Research Article

INTELLIGENCE: A RISK TOO FAR, OR "DIGNITY AND JUSTICE FOR ALL OF US"?

Alan Beckley[**]

This study takes the form of a critical discussion that examines the growth of surveillance and intrusion into the privacy of Australian citizens for the ostensible purpose of gathering intelligence and maintaining security. It investigates the history of the growth of surveillance during the last decade and comments on the intrusion on privacy by public sector organisations, but mainly focuses on the growth in data harvesting carried out by private sector or quasi-governmental outsourced organisations while noting the lack of accountability of such agencies. It examined the level of intrusion, the possible uses of the data, along with outcomes and issues of incursion into citizens' privacy. The study analysed selected cases were data had been gathered by some (but not all) modern methods of gathering intelligence, such as closed circuit television (CCTV); travel and transport; private communications, social media; DNA sampling and databases. It quantified the effects of intelligence gathering, identifying and analysing cases where organisations had exceeded their powers in obtaining data and recommended several means of ensuring proper accountability and the implications for government policy.

Keywords: intelligence; privacy; CCTV; telephone-tapping; social media; DNA

INTRODUCTION

This critical discussion is intended to stimulate debate regarding the justification of gathering intelligence for a variety of purposes, the necessity to gauge its value to society and that the value should be balanced against its effects on the privacy of the individual citizen. The interpretation of the term *intelligence* in this context means sensitive and intimate personal data that is

[**] Corresponding author: a.beckley@uws.edu.au

being collected relating to the private lives of individual citizens in Australia. Intelligence is being gathered by both private and public organisations in an ever-increasing variety, intensity and depth. It should be noted that this study is mainly focused on intelligence gathering by private sector organisations; therefore readers should gauge its contents as only a partial discussion of the entire situation.

Developments in the power and speed of information communication technology have enabled the opportunity to build databases linking intelligence and data of private information about individual citizens, facilitating cross-referencing to identify personal traits and attributes to build a lifelike "virtual" portrayal of the person. The discussion suggests that information gatherers should be vigilant and conscious of their intrusions into personal privacy and be held accountable to justify their reasons and purpose for collection of such data. Legitimate investigatory agencies that are legally empowered to collect personal data such as criminal intelligence should confirm their operatives are aware of the responsibilities to cause as little intrusion in the lives of the citizens as possible along with the maximum attention to safeguard sensitive personal data and ensure confidentiality (Beckley, 2000: 18).

This critical discussion will first examine some recent developments in law and practice and then investigate techniques to manage the impact and risk of intelligence gathering. It will discuss the actual situation regarding the operations of closed circuit television (CCTV); transport and travel; personal communications and social media; and collection of DNA (deoxyribonucleic acid) samples and databases. By drawing the effects of these areas together, the reader can make a judgement on the overall intrusion into their privacy from these examples. It should be noted that these forms of intrusion are only examples and are not an exhaustive examination of all the means of intrusion into the privacy of citizens in democratic societies. The discussion has used a specific definition of *intelligence* for the purpose of inclusion of the private and public sectors:

> A value-added product, derived from the collection and processing of all relevant information relating to client needs, which is immediately or potentially significant to client decision-making (ACS, 2000: 15).

Therefore *intelligence* can be viewed from the different perspectives of criminal intelligence or data for the purposes of customer relationship management (CRM) informing suppliers of retail customers' needs and requirements. Whatever the purposes of gathering intelligence, it inevitably leads to intrusion into the privacy or bodily integrity of the individual citizen, but most countries have statutes, rules and regulations about the collection, recording and dissemination of intelligence for police, law enforcement or security purposes. The states and territories of Australia have different legal frameworks in relation to human rights and fundamental freedoms, but the country as a whole is signed up to relevant Treaties (Gans, Henning, Hunter, Warner, 2011: 9–10) that respect and protect the right to private and family life (for example: International Covenant on Civil and Political Rights (ICCPR) came into force in Australia 13 November 1980—enacted in Australia as the *Privacy Act 1988*). Australia also recognises the *Universal Declaration of Human Rights* (UN, 1948) which although not a treaty, is regarded as an important reference point on citizen rights (Gans, et al., 2011: 10); it states:

> The United Nations Universal Declaration of Human Rights (1948)—Right to Privacy
>
> Article 12. No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. (UN, 1948)

The months of June to August of 2013 were especially influential in providing information internationally about data collection and security intelligence on individual citizens by governments. This period included the trial of Bradley Manning, (a low-level intelligence operative employed in the US military) in the so-called "Wikileaks" incident, who pleaded guilty to the release of classified information into the public domain that resulted in intense media scrutiny (for example: McGeough, 2013, July20). The military court which tried him suggested he could be imprisoned for up to 136 years for leaking 700,000 diplomatic and security documents.

Also, an-ex National Security Agency (NSA) contractor Edward Snowden admitted leaking information to international media sources about the "Five Eyes" nations (Australia, Canada, New Zealand, the United Kingdom, and the United States). These partners have access to an information technology system

called *PRISM* which is able to scrutinise and analyse most electronic messages and on-line activities to produce intelligence reports for national security purposes. The NSA is able to trace telephone calls and store the telephone numbers of citizens without their knowledge or consent (Dorling, 2013).

These announcements and developments have caused concerns to citizens regarding the privacy and confidentiality of their personal details. Indeed, many politicians have questioned the need for this extreme level of intrusion (Risen, 2013), although an ex-chief of the NSA was quoted as saying that "spying on citizens' web activity [was] good news" (Gallagher, 2013). At the time of writing these are recent disclosures and it will take some time for protests against intrusion to prevail and legislation to respond, depending on the strength of public opinion pressure. This is clearly the age of surveillance on the citizen, from their private communications to their activities in public spaces covered by CCTV.

CLOSED CIRCUIT (CCTV)

Beckley (2002) published a journal article on the subject of the proliferation of CCTV in the UK, but by 2012 the number of cameras had trebled (McCahill & Norris, 2012: 6) and was estimated to be "at least" 4 million (Porter, 2009: 11). However, the Director (Alex Deane) of "Big Brother Watch," the organization which carried out the camera survey, said: "The evidence for the ability of CCTV to deter or solve crimes is sketchy at best" (BBC, 2009). Local councils and the police say that the cameras help to cut crime (AIC, 2009), catch criminals and lower the levels of the fear of crime (Anderson & McAtamney, 2011). Indeed, some research (Welsh & Farrington, 2008) suggested that crime can be reduced by 51% in car parks and 23% on public transport by the use of CCTV.

An evaluation report on Perth Transport Authority claimed a 50% reduction in assaults on trains covered by CCTV (WA Auditor General, 2011). Also, members of the public appear to support the introduction of CCTV (Bennett & Gelsthorpe, 1998; Ditton, 1998). There is conflicting evidence to support the cases for or against CCTV, despite considerable academic research (Pointing, 2012). In the case of the specific incident of the London transit bombings in July 2005 (Brooks & Corkhill, 2012: 58) it was stated that data from CCTV proved to be "an effective and valuable source of information in the investigation" (Bloss, 2009: 235). Also, in the case of Jamie Bulger, a toddler

who was abducted and murdered in Liverpool (UK), the perpetrators would not have been identified without the benefit of CCTV cameras (Scott, n.d.).

In Australia, the number of CCTV systems has been described as "more restrained than the UK" (Sutton & Wilson, 2004: 312), but in 2003, it was said (Wilson & Sutton, 2003: 5), "With systems already established in all Australian capital cities except Darwin, future expansion is likely to be in regional centres and suburban locations. Digital technology is also likely to become the industry standard." Cubbage (2012: 55) reported that the CCTV cameras in Australia are not so state-of-the-art, lacking high definition, precision and operability, thereby making identification of suspects more difficult. But projects are proposed (Carnovale, 2011) to combine CCTV with facial recognition systems (McDevitt, 2010) which may be more effective crime detection/prevention measures (Cameron, 2011) although it has taken a considerable time to develop the technology. The detection of a crime of murder in Victoria was mainly due to a CCTV recording (Dowsley & Flower, 2012) from a shop which viewed passers-by on the footpath outside, which could have been unlawful (Arnold, 2008). The video material, when transmitted on television, led directly to the arrest of the person subsequently found guilty of the crime (Silvester & Butt, 2012).

Although most CCTV operations are for laudable and sound reasons, the majority of the establishments in this field are private or outsourced organisations staffed by private operatives observing their community and its inhabitants from remote locations. This can lead to unapproved and unwarranted intrusion into the private affairs of individuals especially when cameras are used over-zealously or data is shared without proper authority or control and with little or no accountability. The focus of the critical discussion will now turn to transport and travel.

TRANSPORT AND TRAVEL

Automatic Number Plate Recognition

There is a similar situation between the UK and Australia with CCTV on traffic cameras or automatic number plate recognition (ANPR) systems; that is, where the UK leads, Australia appears to follow. In the UK, the National Policing Improvement Agency, whose operational responsibility in 2012 was handed over to the UK Home Office, received 15 million ANPR records per day (NPIA, 2012). The ANPR system is to be further rolled out throughout the UK from its concentration on motorways and ports and borders because of its positive

outcomes on the "fight on crime." For example, in the year 2006–2007, ANPR led to: "the arrest of 20,592 individuals; the identification of 52,037 vehicle related document offences; the seizure of 41,268 vehicles for document offences; the identification and recovery of 2021 stolen vehicles" (NPIA, 2012).

Sophisticated cameras are able to record the registration number of motor vehicles and track their journeys all over the country; the system is able to produce warnings and alerts to police officers thereby reducing crime and enhancing police officer safety. However, in Australia, according to Clarke (2009: 47):

> Australian policing agencies have been variously piloting and deploying ANPR, but without public oversight or control. A national agency, Crimtrac, is proposing to develop a vast database, which would store billions of entries showing the whereabouts of vehicles about which no suspicion of wrongdoing exists. Its purpose is expressly to facilitate mass surveillance of the Australian population. This represents national security extremism, and is a gross breach of trust by law enforcement agencies in Australia.

The records from ANPR were originally to be retained for 2 years (Watson & Walsh, 2008), but this, in 2006, was extended to 5 years; from its stated intention to be a counter terrorist measure it suffered from "function creep," and it is now a law enforcement aid. Indeed, Watson & Walsh, (2008: 4) describes ANPR in Australia thus: "This is a very large tool being used to monitor a very small percentage of the population, whilst containing a great deal of information about every person in the country."

The Federal Privacy Commissioner had previously commented on the plan: "The Office would caution against establishing infrastructure that could be used in such an expansive and invasive manner" (OFPC, 2008: 7). Crimtrac (McDevitt, 2010) proposed a network of about 100 fixed and additional mobile and in-vehicle ANPR linked cameras feeding into a national recording system. McDevitt (2010: slide 6) also stated that ANPR system tracks "vehicles not people" with tripartite benefits to traffic, law enforcement and national security.

From the traffic point of view, there are many advantages in using cameras to prevent "red-light running" especially in targeted road junctions with the highest number of offences. In the UK, red-light running results in 4,000–5,000

injury road collisions per year (Lawson, 1991). In terms of financial costs, according to research completed by Ayuso, et al. (2009) in Europe slight injury road traffic collisions cost the equivalent of A$71,000 and fatal incidents slightly over A$1m. Although some aspects of monitoring of traffic can be justified on the grounds of road safety, and the equipment is managed by publicly accountable bodies, there does not appear to be a rational explanation for the extent and volume of the data being collected, and thus its proportionality regarding the invasion of citizens' privacy.

Security Monitoring of Public Transport/Transit Areas

In response to the US-led program (US-VISIT) of biometric, physical and documentary profiling for foreign visitor surveillance; (Bloss, 2009; Goold, 2010) many other countries, including Australia are following suit, although the security in this area is provided and managed by private out-sourced companies or quasi-governmental organisations.

Australia invested A$69m to enhance immigration systems with a biometric-based visa system (fingerprint and facial images) from visa applicants from ten overseas locations, to "reduce the risks of terrorists, criminals and other persons of concern" (DPMC, n.d.) from entering Australia. In an audit of the management of the Department of Immigration and Citizenship (DIAC) the Auditor-General reported that the "benefits of biometrics in the area of border security generally relates to reduced rates, and financial impacts, of identity fraud, improved confidence in administration and national security, and greater efficiency in border processing. Some of these benefits, and their additional costs, are difficult to quantify" (Auditor-General, 2008: 13).

In addition, full body scanning equipment has been introduced throughout Australian airports, but there are some concerns relating to privacy (Silmalis, 2012). For example, a former model and actress claimed she was singled out on a US internal flight and saw the Transportation Administration (TSA) officials "leering" at the sight of her full-body scan (Barlass, 2011). In May 2013 it was reported that the TSA had replaced the original scanners in favour of those showing only "generic images" of the body (Fox News, 2013). In Australia, a businessman and the leader of the United Australia Party, Mr Clive Palmer, stated in July 2013 that such scanners were "highly invasive" and, if elected, he would ban them (Feeney, 2013). There is also an issue of what to do about

passengers who refuse to undertake the full body scan and the religious and cultural factors.

Also on the subject of transport, routinely, cameras are installed in taxis to record the faces of passengers, ostensibly for crime prevention purposes and specifically to prevent persons absconding without paying the fare. Research has shown in Perth (Mayhew, 2000), and USA (Smith, 2005) that cameras in taxis do reduce crime. Although under the umbrella of publicly-accountable bodies, the examples of data collection cited above are almost entirely managed on a day-to-day basis by private organisations fulfilling outsourced contracts for government departments. Several cases of personal harassment or embarrassment relating to the privacy of citizens have been identified and there is also a question over what is done with the data after the citizen exits the means of transport. The next issue under discussion relating to privacy is intrusion into private communications.

INTRUSION INTO PRIVATE COMMUNICATIONS

Although in Australia there are strict laws (*Telecommunications (Interception and Access) Act 1979*) which have recently been strengthened relating to interception and access to telecommunications, there have been a number of concerns (e.g. Australian Government, n.d.; Bronitt & Stellios, 2006; Bronitt, Harfield, Michael, 2009; CJC, 1995; Grabosky, 1986; Grabosky, 1989; McGrath, 1990; Queensland Parliament, 2003; Stewart, 1986; Victorian Privacy Commissioner, 2004) over the years relating to the gathering of intelligence by this means. This includes the statement in the Stewart Royal Commission (1986: 1) that there was evidence New South Wales Police had been illegally intercepting telephone calls for 20 years (Dorling, 2012). In Australia, there have been five major reports (*Barrett Review* (1994); *The Boucher Review* (1999); *Ford Review* (1999); *Sherman Review* (2003); *Blunn Review* (2005)) dealing with telecommunications interception. Bronitt and Stellios (2006: 414) found legislators described that the overhaul of the legislation was "an exercise in 'balancing' the interests of privacy against the interests of security and law enforcement."

That was despite the New South Wales Law Reform Commission (NSWLRC, 2001: paragraph 24) concluding (in 2001) that the balancing approach was "inherently flawed." The Blunn Report (2005: 10) examined telephone interception and found there was a need for, "comprehensive and over-

riding legislation dealing with access to telecommunications data for security and law enforcement purposes be established"; which led to the *Telecommunications (Interception and Access) Amendment Act 2007*.

The then Attorney-General described the 2006 legislation amendments as "enhanc[ing] interception powers and privacy protection" (Ruddock, 2006), but Bronitt & Stellios (2006: 424) concluded "While the reforms do enhance interception powers, we believe that these measures do not, to any *significant* degree, enhance privacy protections" (emphasis by original authors). The current law subject to various exemptions, states that a person shall not intercept, authorise, suffer or permit another person to intercept a communication passing over a telecommunications system. Time will tell if that updated law is effective in safeguarding privacy.

There have been a large number of enquiries and considerable public and political concern about "hacking" of mobile telephones in the UK following the investigation into illegal activities of reporters mainly from the *News of the World* newspaper which was owned by businessman, (Keith) Rupert Murdoch, AC, KSG. The full details and effects of what has been reported as disgraceful events were presented at the Canberra symposium on 8 August 2013 where this paper was presented (Beckley, 2013). The Leveson Inquiry (2012) interviewed 337 witnesses and found that newspaper reporters and operatives acquired 4,375 names and phone numbers of private citizens which involved 829 victims of mobile phone hacking. The Inquiry recommended a "genuinely independent and effective system of self-regulation" (Leveson, 2012: 13) but the UK Government is still considering this suggestion (i.e. at the time of this writing).

There is also concern about the development of "location based people tracking" (Michael & Clarke, n.d.) where mobile telephones with internal GPS (global positioning systems) tracking devices enabling satellite navigation also allow the individual mobile phone to be tracked within an accuracy of within a few metres, using triangulation methods. Researchers (Michael & Clarke, n.d.; Michael & Michael, 2009) describe location based people tracking as "uberveillance" which enables mobile phone companies to track customers so that commercial information and personal data can be extracted and fed into customer relationship management databases (Techtime, 2012).

Some of the outcomes of this tracking are undesirable (Haggerty & Samatas, 2010: 111–126 & 231–236; Neely & Barrows, 2012). Michael &

Michael (2009) found that data can be used to construct behavioural profiling and link owners to financial transactions and they warn of possible future "dystopian" scenarios in society. In addition, "Location-Based Social Networking" (LBSN) allows a member of a social network (e.g. Google Latitude, Loopt and BrightKite) to contact a "friend" remotely using a mobile telephone or other devices. This location information can be shared by persons known to the user or strangers and the service providers (Fusco, et al., n.d.). This issue links to the relatively recent phenomenon of social media.

Social Media

There is almost universal use of mobile phones, and Arthur (2012) explains that *Apps* on every smartphone are sharing data and uploading the phone owner's private contacts to the phone or social networking company (Facebook, Instagram, Yelp among others) but the phone user may be unaware that it is happening (Sarno, 2012). Mobile telephone users do not check the conditions of use provided with Apps that allow this data exchange to occur. Social media has achieved some good outcomes such as the so-called *Arab Uprising* that resulted in the overthrow of the Libyan dictator, Colonel Gaddafi; and the cause of *Kony 2012* (a major social media campaign organized by NGO *Invisible Children).* But, social media is also perceived negatively when used as a dynamic messaging device in incidents such as the street riots in the UK in 2011 (eBriefs, 2012).

There should be a great deal of concern over privacy issues relating to private communications and social media. It appears that citizens of the world are acquiescing to the ability of multi-national and trans-national private organisations collecting detailed personal and private data about their whereabouts, their needs and preferences and their financial status and spending. It also appears that technical experts can access private communications on mobile phones at will, again with little or no accountability. This critical discussion now turns its attention to DNA forensic strategies which in the UK were aimed at increasing the police detection rate by, "...deploying new technology, including enhanced DNA testing ... across the country to target criminals more effectively" (Home Office, 2004: 10).

DNA FORENSIC SAMPLES

In the UK, between 1 April 2011 and 30 September 2011 the National DNA Database produced 62 matches to murder, 285 to rapes and 15,685 to other crime

scenes (NPIA, 2011). The DNA databank in the UK in 2011 contained over 9 million records, which is one of the largest in the world and is a high proportion of the total population. However, researchers into crime detection statistics and the theory of *intelligence-led policing* (Ratcliffe, 2003) conclude that only a small percentage of the population is responsible for the majority of the crime (Audit Commission, 1993) although the perpetrators still need to be found in the database. The indefinite retention policy relating to DNA samples collected in the UK was challenged and found to be overly-invasive by the European Court of Human Rights in 2004.

In Australia, there are three DNA databases for law enforcement purposes. It is reported (Francis, et al., 2012) that there are over 450,000 person profiles (samples taken from suspected and charged persons) and 180,000 crime profiles (evidence taken from the scene of the crime). In 2010, Australia signed up to exchange DNA data with INTERPOL which is an international policing organization with 190 member countries. A research project in the USA (Roth, 2010) outlined concerns about DNA technology that makes it difficult for defendants to challenge and there is a chance of: (i) false matches and/or (ii) true match but coincidental. There are examples of DNA material being obtained by police by a trick (*Fleming v The Queen*, [2009] NSWCCA 233) and a "DNA testing flaw" found in Victoria (Silvester, 2009) that rendered some convictions unsafe (Griffith & Roth, 2006).

Research by Goodman-Delahunty & Hewson (2010) also found that statistics of certainty of matching quoted in DNA cases are difficult to understand for juries and there is an assumption ("the CSI effect") of the infallibility of the identification process. Roth (2010: 1,135) identified several problem issues and clear mistakes in the UK and the USA emanating from the main two types of DNA testing: confirmatory and cold case. All of the above is complicated by the latest developments in familial matching of DNA samples, the accuracy of which is not yet accepted globally, but was recently vindicated in proving that the Boston strangler crimes, the killing of 11 victims between 1962 and 1964, was in fact committed by the main suspect (Sherwell, 2013).

Although most DNA samples in the criminal justice system are collected by accountable organisations, in fact, most of the analyses of the samples are carried out by private laboratories or organisations which might lack accountability and security safeguards. The concerns relating to DNA samples and databanks are that confidential data could be obtained by health agencies and

insurance agencies, along with growth of the databanks which are described as being operated with a risk-based approach (Campbell, 2011: 55). This could lead to discrimination or restriction of goods and services to specific citizens suspected of debilitating medical conditions. There is evidence that "third party trackers" obtain user data from enquirers on websites relating to mental and medical health (*Sydney Morning Herald*, 2013). Having listed various issues relating to the privacy of the individual in democratic countries, this critical discussion will now draw some findings and conclusions from the previously discussed evidence.

CONCLUSION

Most organisations in the business of collecting intelligence will operate with the objective of acting lawfully and ethically but effective accountability needs to be established as this does not appear to be in place. This discussion has highlighted the fact that an increasing amount of personal data is being collected by private and public sector organisations through a variety of means such as CCTV and personal communications. It is necessary to reflect on the overall situation regarding the speed and intensity of data collection, performed by private and public sector organisations, which is increasing daily at a bewildering rate and is heavily impacting on the privacy of the individual citizen.

Details of investigations and whistle-blower announcements have revealed concerning issues relating to accountability of organisations that should have enhanced scrutiny and monitored the activities of their staff. It is not sufficient for executive managers to say they did not know the detailed activities of their subordinates; active supervision is required to prevent over-zealous or clearly criminal behaviour. The need to collect data should be balanced against the perceived outcomes, for example most research indicates that CCTV has no effect on reducing crime and anti-social behaviour although it does produce societal benefits in a few specific cases.

In terms of personal communications, there is a revolution and expansion of social media formats which enables the ability to contact and make acquaintances easily but also allows the facility to track and monitor personal locations, opinions, needs and requirements, which raises concern for confidentiality in the future. International cases raise the apprehension that criminals or hackers can access personal messages and private information from

mobile phones at will, raising an argument for greater encryption of mobile communications.

This critical discussion raises a debate around assessing the risk to the intrusion of intelligence gathering by investigating agencies (from the public *and* private sectors) on members of the public (the citizens and consumers) and asks the question: do the ends justify the means? The question is based on the test to decide if an action to obtain intelligence is ethically sound by asking several stages of questions relating to the good of the eventual outcome. That is: whether the means used will work effectively; whether there is a less harmful alternative and finally if the means undermines some equal or more important value. The intelligence gathering operative and practitioner should also recognise the risks relating to the justification of infringing human rights for the purpose of obtaining intelligence. A risk assessment should be carried out to establish the likelihood of harm occurring and the level of seriousness of the impact on the individual of the collection of intelligence (Beckley, 2012: 259); only where the risk is justified should the operation proceed.

The conclusion from this discussion must be that stronger scrutiny and safeguards are required to protect the privacy of the citizen in democratic societies. Judging by the comments of advice from the Federal Privacy Commissioner quoted above, it appears that individuals entrusted with guarding privacy have not been given adequate powers to enforce compliance.

Perhaps it is time for Australia to consider the introduction of the post of Surveillance Camera Commissioner (SSC) such as that in the UK. The SSC, who was appointed under the Protection of Freedom Act 2012, is about to issue new guidelines on surveillance cameras and ANPR (UK, 2013). Gathering all the evidence together about the daily erosion of personal privacy and confidentiality it is clearly time to take effective action to address these issues. On the positive side of the privacy equation, organisations responsible for gathering intelligence set a good example if, on every occasion, they are truly able to justify the resulting intrusions on the privacy of the individual citizen and retain dignity and justice for all of us which was the stated purpose of the *Universal Declaration of Human Rights* (UN, 1948).

REFERENCES

Anderson, J., & McAtamney, A. (2011). "Considering local context when evaluating a closed circuit television system in public places." *Trends & issues in crime and criminal justice*. Canberra: Australian Institute of Criminology.

Arnold, B. (2008). "Privacy guide: CCTV & other cams." *Caslon*, Retrieved 14/02/2012, from www.caslon.au

Arthur, C. (2012, March 3). "Nothing sacred in online grab for data." *The Age*.

Audit Commission. (1993) *Helping with enquiries: tackling crime effectively*. London: HMSO

Auditor-General, The. (2008) *DIAC's management of the introduction of biometric technologies.* Audit Report No.24 2007–8 Performance Audit. Canberra: Australian National Audit Office.

Australian Customs Service. (2000) *Intelligence doctrine*, Canberra: Author.

Australian Government. (n.d.) 73—Other telecommunications privacy issues—interception and access. *ALRC.* http://www.alrc.gov.au/publications/73.%20Other%20Telecommunications%20Privacy%20Issues/interception-and-access

Australian Institute of Criminology. (2009). Using CCTV to reduce antisocial behaviour. *AICrime Reduction Matters.* Canberra: Author.

Ayuso, M., Guillen, M., Alcaniz, M. (2009) The impact of traffic violations on the estimated cost of traffic accidents with victims. *Accident Analysis and Prevention* 42 (2010) 709-717

Barlass, T. (2011, March 27). G-rated scanners for travellers. *The Sydney Morning Herald*.

BBC News (2009, December 19) *Councils 'treble CCTV in decade'*. Retrieved from: http://news.bbc.co.uk/go/pr/fr/-/2/hi/uk_news/8419358.stm

Beckley, A. (2000) *Human rights: the pocket guide.* London: The New Police Bookshop.

Beckley, A. (2002). The future of privacy in law enforcement or how Michael Douglas helped frame the law. *Society of Police Futurists International*: http://www.policefuturists.org/

Beckley, A. (2012) Capacity building, chapter 8. In: Aepli, P. (Ed.) *Toolkit on police integrity*. Geneva: Geneva Centre for the Democratic Control of Armed Forces.

Beckley, A. (2013) *Intelligence: a risk too far or "dignity and justice for all of us?*" Conference presentation: *A symposium on the privatisation of intelligence* 08/08/2013, The National Press Club, 16 National Circuit Barton, Canberra. ARC Centre for Excellence in Policing and Security.

Bennett, T., & Gelsthorpe, E. (1998) Public attitudes towards CCTV in public places, studies in crime prevention. In Norris, C., Moran, J., Armstrong, G. (Eds.) *Surveillance, CCTV and Social Control*, Aldershot: Ashgate.

Bloss, W. P. (2009). Transforming US police surveillance in a new privacy paradigm. *Police Practice and Research: An International Journal*, 10 (3), 225–238.

Blunn, A. (2005). *Report of the review of the regulation of access to communications*. Canberra: Australian Government.

Bronitt, S., & Stellios, J. (2006) Regulating telecommunications interception and access in the twenty-first century: technological evolution or legal revolution? *Prometheus* 24:4, 413–428

Bronitt, S., Harfield, C., Michael, K., (Eds.) (2009). *The social implications of covert policing*. Wollongong: University of Wollongong Press.

Brooks, D., & Corkhill, J. (2012). The many languages of CCTV. *Australian Security Magazine*. Feb/March 2012: 57–59. Morley: My Security Media Pty Ltd.

Cameron, I. (2011) The cost of seeing clearly. *Policing Today*, 15.5, pp. 31–33.

Campbell, L. (2011) 'Non-conviction' DNA databases and criminal justice: a comparative analysis. *Journal of Commonwealth Criminal Law*, Issue 1, May 2011, pp.55–77

Carnovale, M. (2011). The face of crime. *Police Life*. April 2011, 28–29. Melbourne: Victoria Police Service.

Clarke, R. (2009) The covert implementation of mass vehicle surveillance in Australia. Chapter 6: pp. 47–62. In: Bronitt, S., Harfield, C., Michael, K. (Eds.) (2009) *The social implications of covert policing*. Wollongong: University of Wollongong Press.

Criminal Justice Commission. (1995). *Telecommunications interception and criminal investigation in Queensland.* Report 42. Brisbane: Author.

Cubbage, C. (2012). Public CCTV surveillance: networks & awareness. *Australian Security Magazine*. February/ March 2012: 56–57. Morley: My Security Media Pty. Ltd

Department of the Prime Minister and Cabinet (n.d.) Counter-terrorism white critical discussion: securing Australia protecting our community. *DPMC.* Retrieved from: http://www.dpmc.gov.au/publications/counter_terrorism/5_protection.cfm

Ditton, J. (1998) Public support for town centre CCTV schemes – myth or reality? In Norris, C., Moran, J., Armstrong, G. (Eds.) (1998) *Surveillance, CCTV and social control*, Aldershot: Ashgate

Dorling, P. (2012, February 18). Police spy on web, phone usage with no warrants. *The Sydney Morning Herald*.

Dorling, P. (2013, August 2) Spy program tracks "nearly all" web use. *The Age*: Retrieved from: http://www.theage.com.au/technology/technology-news/spy-program-tracks-nearly-all-web-use-20130801-2r2dc.html

Dowsley, A., & Flower, W. (2012, September 23) CCTV shows man in a blue hoodie spoke to missing ABC worker Jill Meagher moments before she disappeared. *Herald Sun*. Retrieved from: http://www.heraldsun.com.au/news/true-crime-scene/missing-woman-jill-meagher-seen-on-cctv-speaking-to-man-in-blue-hoodie-before-vanishing/story-fnat7jnn-1226479708333

eBriefs (2012, August 11) Police Superintendents Association of England and Wales: Cameron makes a statement of public disorder. House of Commons Main Statement. *UK Policing.* Retrieved from www.ukpolicing.info

Feeney, K. (2013, July 12) Palmer vows to ban body scanners after airport dispute. *Brisbane Times*. Retrieved from: http://www.brisbanetimes.com.au/queensland/palmer-vows-to-ban-body-scanners-after-airport-dispute-20130712-2pur0.html

Fox News, (2013, May 31) TSA gets rid of full-body scanners at US airports. Retrieved from: http://www.foxnews.com/politics/2013/05/31/tsa-gets-rid-full-body-image-scanners-at-us-airports/

Francis, B., Walsh, S., Hitchin, S. (2012) Australia signs on to the INTERPOL database. *Australian Police Journal,* March 2012, pp. 24–27

Fusco, S. J., Michael, K., Aloudat, A., Abbas, R., (n.d.). *Monitoring people using location-based social networking and its negative impact on trust*. Wollongong: University of Wollongong, School of Information Systems and Technology.

Gallagher, R. (2013, August 9) NSA spying on citizens' web activity "good news," ex-chief says. *The Sydney Morning Herald*

Gans, J., Henning, T., Hunter, J., Warner, K. (2011) *Criminal process and human rights*. Sydney: The Federation Press

Goodman-Delahunty, J. & Hewson, L. (2010) *Improving jury understanding and use of expert DNA evidence*. AIC Reports, technical and background Paper 37. Canberra: Australian Institute of Criminology.

Goold, B. (2010). How much surveillance is too much? Some thoughts on surveillance, democracy, and the political value of privacy. In: Schartum, D. W. (Ed.) *Surveillance in a constitutional government*. Social Science Research Network: 38–48.

Grabosky, P. (Ed.) (1986) *Government illegality*. Canberra: Australian Institute of Criminology

Grabosky, P. N. (1989). *Chapter 3: Telephone tapping by the New South Wales Police. Wayward governance: illegality and its control in the public sector.* Canberra: Australian Institute of Criminology: 47–65.

Griffith, G., & Roth, L. (2006) *DNA evidence, wrongful convictions and wrongful acquittals*. Briefing Paper No 11/06. Sydney: NSW Parliamentary Library Research Service.

Guardian, The. (2012, November 30) David Cameron statement in response to the Leveson Inquiry report. *The Guardian.* Retrieved from: http://www.guardian.co.uk/media/2012/nov/29/leveson-inquiry-david-cameron-statement

Haggerty, K. D., & Samatas, M. (Eds.) (2010). *Surveillance and democracy*. Oxford: Routledge.

Home Office (2004) *Cutting crime, delivering justice*, Cm 6288. London: HMSO

Kleinig, J., Mameli, P., Miller, S., Salane, D., Schwartz, A. (2011) *Security and privacy: global standards for ethical identity management in contemporary liberal democratic states*. Canberra: The Australian National University.

Lawson, S. D. (1991) *Red-light running: accidents and surveillance cameras*. Birmingham: AA Foundation for Road Safety Research and Birmingham City Council.

Leveson, B. (2012) *An inquiry into the culture, practice and ethics of the press*. The Leveson Inquiry. Executive Summary. November 2012. HC779. London: The Stationery Office.

Mayhew, C. (2000) Preventing assaults on taxi drivers in Australia. No. 179, November 2000. *Trends and issues in crime and criminal justice.* Canberra: Australian Institute of Criminology.

McCahill, M., & Norris, C. (2012) *CCTV in London*, Working Critical discussion No.6. Berlin: Urbaneye

McDevitt. B. (2010, October) *Automatic number plate recognition systems*. Presentation at *International and Serious Organised Crime Conference.* 18–19 October 2010, Melbourne: Australian Institute of Criminology.

McGeough, P. (2013, July 20) Manning may spend life in jail as judge upholds crucial charge *The Sydney Morning Herald*, p14

McGeough, P. (2013, August 1) Pyrrhic victory seals leaker's fate. *The Sydney Morning Herald*

McGrath, G. M. (1990) *Telephone interception: watching brief report*. Sydney: National Police Research Unit.

Michael, K., & Clarke, R. (n.d.) *Location privacy under dire threat as uberveillance stalks the streets*. Wollongong: University of Wollongong

Michael, M. G., & Michael, K. (2009). *The fall-out from emerging technologies: on matters of surveillance, social networks and suicide.* Wollongong: University of Wollongong.

National Policing Improvement Agency. (2011) *DNA technology crime detection*. Retrieved from: http://www.npia.police.uk/en/8934.htm

National Policing Improvement Agency. (2012) *Automatic number plate recognition*. Retrieved 2012, February 14 from: http://www.npia.police.uk/

Neely, A., & Barrows, E. (2012). *Are you giving away your most intimate secrets when you shop? See how Target learns about you through the power of analytics*. Retrieved 2012, March 8 from: www.cambridgeperformancepartners.com/blog/2012/2/19/are-you-giving-away-your-most-intimate-secrets-when-you-shop.html

New South Wales Law Review Committee (2001) *Surveillance: an interim report*. No 98, 2001. Sydney: NSW Government.

OFPC (2008) *Inquiry into automatic number plate recognition technology submission to the Queensland Parliamentary Travelsafe Committee*: Issues Critical discussion No. 12. Office of the Federal Privacy Commissioner, February 2008. Retrieved from: http://www.parliament.qld.gov.au/view/committees/documents/TSAFE/inquiry/ANPR%20technology/Submissions/28.pdf

Pointing, B. S. (2012) Effective use of CCTV camera operators. Perth: *Australian Security Magazine*, February/March 2012

Porter, G. (2009) CCTV images as evidence. *Australian Journal of Forensic Sciences*, 41:1, 11–25

Queensland Parliament. (2003) *"Telephone tapping" powers for Queensland law enforcement agencies: the Telecommunications (Interception) Queensland Bill 2003 (Qld)*. Brisbane: Queensland Parliament.

Ratcliffe, J. H. (2003) Intelligence-led policing. *Trends & issues in crime and criminal justice* April 2003, No.248. Canberra: Australian Institute of Criminology.

Roth, A. (2010) Safety in Numbers? Deciding when DNA alone is enough to convict. *New York University Law Review*, vol 85: 1130.

Risen, J. (2013, July 9) Privacy lobby challenges NSA spying in highest court. *The Sydney Morning Herald*

Ruddock, P. (2006, March 30) *Enhanced interception powers and privacy protections*, Press Release, 30 March 2006. Sydney: NSW Government

Sarno, D. (2012, February 17). Smartphones exposed to new data mining. *The Sydney Morning Herald*.

Scott, S. L. (n.d.) Death of James Bulger. *Trutv*. Retrieved from: http://www.trutv.com/library/crime/notorious_murders/young/bulger/1.html

Sherwell, P. (2013, July 13) DNA sparks breakthrough in Boston Strangler case. *The Sydney Morning Herald*

Silmalis, L. (2012, February 5). Full-body scans rolled out at all Australian international airports after trial. *The Sunday Mail*.

Silvester, J. (2009, December 10) New DNA testing flaw. *The Age*. Retrieved from: http://www.theage.com/national/new-dna-testing-flaw-20091209-kk22.html

Silvester, J., & Butt, C. (2012, September 28) Man arrested over Jill Meagher case. *The Sydney Morning Herald*. Retrieved from: http://www.smh.com.au/victoria/man-arrested-over-jill-meagher-case-20120927-26nu7.html

Smith, M. J. (2005) *Robbery of taxi drivers. Problem-oriented guides for police.* Problem-Specific Guides Series No. 34. Washington DC: US Department of Justice. Office of Community Oriented Policing Services.

Stewart, D. (1986) *Royal Commission into alleged telephone interceptions*. April 1986. Sydney: NSW Government

Sutton, A., & Wilson, D. (2004) Open-street CCTV in Australia: The politics of resistance and expansion. *Surveillance and Society* 2(2/3): 310–322.

Sydney Morning Herald, The. (2013, July 10) Health privacy now in the eye of the spy. *The Sydney Morning Herald.*

Techtime. (2012) Futuristic facial detection and tracking technologies help retailers analyse store performance. *Australian Security Magazine*. December 2011/January 2012. Morley: My Security Media Pty. Ltd.

UK Government. (2013) *Surveillance Camera Commissioner*. Retrieved from: https://www.gov.uk/government/organisations/surveillance-camera-commissioner

United Nations. (1948) *Universal declaration of human rights*. Geneva: UN.

Victorian Privacy Commissioner (2004) *Submission to the Commonwealth Parliament's Senate Legal and Constitutional Committee on its inquiry into the provisions of the Surveillance Devices Bill 2004*. (23 April 2004).

Victoria: Government Printers.

Watson, B., & Walsh, K. (2008) *The road safety implications of automatic number plate recognition technology*. Brisbane: The Centre for Accident Research & Road Safety.

Welsh, B. P., & Farrington, D. C. (2008). Effects of closed circuit television surveillance on crime. *Campbell Systematic Reviews*, 2008:17, Retrieved 2013, May 17 from: http://www.campbellcollaboration.org/

Western Australia Auditor General. (2011) *Use of CCTV equipment and information*. Western Australia Auditor General's Report. Perth: WAAG.

Wilson, D., & Sutton, A. (2003). Open-street CCTV in Australia. *Trends and issues in crime and criminal justice* (271). Canberra: Australian Institute of Criminology.

ABOUT THE AUTHOR

Alan Beckley is Evaluation Manager and Adjunct Research Fellow at University of Western Sydney. He is an Associate Investigator with the Australia Centre of Excellence in Policing and Security (CEPS) and was a graduate of FBI National Academy while he was a serving police officer in the United Kingdom. Beckley is currently completing a PhD on Human Rights and Ethical Standards in Policing.

- o O o -