicd/iscop.htm.

21 E.g. *Road Safety Act 1986* (Vic), s.66 (offences detected by a photographic detection device); *Police Powers and Responsibilities Act 1997* (Qld), Part 10 (surveillance powers).

22 E.g. *Security and Investigation Agents Act 1995* (SA); *Security and Related Activities (Control) Act 1996* (WA).

23 E.g. *Invasion of Privacy Act 1971* (Qld); *Information Privacy Act 2000* (Vic).

24 'The all-seeing place'.

Australian statutes

Australian Federal Police Act 1979 (Cth)
Australian Security Intelligence Organisation Act 1979 (Cth)
Children and Young Persons Act 1989 (Vic)
Commonwealth of Australia Constitution Act 1900 (Cth)
Confiscation Act 1997 (Vic)
Crimes (Confiscation of Profits) Act 1988 (WA)
Crimes (Confiscation of Profits) Act 1993 (Tas)
Crimes (Confiscation) Act 1989 (Qld)
Crimes (Forfeiture of Proceeds) Act 1988 (NT)
Crimes (Superannuation Benefits) Act 1989 (Cth)
Crimes Act 1914 (Cth)
Crimes Act 1958 (Vic)
Criminal Assets Confiscation Act 1996 (SA)
Criminal Assets Recovery Act 1997 (NSW)
Customs Act 1901 (Cth)
Financial Transactions Reports Act 1988 (Cth)
Information Privacy Act 2000 (Vic)
Invasion of Privacy Act 1971 (Qld)
Listening Devices Act 1972 (SA)
Listening Devices Act 1978 (WA)

Listening Devices Act 1984 (NSW)
Listening Devices Act 1990 (NT)
Listening Devices Act 1991 (Tas)
Migration Act 1958 (Cth)
Police Powers and Responsibilities Act 1997 (Qld)
Privacy Act 1988 (Cth)
Proceeds of Crime Act 1987 (Cth)
Proceeds of Crime Act 1991 (ACT)
Privacy Amendment (Private Sector) Act 2000 (Cth)
Road Safety Act 1986 (Vic)
Security and Investigation Agents Act 1995 (SA)
Security and Related Activities (Control) Act 1996 (WA)
Surveillance Devices Act 1999 (Vic)
Telecommunications (Interception) Act 1979 (Cth)
Telecommunications (Interception) Legislation Amendment Act 2000 (Cth)
Workplace Video Surveillance Act 1998 (NSW)

United Kingdom statutes

Police Act 1997 (UK)
Regulation of Investigatory Powers Act 2000 (UK)

United States statutes

Communications Assistance for Law Enforcement Act 1994 (US)

References

Akdeniz, Y., N. Taylor and C. Walker (2001) 'Regulation of Investigatory Powers Act 2000: Bigbrother.gov.uk: State Surveillance in the Age of Information and Rights', *Criminal Law Review* February: 73–90.

Ali, I. and P. Biskup (1996) 'Pornucopia on the Net: A Contribution to the Recent Censorship Debate in Australia', *Australian Academic and Research Libraries* 27(4): 270–88.

Australian Centre for Policing Research (2000) *The Virtual Horizon: Meeting the Law Enforcement Challenges—Developing an Australasian Law Enforcement Strategy for Dealing with Electronic Crime*. Police Commissioners' Conference Electronic Crime Working Party (Report Series No. 134.1). Available at www.acpr.gov.au.

Australian Law Reform Commission (1983) *Privacy* (Australian Law Reform Commission Report No. 22). Sydney: ALRC.

Australian Transactions Reports and Analysis Centre (2000) *Annual Report 1999–2000*. Sydney: AUSTRAC. Available at www.austrac.gov.au.

Baker, S.A. and P.R. Hurst (1998) *The Limits of Trust: Cryptography, Governments, and Electronic Commerce*. The Hague: Kluwer.

Bentham, J. (1995) *The Panopticon Writings*, ed. M Bozovic. London: Verso.
Bok, S. (1983) *Secrets*. Oxford: Oxford University Press.
Bronitt, S. (1996) 'Electronic Surveillance and Informers: Infringing the Rights to Silence and Privacy', *Criminal Law Journal* 20(3): 144–52.
Bronitt, S. (1997) 'Electronic Surveillance, Human Rights and Criminal Justice', *Australian Journal of Human Rights* 3(2): 183–207.
Bushell, S. (1999) 'Spies on the Net', *Bulletin*, 11 May, pp. 92–3.
Casey, E. (2000) *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. San Diego, CA: Academic Press.
Clarke, R. (2000a) 'Technologies of Mass Observation', Notes for the Mass Observation Movement Forum, Melbourne, 26 October. Available at www.anu.edu.au/people/Roger.Clarke/DV/MassObsT.html.
Clarke, R. (2000b) 'While You Were Sleeping. . . Surveillance Technologies Arrived', *Australian Quarterly* 73(1): 10–14.
Colvin, M. (1998) *Under Surveillance, Covert Policing and Human Rights Standards*. London: JUSTICE.
Congress, Office of Technology Assessment (1995) *Electronic Surveillance in a Digital Age* (July). Washington, DC: (US) Government Printing Office. Available at http://www.wws.princeton.edu:80/~ota/disk1/1995/9513_n.html.
Dancer, H. (1999) 'Internet Spy', *Bulletin*, 11 May, pp. 84–7.
Davies, S. (1992) *Big Brother: Australia's Growing Web of Surveillance*. Roseville, NSW: Simon & Schuster.
Davies, S. (1996) *Monitor: Extinguishing Privacy on the Information Superhighway*. Sydney: Pan Macmillan.
Duff, L. and S. Gardiner (1996) 'Computer Crime in the Global Village: Strategies for Control and Regulation—in Defence of the Hacker', *International Journal of the Sociology of Law* 24(2): 211–28.
Enos, R., J.E. Holman and M.E. Carroll (1999) *Alternative Sentencing: Electronically Monitored Correctional Supervision*, 2nd edn. Bristol: Wyndham Hall Press.
Ericson, R.V. and K.D. Haggerty (1997) *Policing the Risk Society*. Toronto: University of Toronto Press.
EU JHA-Council (1995) 'Memorandum of Understanding on the Lawful Interception of Communications, 25 October', in M. Colvin (1998) *Under Surveillance, Covert Policing and Human Rights Standards*, pp. 29–30. London: JUSTICE.
Fay, S.J. (1998) 'Tough on Crime, Tough on Civil Liberties: Some Negative Aspects of Britain's Wholesale Adoption of CCTV Surveillance during the 1990s', *International Review of Law, Computers and Technology* 12(2): 315–47.
Flemming, P. and M. Stohl (2000) 'Myths and Realities of Cyberterrorism', paper prepared for the International Conference on Countering Terrorism through Enhanced International Cooperation, Courmayeur, Italy, 22–4 September. Available at www.ippu.purdue.edu/info/gsp/cyberterror_intro.html.
Forde, P. and A. Patterson (1998) 'Paedophile Internet Activity', *Trends and Issues in Crime and Criminal Justice* (No. 97). Canberra: Australian Institute of Criminology.

Foucault, M. (1978) *Discipline and Punish: The Birth of the Prison*, trans. A. Sheridan. New York: Pantheon.
Fox, R.G. (1987) 'Dr Schwitzgebel's Machine Revisited: Electronic Monitoring of Offenders', *Australian and New Zealand Journal of Criminology* 20(3): 131–47.
Fox, R.G. (1995) *Criminal Justice on the Spot: Infringement Penalties in Victoria*, Australian Studies in Law, Crime and Justice. Canberra: Australian Institute of Criminology. Available at http://www.aic.gov.au/publications/lcj/index.html.
Garfinkel, S. (2000) *Database Nation: The Death of Privacy in the 21st Century*. Sebastopol, CA: O'Reilly.
Giddens, A. (1987) *The Nation-State and Violence*. Berkeley, CA: University of California Press.
Grabosky, P.N. (1998a) 'Crime in a Shrinking World', *Trends and Issues in Crime and Criminal Justice* (No. 83). Canberra: Australian Institute of Criminology.
Grabosky, P.N. (1998b) 'Technology and Crime Control', *Trends and Issues in Crime and Criminal Justice* (No. 78). Canberra: Australian Institute of Criminology.
Grabosky, P.N. and R.G. Smith (1998) *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*. Annandale: Federation Press.
Grabosky, P.N., R.G. Smith and G. Dempsey (2001) *Electronic Theft: Unlawful Acquisition in Cyberspace*. Cambridge: Cambridge University Press.
Greene, T.C. (2000) 'FBI Warns Congress: Foreign Telecomms May Inhibit Wiretaps', reported on-line 8 September at www.theregister.co.uk/content/1/13096.html.
Greenleaf, G. (1987) 'The Australia Card: Towards a National Surveillance System', *Law Society Journal* 25(9): 24–30.
Greenleaf, G. (1991) 'Can the Data Matching Epidemic Be Controlled?', *Australian Law Journal* 65(4): 220–3.
Hager, N. (1996) *Secret Power: New Zealand's Role in the International Spy Network*. Nelson, NZ: Craig Potten Publishing.
Hughes, G. (1998) *Understanding Crime Prevention, Social Control, Risk and Modernity*. Buckingham: Open University Press.
Hume, J. and J. Adams (1996) 'Successful Public Surveillance: Controlling Crime without Social Control', *Security Australia* 16(2): 20–2.
Kirby, M. (1998) 'Privacy in Cyberspace', *University of New South Wales Law Journal* 21(2): 323–33.
Lewis, P.H. (2000) 'Snoopware Crosses Moral Divide', *The Age*, Green Guide, 29 June, pp. 17, 22–3.
Lyon, D. (1994) 'From Big Brother to Electronic Panopticon', in D. Lyon (ed.) *The Electronic Eye: The Rise of Surveillance Society*, 57–80. Minneapolis, MN: University of Minnesota Press.
Lyon, D. and E. Zureik (eds) (1996) *Computers, Surveillance and Privacy*. Minneapolis, MN: University of Minnesota Press.
McBride, T. (1997) 'State Surveillance—the Slippery Slope', *Privacy Law and Policy Reporter* 4(4): 71–4.

McCarthy, M. (1997) 'Censornet: The Competing Ideals of Censorship and Cyberspace', *Victoria University of Wellington Law Review* 27(2): 349–74.

McDonald, W. (ed.) (1997) *Crime and Law Enforcement in the Global Village*. Cincinnati, OH: Anderson Publishing.

McMullan, J. (1998) 'Social Surveillance and the Rise of the "Police Machine"', *Theoretical Criminology* 2(1): 93–117.

Mann, D. and M. Sutton (1998) 'Netcrime: More Change in the Organization of Thieving', *British Journal of Criminology* 38(2): 201–29.

Manning, I. (1996) 'Maintaining the Integrity of a Casino Security and Surveillance System', *National Association for Gambling Studies Journal* 8(1): 20–3.

Marx, G.T. (1988) *Undercover: Police Surveillance in America*. Berkeley, CA: University of California Press.

Michael, J. (1994) *Privacy and Human Rights: An International and Comparative Study, with Special Reference to Developments in Information Technology*. Paris: UNESCO Publishing.

Minister for Justice and Customs (Australia) (2000) *Transnational Crime Needs Transnational Law Enforcement*, Press Release 9 March. Available at http://law.gov.au/aghome/agnews/2000newsjus/40_00.htm.

New South Wales Law Reform Commission (1997) *Surveillance* (Issues Paper No. 12). Sydney: NSWLRC.

Norris, C., J. Moran and G. Armstrong (eds) (1998) *Surveillance, Closed Circuit Television and Social Control*. Aldershot: Ashgate.

Office of Strategic Crime Assessments (Australia) (1995) *Australia's Move to a Cashless Society: Some Implications for Law Enforcement*, Proceedings of OSCA Seminar (18 August). Canberra: Office of Strategic Crime Assessments.

Ogilvie, E. (2000) 'Cyberstalking', *Trends and Issues in Crime and Criminal Justice* (No. 166). Canberra: Australian Institute of Criminology.

O'Malley, P. (ed.) (1998) *Crime and the Risk Society*. Aldershot: Dartmouth.

O'Malley, P. (1999) *The Risk Society: Implications for Justice and Beyond*. Victoria: Report commissioned for the Department of Justice.

Organisation for Economic Co-operation and Development (1997) *Guidelines for Cryptography Policy*. Paris: OECD.

Painter, K. and N. Tilley (eds) (1999) *Surveillance of Public Space: CCTV, Street Lighting and Crime Prevention*. Monsey, NY: Criminal Justice Press.

Parliament of Victoria, Law Reform Committee (1999) *Technology and the Law*. Melbourne: Government Printer.

Privacy Commissioner (Commonwealth of Australia) (1994) *Privacy Implications of New Communications Networks and Services: Information Paper No. 1*. Canberra: Australian Government Publishing Service.

Privacy Committee of New South Wales (1995) *Invisible Eyes: Report on Video Surveillance in the Workplace*. Sydney: Privacy Committee of New South Wales.

Privacy Committee of New South Wales (1995–6) *Annual Report 1995–1996*. Sydney: Privacy Committee of New South Wales.

Privacy Committee of New South Wales (1996–7) *Annual Report 1996–97*. Sydney: Privacy Committee of New South Wales.

Reeve, A. (1998) 'The Panopticisation of Shopping: CCTV and Leisure Consumption', in C. Norris, J. Moran and G. Armstrong (eds) *Surveillance, Closed Circuit Television and Social Control*, pp. 69–87. Aldershot: Ashgate.

Richelson, J.T. and D. Ball (1990) *Ties that Bind: Intelligence Co-operation between the UKUSA Countries: The United Kingdom, the United States of America, Canada, Australia, and New Zealand*, 2nd edn. Sydney: Unwin Hyman.

Rimm, M. (1995) 'Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories and Animations Downloaded', *Georgetown Law Journal* 83(5): 1849–2008.

Rosen, J. (2000) *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House.

Rule, J.B. (1973) *Private Lives and Public Surveillance*. London: Allen Lane.

Shapiro, A.L. (1999) *The Control Revolution*. New York: Public Affairs.

Shearing, C.D. and P.C. Stenning (1985) 'From the Panopticon to Disney World: The Development of Discipline', in A.N. Doob and E.L. Greenspan *Perspectives in Criminal Law: Essays in Honour of John Ll. J. Edwards*, pp. 335–49. Toronto: Canada Law Book Inc.

Shearing, C. and P. Stenning (eds) (1987) *Private Policing*. Beverley Hills, CA: Sage.

Smith, R.G., M.N. Holmes and P. Kaufman (1999) 'Nigerian Advance Fee Fraud', *Trends and Issues in Crime and Criminal Justice* (No. 121). Canberra: Australian Institute of Criminology.

Staples, W.G. (1997) *The Culture of Surveillance: Discipline and Social Control in the United States*. New York: St Martin's Press.

Uglow, S. (1999) 'Covert Surveillance and the European Convention on Human Rights', *Criminal Law Review* April: 287–99.

Victoria, Auditor-General (2000) *Report on Ministerial Portfolios*. Melbourne: Victorian Government Printer. Available at http://home.vicnet.net.au/~vicaud1/mp2000/mp00just.htm.

Victoria, Parliament, Public Accounts and Estimates Committee (2000) *Report on the Outsourcing of Government Services in the Victorian Public Sector*. Melbourne: Victorian Government Printer. Available at www.parliament.vic.gov.au/paec.

Wallace, J. and M. Mangan (1996) *Sex, Laws, and Cyberspace: Freedom and Censorship on the Frontiers of the On-Line Revolution*. New York: Henry Holt.

Waters, N. (1997) 'Telecommunication—Extending the Reach or Maintaining the Status Quo?', *Privacy Law and Policy Reporter* 4(6): 110–12.

Werdegar, M.M. (1998) 'Lost? The Government Knows Where You Are: Cellular Telephone Call Location Technology and the Expectation of Privacy', *Stanford Law & Policy Review* 10(1): 103–17.

Westin, A.F. (1967) *Privacy and Freedom*. New York: Bodley Head.

Whitaker, R. (1999) *The End of Privacy*. New York: The New Press.

Whitfield, D. (1997) *Tackling the Tag: The Electronic Monitoring of Offenders*. Winchester: Waterside Press.

Whorlow, D.J. and J. Compton (1995) 'Technology and Business Issues of Electronic Toll Collection', *Proceedings of the International Conference on Application of New Technology to Transport Systems*. Melbourne, Victoria, Australia, 2: 15–22.

Williams, D. (Commonwealth Attorney-General) (2000) 'Anderson Legal: Launch of Internet Privacy Survey', Speech, Sydney, 26 October: 1–3.

Williams, K.S. and C. Johnstone (2000) 'The Politics of the Selective Gaze: Closed Circuit Television and the Policing of Public Space', *Crime, Law and Social Change* 34(2): 183–210.

Wood, J.R.T. (Commissioner) (1997) *New South Wales Royal Commission into the New South Wales Police Service: Final Report, Volume 5: The Paedophile Inquiry*. Sydney: The Inquiry.

RICHARD FOX is a Professor of Law, at Monash University in Melbourne, Australia. E-mail: richard.fox@law.monash.edu.au