

The Other Side of “Big Brother”: CCTV Surveillance and Intelligence Gathering by Private Police

David Aspland, Charles Sturt University, Australia

EXECUTIVE SUMMARY

A significant shift has occurred in the nature of policing over the past 30 to 40 years across jurisdictions and contexts. The paradigm of policing as a purely government function is under challenge. Policing is becoming more “pluralised” with a range of actors, both public and private. This shift has significant social implications for the general public, together with the public and private organisations that provide policing services. These implications are discussed and highlighted through the use of information technology by private police in two areas—CCTV surveillance and intelligence gathering. This case discusses this shift between public and private sectors in policing. The situation is more complex than a simple public/private divide and plays host to a range of interactions that bring many actors into contact, competition, and alliance in networks and assemblages. Most research and regulation remains focused on public policing even though, numerically, private policing is now a major provider of policing services in an increasingly fragmented, pluralized, and commodified market. This case considers the regulation of private policing as it exists in the Australian context and how it applies to the use of information technology, together with issues for human rights, especially privacy.

Keywords: CCTV, Human Rights, Intelligence, Pluralization, Privacy, Private Policing, Security, Surveillance

1. INTRODUCTION

It is not just a case of “sleepwalking into” or “waking up to” a “surveillance society”, as the UK’s Information Commissioner famously warned, it feels more like turning a blind eye to the start of a new kind of arms race, one in which all the weapons are pointing inwards. – B. Hayes

What Hayes (2009, p. 5) highlights is the increasing use of information technology in support of surveillance and intelligence gathering in a range of policing methodologies that impact on the daily lives of an increasingly large part of the modern population. Most policing is intrusive and can infringe on individual rights and freedoms. The policing methodologies of surveillance and intelligence gathering are perhaps more intrusive than other models. Whether it be the right to privacy, freedom of speech or the right to come and go as the individual pleases, the actions of police have the potential to curtail these freedoms. One of the freedoms that is most often

DOI: 10.4018/jcit.2011040103

infringed is the right to privacy. This is done through many forms of surveillance ranging from search warrants, telephone taps, email sweeps, observation, CCTV, video recording to intelligence gathering (Bronitt, 1997). These technologies allow for large amounts of data to be gathered and stored on individuals and organisations often without their knowledge or permission (Fox, 2001).

The common paradigm of policing is that it is carried out by properly accountable government agencies with due authority of the law for good of the community. In a major shift to this paradigm, most of this infringement of personal freedoms in our society is no longer carried out by government organizations, but rather is carried out by private organisations in a context where security can be purchased as a commodity (Newburn, 2001). The nature of private policing makes it ideally suited to methodologies involving information technology, such as surveillance and intelligence gathering. Indeed this is often its main strength in situational crime control.

The social implications of these activities that infringe on the rights and privacy of the individual are significant. They raise questions of the accountability of the organisations that undertake them and may even shape community attitudes to a range of issues.

Most research into accountability and regulatory frameworks focuses on the public police with relatively little carried out into private policing or its interaction with public policing (Button, 2002, p. 1; Hummer & Nalla, 2003, p. 88; Zedner, 2006a, p. 273; Stenning, 2009). Shearing argues that the focus on public policing has caused a failure of comprehension of the full implications of private policing (1992, p. 424). What needs to be considered is the accountability of private policing in its use of information technology for surveillance and intelligence gathering, as much of it falls outside state oriented regulatory and human rights frameworks (Marx, 1987; Stenning, 2009; Leman-Langlois & Shearing, 2009).

This case aims to discuss the reasons for change and the social implications of the increasing use of surveillance and intelligence gathering. The starting point in this analysis is how and why the policing streetscape has changed in the latter 20th and early 21st centuries. A good understanding of this helps to create a greater understanding of modern private policing methodologies of which surveillance and intelligence gathering form a critical part.

The case then discusses some of the key points through the use of scenarios that illustrate the critical issues that underpin CCTV surveillance and intelligence gathering by private police. The reason for this is that much learning concentrates on the acquisition of facts and principles, often in isolation. The use of scenarios in this instance is aimed at developing critical thinking about the issues and problems created by the use of CCTV and intelligence gathering by private police organisations and engaging in an experiential problem solving methodology utilizing the facts and principles discussed in the case (Hmelo-Silver, 2004; Naidu, Menon, Gunawardena, Lekamge, & Karunanayaka, 2007). The use of scenarios also allows for the effective consideration of complexity in a rapidly changing social environment which more closely reflects a real life application in context (Richards, O'Shea, & Connolly, 2004).

2. SETTING THE STAGE: THE PARADIGM SHIFT FROM PUBLIC TO PRIVATE POLICING

The term "private policing" is perhaps more controversial than "private security" but when examined as part of the overall social function of "policing", this concept is now greater than just the conventional understanding of "the police" as an organized body in the public domain. Shearing defines the function of policing as "the preservation of peace" where people are free from unwarranted interference to go about their business safely (1992, p. 400). Given this

breadth of definition it is logical to expand the concept of “policing” to engage many actors, both public and private.

Public and private policing have always existed side by side in a continuum. The issue of security, or rather insecurity, over the past 30 years has seen the rejuvenation of the private policing sector to a point where it now outweighs public policing in terms of numbers in many areas by a factor of 2 or 3 to 1 (De Waard, 1999).

A common misconception is that there remains a strict public/private divide, even if one ever existed. In modern policing there are a range of “assemblages” and “networks” that provide a complex mix of policing interactions and exchanges on many levels (Wood, 2006). This has seen services previously provided by government agencies, including policing and security, outsourced to the private sector or engaged in joint investigations. There are also private individuals contracting private organizations or organizations where public/private boundaries are blurred and organizations where staff circulate between the two (Marx, 1987; Hoogenboom, 2010, p. 87).

There have been several descriptions of this phenomenon and one of the most logical is that of the “pluralized” policing environment. Public policing remains, legislatively and socially, the dominant arm of policing and would be expected to remain so whilst the nation-state remains the primary political structure. But private policing, in all its forms, is now the largest policing *bloc* in the increasingly fragmented policing streetscape. Any consideration of crime prevention strategies in the 21st century, without considering the role of private policing, ignores a significant factor (Hummer & Nalla, 2003).

There has been an increased demand for policing services driven by many factors including increased fear of crime, insecurity and social unrest; increased levels of recorded crime; greater demands for protection caused by increased property ownership created by rising incomes of both individuals and corporations; shifts in public/private space and increases in mass private space. Also there has been a decline in the social “guardians” such as tram, rail and bus conductors and ticket inspectors; roundsmen/women such as milkmen and postal workers; together with other traditional social controls such as churches, schools, neighbourhoods and families that provided much “secondary” social control (Swanton, 1993; Nina & Russell, 1997, p. 7; De Waard, 1999; Johnston, 1999, p. 179; Jones & Newburn, 2002, p. 141; Neyroud & Beckley, 2001, p. 24; Schneider, 2006, p. 292; Fleming & Grabosky, 2009, p. 282; Caldwell, 2009, p. 114).

Since the 9/11 attacks in New York and the beginning of the “War on Terror” there has been an even greater focus on security at all levels (Perry, 2001). Also, the Global Financial Crisis (GFC) of 2008 has caused a significant reduction in public funding for public police (Gill, Owen, & Lawson, 2010, p. 6). Even before the GFC, increasing demand for policing services was pushing public police organizations to the limit of their capacity (Newburn, 2001, p. 841; Zedner, 2003, p. 153). Grabosky points out that the notion of policing as a “public good” has diminished and that it is unlikely that the state will be able to return to the dominant position of service provision thus ensuring an ongoing role and growth for private policing in a pluralised policing environment (2004, pp. 79-80). Sarre (2008) has noted that the private security sector in Australia grew from around 25000 in 1991 to around 50000 in 2006, whereas the numbers of public police increased from 36000 to 42000 in the same period. He highlights the fact that the increasing demand for policing services has continued unabated into the 21st century.

Another shift in policing style that has given application to the increased use of information technology has been to move away from the paradigm of “post crime” or reactive intervention by the public criminal justice system to the notion of “pre crime” or risk management based prevention strategies being more effective (Swanton, 1993; Zedner, 2006b). This style of crime

prevention is in tune with the “risk society” philosophy of the post-modern world where issues are assessed on the basis of risk management and prevention, rather than reacting to the crime after the event, which may be virtually impossible in the globalised world of business and travel in the 21st century (O’Malley, 2010, p. 3).

Also, with the move to a globalised world where crime is also becoming globalised and macroeconomic, it is fair to expect that business will move to seek a globalised crime or loss prevention mechanism that is free of the geopolitical strictures of the nation state. This is an extension of the “vacuum theory” where private policing continues to exist and flourish in areas where the state cannot guarantee to safeguard the peace and well-being of its citizens. In the post-modern, globalised world this may become more the rule than the exception (Shearing, 1992, p. 406).

It is now a truism that the average member of the public is more likely to come into contact with private policing than public policing in their daily lives (Sklansky, 2006, p. 89). These encounters take place in a wide variety of locations and on a regular basis often without the individual really noticing as they have become second nature. There is the overt presence, whether it is the security guard patrolling the shopping mall, at the airport searching passengers as they board their flights or providing security at government or private buildings where people work. The use of private security guards has extended into other areas, previously the preserve of public police, e.g., private security personnel have been used to control crowds at public demonstrations and protests (Button & John, 2002).

Then there is the not so obvious presence of the CCTV operator, the insurance fraud investigator and the private intelligence organizations that gather data on other businesses and individuals. Much investigation by government agencies in such areas as welfare and taxation fraud is now outsourced to the private sector.

Much of what is referred to as “hidden crime” that impacts on our lives is now investigated by private security organizations (Prenzler, 2001). As these are not public order issues requiring some form of uniformed presence, these areas that are ideally suited to the subtle, persuasive and embedded styles of private policing (Shearing, 1992).

3. POLICING BY TELEVISION: CCTV SURVEILLANCE OF MASS PRIVATE SPACE

Closed Circuit Television (CCTV) and its use to monitor public and private space has led to significant changes in both public and private policing. The use of CCTV has become a critical tool in “situational crime prevention” (Von Hirsch, 2000, p. 59; Wakefield, 2000, p. 128; ASIAL, 2010b). The use of large numbers of CCTV cameras has allowed for surveillance of large areas of public and private space without the need to deploy large numbers of public or private police in an overt manner with the CCTV seen as a preemptive tool for proactive policing (McCahill, 2008). Wakefield makes the point that the “unremitting watch” of private police using CCTV is often a critical aid to public police in identifying serious offenders (2000, p. 142).

Modern cameras allow the CCTV operator to home in on individuals in a crowd and identify troublemakers. It is a tremendous aid to the main power that underpins private policing, exclusion from private property and public/private space (Von Hirsch & Shearing, 2000). The main ethical question that underscores the use of CCTV is that it records all persons present in an area, both persons of interest to the CCTV operator as well as passers-by. The anonymity of the individual in the public environment has been diminished, if not removed altogether (Johnston & Shearing, 2003, p. 69).

In the public environment the individual has a right to privacy and Article 17 of the International Covenant on Civil and Political Rights provides that no one shall be subject to arbitrary interference with their privacy. It would seem at face value that the random sweep of the CCTV is just such an arbitrary interference. But what of “mass private space” such as shopping malls, which are now becoming the hub of much community life?

The laws relating to private property when applied in mass private space preclude private citizens from claiming their civil and human rights to a large degree. When entering mass private space, i.e., shopping malls, mass public transport, residential communities, hotel complexes, factories, manufacturing centres, hospitals, office blocks and other areas that could be deemed to be “private property” (Lippert & O’Connor, 2006, p. 57), the citizen loses the right to privacy having bags or belongings inspected or being under surveillance from CCTV often as a condition of entry. Gone also is the right to come and go as the citizen pleases as the greatest power used by private policing is the arbitrarily applied power of exclusion from private property, with dissension regarding the powers of the property owners (or their agents in the form of private security) being resolved by the surrendering of rights being an implied or explicit condition of entry (Sarre, 1994, p. 264):

Scenario 1: Duncan Fanning worked as a senior retail loss prevention officer for a large chain of retail stores. During his career he had developed a skilled ability to observe and monitor groups and individuals via CCTV in the various retail centres where he had worked. Most people were in the retail centres to enjoy the ordered atmosphere and shopping that was available. Also however, Duncan had observed a wide range of shop stealing methodologies used by a significant number of individuals and groups. Duncan had made sure that he recorded these methodologies and as many individuals as he could identify. He compiled a database which he shared with other loss prevention professionals, both in the retail store where he worked and other retail outlets belonging to the same chain, and with the public police. In that database he compiled lists of identification, recent photographs available from CCTV, the types of goods favoured, seasonal factors and common modus operandi. This information provided a sound basis for Duncan and other loss prevention professionals to exclude “high risk” individuals and groups from the retail centres where they worked.

This scenario discusses several of the key issues concerning the use of CCTV in mass private space; firstly the invasion of privacy and the fact that some people may not wish to be recorded or observed, whilst doing nothing illegal. The CCTV is a “catch-all” technology which is being increasingly widely used and the civil and human rights which underpin our democratic legal system are greatly reduced while the individual is on private property (Fox, 2001). Von Hirsch points out that this covert surveillance by an “unobservable observer” takes people unawares when they think they are free of scrutiny and that the person can feel constrained by the “chilling effect” of covert surveillance even if this is not the case (2000, p. 68). Fox describes this chilling effect as

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 (2001, p. 261).

Research shows that the majority of Australians (92%) are aware of the use of CCTV in public space and 79% of those surveyed are not concerned with this. Those surveyed suggested a range of public places as being appropriate for surveillance including places where people congregate, public transport and stations, shopping malls and private institutions. Of those that were concerned about the use of CCTV in public places the greatest concerns were that the information may be misused or that it was an invasion of privacy. In spite of this the majority of those surveyed nominated "the police" as an appropriate organisation to have access to CCTV footage, with only a few nominating businesses, councils or even the organisation that installed the CCTV as being appropriate (The Wallis Group, 2007, pp. 74-79; Hummerston, 2007).

This raises what Leman-Langlois and Shearing describe as "function creep" (2009, p. 7). Surveillance of this nature was originally aimed at curbing harmful criminal acts, behaviours that degraded life or abuse of state systems. Now the concern is that as society's tolerance of surveillance grows, surveillance can be used at lower levels with less justification, e.g., surveillance methodologies and technologies originally designed for use by government against terrorism end up being used by private organisations to monitor minor anti-social behaviour.

Next there is the issue of the power of exclusion. This is the main power that private policing holds over the individual in order to ensure compliance although in the private context it can be arbitrarily applied (Wakefield, 2000, p. 133). The power of exclusion is used to remove or restrict undesirable elements from mass private space in order to ensure that the retail trade continues without undue interference. According to Nina and Russell:

instead of being concerned about individual civil rights or Human Rights, private security of the "new" public space is more concerned about how to create conditions which can assist in promoting the logic of capital accumulation and the avoidance of any interference in this process (1997, p. 3).

The social implications of this exclusion of certain individuals or groups from mass private space are that anti-social behaviour is increasingly concentrated in lower socio economic areas. These become subject to increasingly disorder-intolerant public policing styles such as zero-tolerance (Kempa, Stenning, & Wood, 2004, p. 577). Also, is there an increase in public anxiety when viewing quantities of CCTV images of minor crime and anti-social behaviour through media outlets?

The interaction between the CCTV operator and other agencies in the pluralistic policing environment raises the issue of what confidentiality requirements are placed upon him/her when communicating observations or releasing video or audio material to other agencies and the risks of unregulated exchanges of information (Von Hirsch, 2000, p. 70). McCahill makes the point that interaction in this environment has assisted the mixing of policing techniques with private police adding "crime fighting" and "law enforcement" to their existing concerns of "private justice" and "loss prevention".

The use of CCTV by security companies is regarded as cost effective and the trend is for continuing growth in this area (Prenzler, Sarre, & Earle, 2009). Walters (2007) states that, based on figures from the Australian Security Industry Association, there are some 40,000 to 60,000 cameras in the Sydney CBD alone and there have also been moves by the NSW State Government, along with many other governments, to compile biometric facial recognition databases for use by police, using photographs collected for drivers licence applications (Jones, 2010). The compiling of these databases without public debate raises the issue of what safeguards are in place to protect the use and sharing of these records both now and in the future (Fox, 2001).

The British experience is even greater with an estimated 4.2 million CCTV cameras deployed in the United Kingdom or about 1 for every 14 citizens (Welsh & Farrington, 2009, p. 19). In addition to the video and audio scanning capacity the British systems also feature sophisticated number plate recognition software that permits large numbers of vehicles to be tracked simultaneously as they travel around major metropolitan areas (McCahill, 2008, p. 215).

The Australian Security Industry Association Limited (ASIAL) provides a specific CCTV Code of Ethics which states, among other things, a CCTV is not to be used solely for monitoring and surveillance but must serve a crime prevention function. This is supported by the Office of the Privacy Commissioner, Australia, who suggests that the use of CCTV surveillance should have a clear objective and are a proportional response to the defined threat (Hummerston, 2007). The possible breaching of privacy by the use of CCTVs is now the subject of reports by the NSW and Australian Law Reform Commissions who recognise that modern technology, whilst a great aid in the workplace, is also a great hazard to confidentiality and privacy (Davitt, 2010, p. 16).

Technology, such as CCTV allows for the covert gathering of a large amount of information on private citizens. This leads to the discussion of another use of information technology by private organisations, the gathering of intelligence.

4. INTELLIGENCE GATHERING: INTRUSION INTO PRIVATE LIVES

Intelligence, the analysed information on which organizations base decisions, is a critical factor in the effectiveness of both public and private of policing. In the digital age it is an area where privacy and policing are often seen to be at odds (Curtis, 2007).

The gathering of intelligence on domestic citizens by public policing agencies has been seen as necessary, in the context of criminal investigations, to track both individual criminals and patterns of crime. It is also seen as a threat to democratic freedom as in the stories of Australian Police Special Branches being used to monitor political activists, especially Communists in the 1950 and 1960s, and in more recent times, others who were considered unreliable or a potential threat to the established order, until these organizations were disbanded in the 1990s (Campbell & Campbell, 2007, p. 92). Domestic intelligence gathering by government is now subject to rigorous parliamentary oversight and is highly accountable.

The thought of private companies gathering intelligence on domestic citizens is the stuff of nightmares. It conjures up images of an unseen “Big Corporate Brother” watching in a futuristic scenario where all individual privacy has been stripped away by electronic corporate databases and information holdings on individuals in a “dataveillance” system that does not forget transgressions (Fox, 2001). This is seen as a threat to democracy itself (Kairys & Shapiro, 1980).

Intelligence gathering on individuals and organisations has increased dramatically since the 1970s as data gathering technology has improved and is carried out every day by many organisations, some as a part of their normal activities while for others it is their sole specialist function (Fox, 2001). The use of private intelligence services by corporations stems from issues of cost, need for specialized information to protect business interests (Hoogenboom, 2006, p. 380; Lippert & O’Connor, 2006). If not directly titled *Intelligence* this can go under the names of risk analyses, protective security services or consultancies (Hoogenboom, 2006, p. 375).

The databases gather an extraordinarily broad range of data and have the ability to retain it indefinitely with significant consequences for individual privacy, especially if there is an error in the data (Leman-Langlois & Shearing, 2009). This gathered intelligence is often shared within “Security Intelligence Networks” taking in public and private organisations (Lippert & O’Connor, 2006, p. 51).

At its most common and seemingly innocuous, the loyalty cards and credit card transactions offered by a wide range of businesses track the spending patterns of clients in order to target them for advertising material and E-tags track vehicle movements. At another extreme insurance companies hold intelligence information on clients claim histories and assessments on a clients insurance risk as a fraud prevention tool. Button cites examples of private security firms involved in retail loss prevention gathering intelligence on shoplifters and sharing that information with other retail organizations and police in intelligence gathering networks (2002, p. 104).

Private corporations hold a wide range of intelligence on individuals, ranging from credit ratings, loan default histories through to background employment checks. If one of the primary roles of private policing is to prevent loss for clients, then intelligence on potential risks is critical to the success of this role. Lippert and O'Connor (2006) make the observation that whilst private security organisations have developed a significant intelligence gathering capacity, they tend to share that intelligence with clients and public police mainly, with only a limited interaction with other corporations, as these are seen as competitors.

Wakefield states that private police, to aid situational crime control in mass private space, can and do develop risk profiles of individuals and groups based on such factors as anti-social behaviour, if they seem "out of place" or they are known offenders. She points out that much of the activity of private policing in this environment is directed toward gathering and sharing information through such activities as CCTV monitoring, data gathering, participating in security networks, engaging in informal liaison with public police and providing information to public police investigations (2000, p. 139). Some aspects of the issues raised are examined in the following scenario:

Scenario 2: In a continuation of Scenario 1, along with the lists, Duncan Fanning would provide a range of information from his own experience on the best way to identify and defeat shopstealing groups and individuals, to the other loss prevention officers within his company. At times he would also share this information with the local police, although not to any extent that would cause loss or embarrassment to his employer and only if it was a situation that he could not resolve without the intervention of public police. The information he gathering and analysed allowed him, and his company, to develop proactive strategies in loss prevention based on the methodologies and key times used by the main offenders. This analysis also permitted the extra resources and visible presence of the local police to be harnessed at times of peak risk. However Duncan was reluctant to share this information, on anything but a limited and informal basis, with loss prevention officers from other retail chains as they were competitors in the same field. Also he was aware of issues of privacy that could impact on any formal arrangement.

When gathering information and intelligence in the area of private security many companies operate without the need for legislative authorisation in many areas, although any organisation dealing in personal information is governed by the Privacy Act 1988 (Hayne & Vinecombe, 2008). The issue of the confidentiality of corporate databases and access to client information is one that will bedevil modern society with respect to the privacy of individuals and to what extent does the private security sector have the right to access confidential information, especially if the information has been supplied by the customer to the company, or another company, for alternative purposes than those for which they are being accessed. Williamson highlights the point, in the Australian context, by stating "most organisations do not have adequate governance over the collection, protection and destruction of personally sensitive data" (2010, p. 12).

In a Review of the Private Sector Provisions of the Privacy Act (Office of the Privacy Commission, 2005, p. 224), the Australian Institute of Private Detectives (AIPD) made a submission

asking for private detectives to be considered as a law enforcement body on par with public police. The basis of this submission was that private detectives had limited access to information and that this could prejudice their clients. The submission was refused mainly on the grounds that, unlike public police, private detectives are not accountable to the government or the community (2005, p. 229).

Prenzler (2001) identified the area of information privacy as a key concern with a number of inquiries taking place in New South Wales and Queensland into the unauthorised trading of information between police, private investigators and their clients (often through “old boy” networks). Prenzler makes the point though that the unauthorised trade could be as much the result of lack of knowledge about the legalities, given the complexity of the regulations governing the sector, as much as any misconduct or wrongdoing (2001, p. 10). Shearing states that this can arise where former public police join private organizations as a career change and vice versa, as quite commonly happens (1992, p. 414). This is topical given that much data handling is now outsourced to organisations that may not even be within the same national borders. This was recently highlighted when a data processing company in India, which processes data from many countries worldwide, including Australia, decided to use inmates from a gaol as data entry staff (Farooq, 2010).

Examples exist of the sharing of information and intelligence between the public and private sectors in law enforcement. These are the Greater Manchester Community Safety Partnership Team in the UK, the Eyes on the Street Program in WA and Operation Piccadilly to reduce Ram Raids on ATMs in NSW, Australia (Lewis, 2008, p. 158; Crime and Research Centre, 2008; Prenzler, 2009). These may well serve as models for the future and have significant social implications as large quantities of data are gathered on citizens and shared across a range of public and private organisations.

However, at present the sharing of intelligence has been identified as one of the main stumbling blocks to partnership policing as indicated by a number of senior police officers (Gill et al., 2010, p. 45). In the Australian context there are significant legislative and policy barriers to the sharing of intelligence between public and private policing organizations. Yet the trading and exchange of information within a trusted network is one of the pillars for effectiveness in pluralistic policing (Wardlaw & Boughton, 2006, p. 141). But, whilst many public policing organizations are prepared to accept information and intelligence, they are unable or unwilling to reciprocate in return and this raises barriers of trust (Harfield & Kleiven, 2008).

5. THE CURRENT CHALLENGES: HOW IS PRIVATE POLICING REGULATED?

The regulation of surveillance and intelligence gathering by private police is becoming more important and has significant social implications as the increasingly fragmented and pluralized policing streetscape is becoming more difficult to regulate. This is partly due to the diversified nature of the private security sector and the complexities of pluralised policing networks. This makes developing partnerships or applying universal standards difficult (Gill et al., 2010, p. 29). The fragmented nature of the industry makes it difficult to regulate as there is no one entity that is “private policing”. Included are a diverse range of manned security contractors, “in house” security, risk consultants, security advisors, technical staff and sales people working for any number of organizations ranging from one person, local operations to multi-national corporations. Also, given the state-based nature of regulation, staff working for the same company in different states of Australia can fall under different regulatory regimes.

Prenzler makes the point that it is difficult to prevent misconduct in public policing organizations which are heavily regulated. He raises the same question with regards to private policing and makes the point that there is a “very high opportunity factor for misconduct” based on “privileged knowledge about clients assets and vulnerabilities, and from the potential ‘Dirty Harry’ style conflict between noble ends and legal constraints” (2001, p. 7).

As previously stated most scrutiny, research and regulation in policing is focused on the public police, yet some of the larger private policing organizations have significant surveillance and intelligence gathering capacities, making them a substantial force in the marketplace. Well run and responsible organizations can be seen as an aid to government in promoting social and international order, yet they could also become a parallel force operating in a quasi-government fashion. The growth of private policing organisations in South Africa provides a useful case study in this area (Nina & Russell, 1997; De Waard, 1999; Defence Sector Program, 2007).

The American criminologist Elizabeth Joh (2006) offers a lesson from U.S. history, warning against the current enthusiasm for private policing organizations as an alternative to fill the void left by public funding shortfalls. She highlights the great risks if the corporate vested interests that control private policing are not properly regulated. As Marx (1987) points out, the regulatory frameworks in most democracies are aimed at limiting the power of the state over the private citizen, but not towards what private citizens do to each other unless that private citizen is in some way acting on behalf, and with the authority, of the state. Shearing advances the idea these experiences in the 19th and 20th century United States have coloured the attitudes of much present day analysis of private policing (1992, p. 405).

The regulation of private policing in Australia relies on state based legislation overseen by the Commissioner of Police for that state and industry codes of practice from bodies such as the Australian Security Industry Association Limited (ASIAL). There is also oversight in some states (notably New South Wales and Victoria) from Security Industry Advisory Councils which are made up of key industry stakeholders.

Sarre observes that while the role of private policing has increased unabated there is still much confusion over the role and powers of these organizations. He states that the “legal authority, rights and powers of private security providers is determined more by a piecemeal array of privileges and assumptions than by clear law” (2008, p. 303). There has been little by way of legislation to recognize any special role of the private security industry, with their powers and role still being largely defined as that of the ordinary citizen. Fox (2001) states that the legislative frameworks that protect citizens from overt and covert monitoring remain weak.

Much of the regulation of the industry in Australia is concerned with administrative issues and licencing rather than any ethical concerns of the interaction between the industry and the public (Button, 2007, p. 118). Queensland is unique in having legislated Codes of Practice at this time. However ASIAL provides a number of codes of practice that are specific in dealing with ethical issues in such areas a public interest, integrity, conflict of interest, unethical conduct, surveillance and privacy (2010a, 2010b).

Another significant basis of the regulation and control of private policing is the contract between the employer and the private policing organization. The employment contract, whether it be for contracted security or “in house” security defines the role, activities and functions of the security organization or employee and gives them the scope of their authority (Sarre, 1994, p. 263). Paradoxically, it is this contract based control that can lead to a number of ethical issues as the consumer of these commodified policing services generally purchases these services reluctantly and with a careful eye to the price, rather than quality (Zedner, 2006a, p. 271). This creates a downward pressure on costs which leads to low wages and high staff turnover in the private security sector which can create an increasing dependency on information technology. It also militates against

the additional costs of training and accreditation which could lead to a decrease in the professional standards of the industry.

Regulation by customer complaint is not to be underestimated. Given that the role of much of private policing is to aid the profitability of the contractor, the industry can be very sensitive to the needs of customers. This includes both those who hold the contracts and those who interact with private police in retail situations in mass private space, although security guards do tend to act in accordance with private interests rather than in the public interest (Wakefield, 2000).

6. CONCLUSION

The rejuvenation and expansion of the private policing sector in the late 20th century leading into the 21st century has seen private police take up many of the roles previously thought to be the prerogative of the public police. This has now included areas such as surveillance and intelligence gathering and has developed to the point where the private citizen is more likely to encounter private policing organizations and forms of policing in their daily lives, than public ones even if they do not realize it, but the regulation of this area remains fragmented.

While it is believed that public policing will remain the dominant policing form, by virtue of its legislative and social position, private policing will continue to grow and further develop to fill roles and functions required in an increasingly commodified and fragmented policing market. These roles will include an expanding use of information technology such as CCTV and intelligence databases. Given the pressure being placed on public policing agencies by ongoing funding and staffing cuts caused by the recent Global Financial Crisis it is likely that this will be the policing model of the future.

The social implications of this for the community as a whole will be significant with accountability of the use of surveillance and intelligence gathering technology being reliant on the governance of a pluralised network. This is likely to become more crucial as the use of this technology increases as people and organisations seek to reduce their risk of being victims of crime.

REFERENCES

- Australian Security Industry Association Limited (ASIAL). (2010a). *Code of Professional Conduct*. Retrieved November 26, 2010, from <http://www.asial.com.au/CodeofConduct>
- Australian Security Industry Association Limited (ASIAL). (2010b). *CCTV Code of Ethics*. Retrieved November 26, 2010, from <http://www.asial.com.au/CCTVCodeofEthics>
- Bronitt, S. (1997). Electronic surveillance, human rights and criminal justice. *Australian Journal of Human Rights*. Retrieved January 1, 2011, from <http://www.austlii.edu.au/au/journals/AUJ1HRights/1997/10.html>
- Button, M. (2002). *Private policing*. Cullompton, UK: Willan Publishing.
- Button, M. (2007). Assessing the regulation of private security across Europe. *European Journal of Criminology*, 4(1), 109–128. doi:10.1177/1477370807071733
- Button, M., & John, T. (2002). 'Plural Policing' in action: A review of the policing of environmental protests in England and Wales. *Policing and Society*, 12(2), 111–121. doi:10.1080/10439460290002659
- Caldwell, C. (2009). *Reflections on the revolution in Europe. Can Europe be the same with different people in it?* London, UK: Allen Lane, Penguin Books.
- Campbell, D., & Campbell, S. (2007). *The liberating of Lady Chatterley and other true stories. A History of the NSW Council of Civil Liberties*. Glebe, NSW, Australia: NSW Council of Civil Liberties.

- Curtis, K. (2007, November 20). *The social agenda: Law enforcement and privacy*. Paper presented at the International Policing: Towards 2020 Conference, Canberra, ACT, Australia.
- Davitt, E. (2010). New laws needed to prosecute invasion of privacy cases. *Australian Security Magazine*. Retrieved from <http://www.securitymanagement.com.au/articles/new-laws-needed-to-prosecute-invasion-of-privacy-cases-130.html>
- De Waard, J. (1999). The private security industry in international perspective. *European Journal on Criminal Policy and Research*, 7, 143–174. doi:10.1023/A:1008701310152
- Defence Sector Program. (2007). *Conference report on the regulation of the private security sector in Africa*. Pretoria, South Africa: Institute for Security Studies.
- Evans, K. (2011). *Crime prevention. A critical introduction*. Thousand Oaks, CA: Sage.
- Farooq, O. (2010). *Company outsources work to Indian prison, plans to employ about 250 inmates*. Retrieved January 21, 2010, from <http://www.news.com.au/business/breaking-news/company-outsources-work-to-indian-prison-plans-to-employ-about-250-inmates/story-e6frfkur-1225865832163>
- Fleming, J., & Grabosky, P. (2009). Managing the demand for police services, or how to control an insatiable appetite. *Policing . Journal of Policy Practice*, 3(3), 281–291.
- Fox, R. (2001). Someone to watch over us: Back to the panopticon? *Criminal Justice*, 1(3), 251–276.
- Gill, M., Owen, K., & Lawson, C. (2010). *Private security, the corporate sector and the police: Opportunities and barriers to partnership working*. Leicester, UK: Perpetuity Research and Consultancy International.
- Grabosky, P. (2004). Toward a theory of public/private interaction in policing. In McCord, J. (Ed.), *Beyond Empiricism: Institutions and intentions in the study of crime (Vol. 13, pp. 69–82)*.
- Harfield, C., & Kleiven, M. (2008). Intelligence, knowledge and the reconfiguration of policing . In Harfield, C., MacVean, A., Grieve, J., & Phillips, D. (Eds.), *The handbook of intelligent policing. Consilience, crime control and community safety* (pp. 239–254). Oxford, UK: Oxford University Press.
- Hayes, B. (2009). *NeoConOpticon. The EU security-industrial complex*. Retrieved January 20, 2011, from <http://www.statewatch.org/analyses/neoconopticon-report.pdf>
- Hayne, A., & Vinecombe, C. (2008, February). *IT security and privacy – the balancing act*. Paper presented at the Securitypoint 2008 Seminar.
- Hmelo-Silver, C. (2004). Problem based learning: what and how do students learn. *Educational Psychology Review*, 16(3), 235–266. doi:10.1023/B:EDPR.0000034022.16470.f3
- Hoogenboom, B. (2006). Grey intelligence. *Crime, Law, and Social Change*, 45, 373–381. doi:10.1007/s10611-006-9051-3
- Hoogenboom, B. (2010). *The governance of policing and security. Ironies, myths and paradoxes*. Houndmills, UK: Palgrave Macmillan. doi:10.1057/9780230281233
- Hummer, D., & Nalla, M. (2003). Modelling future relations between the private and public sectors of law enforcement. *Criminal Justice Studies*, 16(2), 87–96. doi:10.1080/0888431032000115628
- Hummerston, M. (2007, October 2). *Emerging issues in privacy*. Paper presented at the SOCAP- Swinburne Consumer Affairs Course.
- Joh, E. (2006). The forgotten threat: Private policing and the state. *Indiana Journal of Global Legal Studies*, 13(2), 357–398. doi:10.2979/GLS.2006.13.2.357
- Johnston, L. (1999). Private policing in context. *European Journal on Criminal Policy and Research*, 7, 175–196. doi:10.1023/A:1008753326991
- Johnston, L., & Shearing, C. (2003). *Governing Security*. London, UK: Routledge.

- Jones, G. (2010, June 3). NSW Government recording features for facial recognition. *Daily Telegraph*.
- Jones, T., & Newburn, T. (2002). The transformation of policing? Understanding current trends in policing systems. *The British Journal of Criminology*, 42, 129–146. doi:10.1093/bjc/42.1.129
- Kairys, D., & Shapiro, J. (1980). Remedies for private intelligence abuses: legal and ideological barriers. *Review of Law and Social Change*. New York University, 10, 233–248.
- Kempa, M., Stenning, R., & Wood, J. (2004). Policing communal spaces. A reconfiguration of the “mass property” hypothesis. *The British Journal of Criminology*, 44(4), 562–581. doi:10.1093/bjc/azh027
- Leman-Langlois, S., & Shearing, C. (2009). *Human rights implications of new developments in policing*. Retrieved January 20, 2011, from <http://www.crime-reg.com>
- Lewis, S. (2008). Intelligent partnership. In Harfield, C., MacVean, A., Grieve, J., & Phillips, D. (Eds.), *The handbook of intelligent policing. Consilience, crime control and community safety* (pp. 151–160). Oxford, UK: Oxford University Press.
- Lippert, R., & O'Connor, D. (2006). Security intelligence networks and the transformation of contract security. *Policing and Society*, 16(1), 50–66. doi:10.1080/10439460500399445
- Marx, G. (1987). The interweaving of public and private police undercover work . In Shearing, C., & Stenning, P. (Eds.), *Private Policing* (pp. 172–193). Thousand Oaks, CA: Sage.
- McCahill, M. (2008). Plural policing and CCTV surveillance. *Sociology of Crime . Law and Deviance*, 10, 199–219. doi:10.1016/S1521-6136(07)00209-6
- McGinley, I. (2007). Regulating “rent-a-cops” post 9/11: why the Private Security Officer Employment Authorisation Act fails to address homeland security concerns. *Cardozo Public Law . Policy and Ethics Journal*, 6(129), 129–161.
- Naidu, S., Menon, M., Gunawardena, C., Lekamge, D., & Karunanayaka, S. (2007). How scenario based learning can engender reflective practice in distance education. In Spector, J. (Ed.), *Finding your voice online. Stories told by experienced online educators* (pp. 53–72). Mahwah, NJ: Lawrence Erlbaum & Associates.
- Newburn, T. (2001). The commodification of policing: security networks in the late modern city. *Urban Studies (Edinburgh, Scotland)*, 38(5-6), 829–848. doi:10.1080/00420980123025
- Neyroud, P., & Beckley, A. (2001). *Policing, ethics and human rights*. Cullompton, UK: Willan Publishing.
- Nina, D., & Russell, S. (1997). Policing “by any means necessary”: reflections on privatisation, human rights and police issues – considerations for Australia and South Africa. *Australian Journal of Human Rights*. Retrieved January 25, 2010, from <http://www.austlii.edu.au/au/journals/AJHR/1997/9.html>
- O'Malley, P. (2010). *Crime and risk*. Thousand Oaks, CA: Sage.
- Office of the Privacy Commissioner. (2005). *Getting in on the act: the review of the private sector provisions of the Privacy Act 1988*. Melbourne, VIC, Australia: Author.
- Perry, W. (2001). The new security mantra. Prevention, deterrence, defense. In Hoge, J., & Rose, G. (Eds.), *How did this happen? Terrorism and the new war* (pp. 225–240). New York, NY: Public Affairs.
- Prenzler, T. (2001). *Private investigators in Australia: work, law, ethics and regulation*. Retrieved from <http://www.criminologyresearchcouncil.gov.au/reports/prenzler.pdf>
- Prenzler, T. (2009). Strike Force Piccadilly: A public-private partnership to stop ATM ram raids. *Policing: An International Journal of Police Strategies and Management*, 32(2), 209–225. doi:10.1108/13639510910958145
- Prenzler, T., Sarre, R., & Earle, K. (2009). The trend to private security in Australia. *Australasian Policing. Journal of Professional Practice*, 1(1), 17–18.

- Richards, L., O'Shea, J., & Connolly, M. (2004). Managing the concept of strategic change within a higher education institution: the role of strategic and scenario planning techniques. *Strategic Change*, 13, 345-359. doi:10.1002/jsc.690
- Sarre, R. (1994). The legal powers of private police and security providers. In Moyle, P. (Ed.), *Private Prisons and Police. Recent Australian Trends* (pp. 259-280). Leichardt, NSW, Australia: Pluto Press.
- Sarre, R. (2008). The legal powers of private security personnel: some policy considerations and legislative options. *QUT Law and Justice Journal*, 8(2), 301-313.
- Schneider, S. (2006). Privatising economic crime enforcement: exploring the role of private sector investigative agencies in combating money laundering. *Policing and Society*, 16(3), 285-316. doi:10.1080/10439460600812065
- Shearing, C. (1992). The relation between public and private policing. In Tonry, M., & Norval, N. (Eds.), *Modern Policing* (pp. 399-434). Chicago, IL: University of Chicago Press.
- Sklansky, D. (2006). Private police and democracy. *The American Criminal Law Review*, 43(1), 89-105.
- Stenning, P. (2009). Governance and accountability in a plural policing environment – the story so far. *Policing*, 3(1), 22-33. doi:10.1093/police/pan080
- Swanton, B. (1993). *Police & private security: possible directions*. Trends & Issues in Crime and Criminal Justice.
- The Wallis Group. (2007). *Community attitudes to privacy*. Melbourne, VIC, Australia: Office of the Privacy Commissioner.
- United Nations. (1966). *International Covenant on Civil and Political Rights*. New York, NY: Author.
- Von Hirsch, A. (2000). The ethics of public television surveillance. In Von Hirsch, A., Garland, D., & Wakefield, A. (Eds.), *Ethical and social perspectives on situational crime control* (pp. 59-76). Oxford, UK: Hart Publishing.
- Von Hirsch, A., & Shearing, C. (2000). Exclusion from public space. In Von Hirsch, A., Garland, D., & Wakefield, A. (Eds.), *Ethical and social perspectives on situational crime control* (pp. 77-96). Oxford, UK: Hart Publishing.
- Wakefield, A. (2000). Situational crime prevention in mass private property. In Von Hirsch, A., Garland, D., & Wakefield, A. (Eds.), *Ethical and social perspectives on situational crime control* (pp. 125-146). Oxford, UK: Hart Publishing.
- Walters, C. (2007, September 22). There is nowhere to hide in Sydney. *Sydney Morning Herald*. Retrieved January 20, 2011, from <http://www.smh.com.au/news/national/there-is-nowhere-to-hide-in-sydney/2007/09/21/1189881777231>
- Wardlaw, G., & Boughton, J. (2006). Intelligence led policing – the AFP approach. In Fleming, J., & Wood, J. (Eds.), *Fighting crime together. The challenges of policing and security networks* (pp. 133-149). Sydney, NSW, Australia: UNSW Press.
- Welsh, B., & Farrington, D. (2009). *Making public places safer. Surveillance and crime prevention*. Oxford, UK: Oxford University Press.
- Williamson, G. (2010). The problem with privacy. *Australian Security Magazine*, 10-12.
- Wood, J. (2006). Dark networks, bright networks and the place of police. In Fleming, J., & Wood, J. (Eds.), *Fighting crime together. The challenges of policing and security networks* (pp. 246-269). Sydney, NSW, Australia: UNSW Press.

Zedner, L. (2003). The concept of security: an agenda for comparative analysis. *Legal Studies*, 23(1), 153–176. doi:10.1111/j.1748-121X.2003.tb00209.x

Zedner, L. (2006a). Liquid security: managing the market for crime control. *Criminology & Criminal Justice*, 6(3), 267–288. doi:10.1177/1748895806065530

Zedner, L. (2006b). Policing before and after the police. *The British Journal of Criminology*, 46, 78–96. doi:10.1093/bjc/azi043

David Aspland is a lecturer with Charles Sturt University at the School of Policing Studies in Goulburn, New South Wales, Australia. He is former Inspector of the New South Wales Police. He holds a Masters Degree in Public Policy and Administration from the Australian Graduate School of Police Management, Charles Sturt University. He is currently undertaking a PhD in Criminology at Griffith University through the Centre for Excellence in Policing and Security (CEPS) looking at the ethical issues in public/private partnerships in policing. He served in the Australian Regular Army, and as an Officer in the Australian Army Reserve. He has been a Member of the Australian Institute of Professional Intelligence Officers (AIPIO) since 1996, Police Futurists International (PFI) and the Advisory Board of the Directors of the US based Public Safety Leadership Development Consortium (PSLDC) since 2007.