When the Profile Becomes the Population: Examining Privacy Governance and Road Traffic Surveillance in Canada and Australia

Ian Warren, Randy Lippert, Kevin Walby and Darren Palmer*

Abstract

Use of automated licence/number plate recognition ('ALPR/ANPR') technologies in Canada and Australia raises significant policy questions for privacy advocates and criminal justice practitioners. The proliferation of mass surveillance through ALPR/ANPR also presents several conceptual puzzles about the links among criminal justice data flows, individual privacy and state responsibility in this actuarial age. In this article, we use case studies of ALPR/ANPR in Canada and Australia to examine privacy as a technique for governing road traffic surveillance. We explain our findings in light of Harcourt's (2007) argument against the use of actuarial prediction and 'hit rates' that are rationalised as the chief measure of law enforcement activities and effectiveness. Finally, we question the regulation of surveillance technologies such as ALPR/ANPR through current Canadian and Australian information privacy laws, with specific focus on privacy by design ('PbD'), a strategy that favours improving law enforcement efficiency at the expense of privacy.

Introduction

The dilemma of reconciling law enforcement mandates with information privacy rights has international relevance. This tension is acute in situations where law enforcement agencies adopt new technologies to replace manual identity matching and criminal history checks involving a growing range of publicly accessible and private information. Digital technologies enable the rapid sorting of increased volumes of information to assist with the efficient detection and prevention of serious crime and enforcing a larger array of low-level fines (Brown et al 2013). Automated data sorting is increasingly evident in contemporary law enforcement through mobile applications of camera surveillance technologies, such as Automatic Licence Plate Recognition ('ALPR'). However, the

* Ian Warren, Senior Lecturer, School of Humanities and Social Sciences, Deakin University, Geelong, Victoria, Australia, email: ian.warren@deakin.edu.au; Randy Lippert, Professor, Department of Sociology and Criminology, University of Windsor, Windsor, Ontario, Canada, email: lippert@uwindsor.ca; Kevin Walby, Assistant Professor, Department of Criminal Justice, University of Winnipeg, Winnipeg, Manitoba, Canada, email: k.walby@uwinnipeg.ca; Darren Palmer, Associate Professor, School of Humanities and Social Sciences, Deakin University, Geelong, Victoria, Australia, email: darren.palmer@deakin.edu.au.

mass-population screening potential of these technologies (see Harris 2013; Cousineau 2013; Derby 2011) raises important questions about determining the proper balance between legitimate law enforcement activity, the public interest and privacy.

This article examines the impact of information privacy law and compliance structures in light of the emergence of road traffic surveillance technologies to which both Canadian and Australian drivers are increasingly subject. The article has comparative resonance, especially for scholars working in these and other common law countries with similar information privacy and criminal justice regimes. Our research examining the logics of privacy governance and law enforcement practice suggests current privacy law has limited scope to restrict the expansion of new surveillance and data-sharing technologies that have become routine in contemporary policing. We first examine the Canadian and Australian contexts of privacy governance. We then assess the rationales deployed to justify the expansion of road traffic surveillance in both countries and the possible effects of such surveillance on privacy more generally. We also raise questions about the effectiveness of this approach to traffic control by drawing on Harcourt's (2007) examination of the 'ratchet effect' of data sorting in law enforcement, and 'elasticity', a term invoked to highlight the limitations of these initiatives in reducing aggregate rates of crime and disorder.

We illustrate these processes by analysing information privacy law used to regulate ALPR deployment in Canada, or Automatic Number Plate Recognition ('ANPR') as it is termed in Australia ('ALPR/ANPR' except where these are discussed in a particular national context). ALPR/ANPR is commonly used for the automated collection of tolls on public or privately managed roads, 'controlling access to restricted areas, [administering] congestion taxes, monitoring freight movement and calculating fees for unattended car parks' (VLRC 2010:114). Historically, road traffic control via law enforcement involved multiple forms of manual data matching that required police to access vehicle registration and personal licence information from various discrete sources (O'Malley 2010, 2013). Both Canadian and Australian law enforcement authorities consider ALPR/ANPR valuable in reducing 'auto theft and motor vehicle violations … related to prohibited, suspended, unlicensed and uninsured drivers' (Denham 2012:11) and those driving under the influence of illicit drugs (Wilson 2012). Evidence in both jurisdictions indicates these classes of driver are overrepresented in road collisions and fatalities (Hooper 2013:15).

However, the perceived benefits of fixed or mobile ALPR/ANPR are 'not limited to detecting traffic related offences' (Murphy 2010). This technology can also assist in tracking the movements of organised crime suspects (Parliamentary Joint Committee on Law Enforcement 2012), 'gang members, drug traffickers and sexual predators' (Derby 2011:161). CrimTrac, Australia's leading data repository for DNA samples (Briody and Prenzler 2005), considers ANPR 'one of the most significant breakthroughs in intelligence-led policing' (CrimTrac 2008:33), and favours centralised storage and dissemination of all ANPR data collected by Australian state police agencies to enhance 'national security' and 'community safety' (CrimTrac 2008:34). Equivalent road traffic control, criminal investigations and security benefits are also recognised (Gaumont and Babineau 2008) and questioned (McArthur 2012) in Canada. The appeal of automated data collection, storage and dissemination among law enforcement officials therefore requires inquiry into how information privacy law governs these technologies.

This article critically appraises diverse approaches to privacy governance in Ontario, Canada, and Victoria, Australia, given the rapid emergence of ALPR/ANPR as a potentially valuable and efficient law enforcement technology in these jurisdictions. Our comparative examination identifies distinct approaches to the governance of privacy, which variously

work to constrain or promote further deployment of ALPR/ANPR. Our approach helps to identify and question key rationales for the adoption and acceptance of new surveillance technologies, while interrogating the value of privacy as way to curtail the unregulated flow of personal data between multiple public and private agencies. We highlight similarities and differences in the use of privacy as a form of governance with potential to address regulatory gaps associated with new and emerging technologies that automate otherwise manual police detection and information-sorting processes.

This analysis draws on Harcourt's (2007) argument that questions how identity tracking and actuarial data-sorting technologies are commonly endorsed by referring to 'hit rates'. Harcourt (2007:112–14) demonstrates that the use of 'hit rates' as the dominant measure of law enforcement effectiveness leads to disproportionate targeting of those with an identifiable record of previous 'hits'. New surveillance technologies that efficiently identify hit rates enable police 'to make discriminations among populations' based on 'pure information' or an individual's recorded 'data double' (Haggerty and Ericson 2000:614). Harcourt argues hit rates are a false measure of police effectiveness, because they overlook how those with no recorded 'hits' might contribute to aggregate patterns of offending. Thus, the actuarial potential of ALPR/ANPR technology may be limited when it is deployed to target individuals with a recorded 'criminal and traffic violation history' (Meehan and Ponder 2002:406), or at 'hot spots' where lawbreakers are more likely to be detected (Koper, Taylor and Woods 2013). Selective deployment fails to account for potential differences between the 'elasticity' (that is, group capacity to change behaviour in light of changes in policing activity, such as profiling) of the profiled and non-profiled groups, and fails to account for a potential 'ratchet effect', a self-fulfilling prophecy involving increasing disproportionality that occurs when police continually profile the higher traffic-violating group. While based on different assumptions about offending behaviour (Harcourt 2007), the impact of 'elasticity' and the 'ratchet effect' can lead to overall increases, rather than decreases, in the prohibited targeted behaviour in the population. This possible consequence is entirely missed when hit rates are used as the exclusive measure of ALPR/ANPR's success.

Harcourt's critique of actuarial profiling reveals several less celebrated by-products of ALPR/ANPR and equivalent information sorting and identification technologies that are claimed to prevent or reduce prohibited behaviour. The potential for ALPR/ANPR to be deployed at 'hot spots' or 'hot times' when offending is most likely to be detected and then be used to surveil the entire driving population because overall rates of traffic offending have not declined, is a key example of 'when the profile becomes the population'. We consider Harcourt's prospects of fully randomised checks as one policy alternative to address the problem of selective profiling. We do so in part because of the limited capacity of information privacy law to counter the widely touted benefits of ALPR/ANPR in improving road safety and streamlining fine enforcement (O'Malley 2013:295). Finally, we raise questions about the value of Ontario's approach to information privacy through 'privacy by design' ('PbD') (Lippert and Walby 2013). By requiring police to invoke more stringent technical controls, such as improved data encryption (Diffie and Landau 2010) to comply with privacy requirements, PbD sanctions mass population surveillance and implicitly endorses claims of improved law enforcement efficiency, national security and public safety.

Order, technology, and road traffic control

ALPR/ANPR is part of the next generation of video surveillance (Norris 2011), which combines public camera surveillance with population analysis. Images taken from ALPR/ANPR can be automatically compared with other mass-population data stored in national databases operated and managed by government departments or private entities. Once discrete information, such as criminal, driving or by-law infraction records, is now digitally amalgamated. However, the extent to which technology is used in road traffic enforcement differs across jurisdictions.

O'Malley (2010) pinpoints three interrelated developments associated with the perceived necessity for new surveillance technology to assist with road traffic management. These are: the mass population surge that justifies automated modes of order maintenance to minimise the burdens of manually checking errant criminal and driving histories; the availability of technology as a suitable proxy for real-time enforcement measures, such as the use of checkpoints; and the concept of the 'dividual'. Dividualisation involves the aggregation of personalised identity records into 'masses, samples, data, markets, or *banks*' (Deleuze 1992:5 emphasis in original). In road traffic enforcement, 'data doubles' (Haggerty and Ericson 2000:613–4) emerge from the digitisation of vehicle registration, driver licensing and police enforcement records (O'Malley 2010:796). The primary identifier is the vehicle registration plate. Its unique signifier can be automatically linked to previous offences directly associated with the vehicle, including auto theft, emissions and safety violations, or lapsed registration. These vehicle records generate secondary links to the 'data double' of the registered vehicle owner that can reveal individual offences such as licence invalidity, outstanding fines or other recorded offences. The automated cross-matching of vehicle and individual licensing with criminal offence records is seemingly devoid of human error and can be linked to other forms of data administered by government or private organisations, such as computerised vehicle or personal insurance records that do not necessarily relate directly to road traffic enforcement.

A central variable in the relationship between privacy and efficient road traffic control is the ability of police to match data collected by multiple agencies. Historically, police maintained independent records of suspect vehicle registration plates, or manually inspected driving licences whenever a potential infraction was detected. Today, automated data matching is possible using technologies deployed by public vehicle registration, law enforcement or insurance authorities operating in different provincial, state or national jurisdictions. ALPR/ANPR offers the additional benefit of matching electronic information identifying a registration plate — and even the driver or passenger — at the time and location the image is recorded with existing police records, registration data or private tollway and insurance information. Records of previous 'hits' alert police to a suspect vehicle, indicating that further investigation into any criminal or regulatory breaches linked to that vehicle or its registered owner is warranted. Although the majority of vehicle plate information entered into ALPR/ANPR systems generates no alert warning, the technology automatically matches road traffic and criminal enforcement 'hits' to instantly identify registered drivers with relevant 'data doubles' that record outstanding fines or warrants as well as any number of additional legal infractions. The potential law enforcement gains of this form of 'mass surveillance' are clear given the cumbersome nature of manually sifting multiple police, registration or private road traffic databases. The efficient flow of information between multiple agencies is evident in the following description of how ALPR operates in British Columbia:

> A police officer who is not using ALPR visually identifies a vehicle of interest and enters its license plate number into a mobile workstation to query the ICBC, Canadian Police Information Centre ('CPIC') and Police Records Information Management Environment ('PRIME') databases. This provides the officer with information related to the license plate, such as the name of the registered owner, whether that owner has a driver's license, and whether the vehicle is insured. After evaluating the results, the officer decides whether or not further investigation is warranted (Denham 2012:11–12).

Some jurisdictions have imposed restrictions on the collection and retention of data about the movement of vehicles with no previous enforcement records, or 'non-hits'. For example, legislation in Maine, United States, requires police to remove all 'non-hit' data every 21 days. In Germany, a Federal Constitutional Court has ruled the retention of data about vehicles with no previous road traffic violations contravenes the right to 'informational self-determination' (Denham 2012:10). In the United Kingdom, ALPR/ANPR is used for various 'policing and intelligence purposes' (Derby 2011:160) and is admissible evidence in criminal trials. Data can be retained for up to two years for a specified enforcement purpose in accordance with relevant privacy and human rights laws (VLRC 2010:114; NPIA 2009:19). These divergent approaches to data retention contrast with the improved efficiencies of automated vehicle and driver identity verification through ALPR/ANPR and related law enforcement technologies. This tension highlights the importance of comparative inquiry into how privacy standards are established for this form of law enforcement surveillance.

Privacy is significant for all vehicle owners identified by ALPR/ANPR systems, regardless of their previous history of 'hits' and 'non-hits'. Equally, privacy is a significant concern when police deploy ALPR/ANPR to detect behaviour unrelated to road traffic control. These issues warrant consideration in light of police claims that ALPR/ANPR enhances traffic management, road safety and data sharing between law enforcement agencies, independently of its potential to assist with other criminal investigations. Before assessing these claims, it is necessary to outline how Canadian and Australian administrative law protects the right to privacy as a counterpoint to the mass collection and sharing of personal information among public and private organisations.

Canadian information privacy law and policy

Privacy laws are designed to limit technological intrusion and the uses of personal information by government and private agencies. However, the operation of these regulatory and compliance models differs in each provincial, state and national jurisdiction. Canada and Australia share similar multi-tiered administrative structures that aim to protect five key information privacy principles:

> *Control over information*, including the assurance that personal information will be used according to contractual arrangements;
>
> *Secrecy of information*, including the ability to escape surveillance or protect against unwanted prying, or access to anonymity;
>
> *Desire to protect personal space*, involving the psychological need to retreat to non-social space (even if in the public arena) to engage in individual activities;
>
> *Right to keep secrets*, involving rules defining institutional, social, political or administrative limits to collecting and sharing information;

> *Data security*, including the development of appropriate technical safeguards against unauthorized access to protected information (Leman-Langlois 2008:113).

In Canada, the foundation of privacy law is preserved by the *Charter of Rights and Freedoms*, which establishes 'the right to be secure against unreasonable search and seizure' (*Constitution Act 1982* (Can) s 8). Several common law rulings identify 'a reasonable expectation of privacy' as the key constraint on intrusive search and seizure procedures (Johnson 2011). Canada also has several national and provincial statutes establishing a compliance model for the use of surveillance and personal information by public and private organisations. The federal *Privacy Act 1985* (Can) governs the collection, use and right to access personal information from any national public service or 'government institution'. The federal *Personal Information and Electronic Documents Act 2000* (Can) ('*PIPEDA*') s 4) regulates the collection and use of personal information by private sector organisations for 'commercial activities'. Every Canadian province has a *Freedom of Information and Protection of Privacy Act* ('*FIPPA*') that regulates the collection of personal information by provincial government agencies, while Municipal Freedom of Information and Protection of Privacy Acts ('MFIPPA') apply to local government authorities, including many police agencies.[1] Federal and provincial Privacy Commissioners have powers to investigate complaints into suspected privacy breaches and distribute relevant compliance directives under their respective jurisdictions.

Within this multi-tiered public and private administrative legal structure, compliance largely depends on the trust conferred on public bureaucracies or private businesses. This has contributed to the 'uneven diffusion of systems' and standards for the administration of many law enforcement and crime-prevention technologies, including open space closed-circuit television (Hier and Walby 2011). Below we demonstrate the limited ability of provincial Privacy Commissions to implement clear and transparent standards for the use of surveillance technologies by law enforcement agencies. To do so, we examine ALPR data-sharing practices by the Victoria Police Department ('VICPD') in British Columbia ('BC') and the Royal Canadian Mounted Police ('RCMP').

ALPR data collected by VICPD was transferred to the equivalent RCMP database via a portable USB hard-drive. The aim was to identify 'hits' that detected stolen vehicles. RCMP personnel manually deleted the identities of all 'non-hit' vehicles with no recorded criminal or road traffic violations, but retained the time and location of all vehicles photographed by the VICPD system. The BC Privacy Commissioner criticised these data-sharing and retention practices. Most provinces expressly exempt police from informing citizens that their personal data is being collected and potentially exchanged with other agencies for a valid law enforcement, criminal intelligence or investigative purpose (*FIPPA 1996* (BC) s 33.1(2)(a) and sch 1; *FIPPA 1990* (Ont) ss 42(1)(f)–(g); Denham 2012:21). However, the 'indiscriminate reach' (Denham 2012:29) of ALPR in collecting 'information about the law-abiding activities of individuals that the police have no reason to believe relates to criminal activity' (Denham 2012:23) also contradicts principles of reasonable suspicion that require police to gather targeted evidence about crime suspects. Consequently, the Privacy Commissioner directed the Ministry of Justice to specify where and why ALPR was being deployed. VICPD was also directed to reconfigure its system to automatically 'delete personal information associated with "non-hits" immediately after the system determines it

[1] Canadian policing involves federal contracts between the Royal Canadian Mounted Police and provincial or municipal agencies. Australian state policing involves a combination of state and territory police agencies that collaborate with the Australian Federal Police ('AFP') on certain criminal investigations, while policing in the Australian Capital Territory is provided solely by the AFP under a renewable contract.

does not match a license plate number in the Alert Listing' (Denham 2012:28). However, VICPD Chief Jamie Graham 'respectfully disagreed' with this directive, arguing the benefits of improved law enforcement efficiency superseded concerns relating to maintaining the privacy of vehicles with no previous 'hits' entered into each ALPR database.

Aside from the Chief's challenging of this privacy ruling, the example reveals the acceptance of using technical constraints to protect information privacy as a key method of governing surveillance technologies in contemporary law enforcement. This approach is exemplified in Ontario, where Privacy Commissioner Ann Cavoukian pioneered the integration of PbD into law enforcement technologies (Lippert and Walby 2013). In recent public presentations, Commissioner Cavoukian has argued privacy law should not prevent law enforcement agencies from adopting new surveillance technologies, as PbD facilitates the use of 'security technologies enabling privacy' ('STEPS'). Cavoukian identifies numerous STEPS considered to successfully incorporate PbD, including 3-D body scanners to screen airline passengers, improved methods of biometric encryption, and technical protocols used in 'IT systems, accountable business practices, and physical design and networked infrastructure'. While promoting improved data protection, PbD also legitimises the introduction and normalisation of contentious new surveillance projects by Canadian law enforcement agencies. Ontario's PbD policy equates privacy with enhanced data security, while overlooking several additional dimensions of privacy regulation regarding the control of personal information and clarifying the institutional, social, political or administrative limits of its collection and use in contemporary law enforcement (Leman-Langlois 2013:113).

Australian information privacy law and policy

While Australia has no equivalent to Canada's constitutional protection against unreasonable search and seizure, federal (*Privacy Act 1988* (Cth)) and state (for example, *Information Privacy Act 2000* (Vic)) legislation empowers Privacy Commissioners[2] with equivalent investigative and compliance powers. Specific legislation also governs the collection, storage and dissemination of information using surveillance devices (*Surveillance Devices Act 1999* (Vic)). A national charter of rights does not exist, although in 2008 a non-binding legislative Charter of Human Rights and Responsibilities became fully operational in Victoria. This legislation includes a general 'right to privacy' aimed at preserving any person's 'family, home or correspondence' from unlawful or arbitrary interference under any legislative enactment, justiciable ruling or the activities of any state and municipal authorities (*Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13). There is no reasonable expectation of privacy regarding the use of surveillance devices in public spaces. A common law tort enables suspected invasions of privacy to be litigated in some jurisdictions as a proxy for the lack of explicit constitutional recognition of the right to privacy under Australian law (Butler 2005; NSWLRC 2007; VLRC 2010: 128–68).

State and Federal Privacy Commissioners commonly develop protocols or Codes of Conduct in collaboration with public and private sector industries governing the collection,

[2] From 1 November 2010, the Commonwealth Office of the Privacy Commissioner was integrated into the Office of the Australian Information Commissioner. This amended structure also applies at state level to oversee the implementation of extensive information privacy reforms introduced into the Australian Federal Parliament in May 2012.

use and disclosure of personal information for specified purposes. Several additional legislative requirements preserve the accuracy, security, international transfer and anonymity of an individual's data, but state legislation only applies to government and municipal authorities or small businesses with an annual turnover of A$3.6 million or less. Unlike Canada, where freedom of information is incorporated into privacy legislation, separate federal and state laws govern the disclosure of information held by public authorities. However, information regarding 'the prevention, detection, investigation, prosecution or punishment of criminal offences or breach of a law' and the 'protection of public revenue' (*Information Privacy Act 2000* (Vic) sch 1 ss 2.1(d)–(h)) is normally exempt from these provisions.

In general, Australian police agencies may use 'a data surveillance device, a listening device, an optical surveillance device or a tracking device' (ALRC 2008:415) without a warrant in a public place (*Surveillance Devices Act 1999* (Vic); NPIA 2009:18). Warrants are customarily obtained for the installation of tracking devices in private places, although some legal variations are evident in state legislation. For example, New South Wales allows 'the installation, use or maintenance of a tracking device for a lawful purpose' (*Surveillance Devices Act 2007* (NSW) s 9(2)(c); VLRC 2010:114) without a warrant. The terms 'law enforcement purpose' and 'crime' are particularly broad and are arguably the most significant barrier to reasoned public debate about the deployment of new surveillance technologies by Australian law enforcement agencies (Palmer and Warren 2012). There is further doubt about whether 'crime' includes regulatory infractions or road traffic infringements enforced by the public police. However, the artificial separation of competing privacy and security interests in contemporary law enforcement discourse mirrors equivalent concerns identified in Canadian and United States literatures (Solove 2011). This is of concern in light of CrimTrac's preference to host a centralised data storage and dissemination facility that maximises the 'national security' and 'community safety' benefits of ANPR technology, and the willingness of police to adopt untested surveillance and identity verification technologies to improve efficiencies in major criminal investigations, fine enforcement and crime prevention (Brown et al 2013; VLRC 2010).

ALPR and privacy in Ontario, Canada

The use of ALPR in Ontario precedes PbD, where it has been deployed at on- and off-ramps on a select number of tollways in the Greater Toronto Area since 1997. In 2003, a Mobile License Plate Recognition ('MLPR') system was piloted by the Toronto Police Service ('TPS') to help detect stolen vehicles in public car parks, which was subsequently investigated by the Office of the Information and Privacy Commissioner ('OIPC') in Ontario. A 'street sweeper' camera system developed by a Montreal company that marketed this technology to both government departments and private businesses was mounted atop a TPS vehicle. The images were then conveyed from the TPS system to the RCMP's Canadian Police Information Centre ('CPIC') database, where they were cross-matched with stolen vehicle records. On receiving an automatic alert identifying any 'hits' matching the MLPR photographs with CPIC data, the parking officer would save the scanned licence plate number in the MLPR system for further processing (OIPC 2003). These images could be retained for up to 72 hours. Reports indicated the pilot helped to recover 153 stolen vehicles and was widely applauded by police for offsetting the complexity and delays associated with manual investigations. The recovery of more stolen vehicles within 30 days of the initial report to police also generated cost savings to the insurance industry due to the marked reduction in the number of replacement vehicles issued to policyholders.

The OIPC investigated whether this use of MLPR complied with both national and provincial privacy requirements after a citizen alleged the 'street sweeper' violated constitutional protections against unreasonable search and seizure (*Constitution Act 1982* (Can) s 8). Commissioner Cavoukian examined whether the disclosure of all licence plate photographs to the corporation in Montreal — for evaluating the system's efficiency and eliminating false positives in the automated data-matching software — contravened the exemptions on the collection and distribution of personal information for 'law enforcement matters' under the *MFIPPA 2007* (Ont) ss 8 and 29. Cavoukian (OIPC 2003) noted licence plates are a form of personal information, as the unique number is assigned to an identifiable driver regardless of their previous history of 'hits' or 'non-hits'. However, the use of MLPR was considered a valid law enforcement activity under the *MFIPPA* because the TPS expressed a clear rationale for collecting, using and storing the photographic information to identify stolen vehicles. The disclosure of MLPR photographs to the Montreal company also complied with the *MFIPPA*, because TPS only transferred the licence plate image and no identifiable names or personal information associated with any photographed 'hits'. Cavoukian recommended police and third parties, such as the Montreal company, should sign contracts with specific clauses preventing the further disclosure of any personal information exchanged for an authorised law enforcement purpose under *MFIPPA*. TPS and any other law enforcement agencies contemplating the introduction of MLPR were instructed to undertake a privacy impact assessment with the OIPC's assistance.

From 2011, several police services across southern and central Ontario began using similar ALPR technologies. South Simcoe Police installed an ALPR system with the capacity to scan 750 licence plate numbers per officer shift compared to the usual 125 undertaken through manual searches. This pilot involved the installation of a C$17 000 camera system on a police vehicle operated by the Traffic and Marine Unit. One police operator remarked that 'it will do the job of an officer' and 'it makes me twice as efficient as I could be' (King 2011). However, such claims provide limited insight into the effectiveness of this technology to reduce prohibited behaviours. In addition, numerous 'false hits' were identified in this pilot as the Ontario licence plate is especially difficult for the technology to read. In 2011, the Ontario Provincial Police ('OPP') also commenced a pilot involving the installation of ALPR technology in four cruisers and an SUV operating near the cities of London and Cornwall. This mobile deployment was vetted by Commissioner Cavoukian to ensure all 'non-hit' information conformed to PbD requirements and was retained for no more than 20 minutes.

In 2012, Ottawa Police Service ('OPS') began using ALPR, but its widespread adoption was stalled pending a series of public consultations and the completion of a privacy impact assessment at Commissioner Cavoukian's insistence. Although the OPS ALPR system purged all 'non-hit' data every 20 minutes, Cavoukian advocated automatic deletion in line with PbD requirements (Boutilier 2013). A subsequent video blog titled 'Commissioner's Corner' reiterated Cavoukian's position that PbD can be integrated in all ALPR systems without compromising individual privacy:

> Our [OIPC's] interest is making sure the people who are not on the hit list, their information is not retained … What I have asked our police forces in Ontario to do is that whenever there is a non-hit, I want that information automatically deleted … from the system immediately because it does not even belong there.

Police officials in Ontario endorse PbD because it adds legitimacy to new forms of mass surveillance and automated data sorting that improve law enforcement efficiency. While Australian Privacy Commissioners have yet to examine ANPR as extensively as

Commissioner Cavoukian, below we suggest PbD has limited capacity to quell the appeal of this technology.

ANPR and privacy in Victoria, Australia

ANPR is part of an array of road safety initiatives introduced throughout Australia since the 1960s to assist police to 'combat dangerous driving and bring down the road toll' (Hamblin 2013). In the early 1990s, Victoria's vehicle registration authority first incorporated ANPR into fixed-speed and red-light cameras at accident 'hot spots' throughout the state. Since 2010, ANPR has been installed in several police vehicles 'to record the details of passing vehicles and detect those that may be unregistered or stolen' or 'to search for persons of interest' (VLRC 2010:114). ANPR also enables vehicles linked to outstanding toll payments, lapsed registration and dangerous driving offences to be identified as 'hits'. Stolen vehicles can also be manually flagged in police systems and automatically compared with photographs of thousands of vehicles taken at a particular place or time, either through privately administered systems or equivalent technologies operated by interstate or federal police agencies.

Victoria's ANPR system records the time, date and location where the image of the vehicle's front licence plate was taken. This data is then automatically cross-matched with relevant police and vehicle registration records. Since 2012, 'up to six vans fitted with ANPR cameras, which can scan up to 2600 plates an hour' (Harris and Moor 2012) have been deployed after several trials conducted throughout the state since September 2009 involving the collection of over 300 000 vehicle records and the detection of over 6000 road traffic offences (VLRC 2010:33). Victoria's BlueNet ANPR system is considered to situate Victoria Police as Australia's leading 'innovative thinkers in the space of road policing enforcement' (Hooper 2013:15) and is widely publicised as a necessary deterrent in line with various other automated road surveillance systems, such as speed and red-light cameras (VLRC 2010:37, 61; O'Malley 2013).

The BlueNet system is linked to databases enabling the rapid identification of 'illegal vehicles' for further interception and formal processing. Its mobility enhances the 'strategic targeting of high-risk unauthorised drivers, unregistered vehicles and high-risk areas' (Kaila 2012). BlueNet automatically matches photographic data with 'hot lists' of 'stolen vehicles, expired registration and vehicles whose registered owner is disqualified … or who is wanted for non-payment of fines or other offences' (Staff Writer 2011). Claims that more than one-eighth of fatal motor vehicle accidents involve unlicensed drivers or unregistered vehicles (Harris and Moor 2012) add legitimacy to ANPR in helping to reduce annual road fatality rates and accident-related trauma in Victoria.

The launch of Operation Break Up in late 2012 highlighted BlueNet's capacity to detect road traffic violations in Victoria's beachside resort towns (Kaila 2012). A report in Geelong during January 2013 indicated '(o)ne in every 70 people checked by police … faced fines or charges' (Hamblin 2013), while over 6000 vehicles scanned in one day at the Mornington Peninsula during the Australia Day long weekend identified 973 vehicles linked to outstanding warrants and A$300 000 in unpaid fines. This 'hit' rate exceeds 16 per cent for outstanding warrants alone, with fines involving various breaches of minor licensing requirements, such as failing to inform road traffic authorities of a change of address, as well as numerous vehicle registration, noise emissions and related safety violations (Evans 2013; Hamblin 2013). The Department of Justice (2013) has also introduced ANPR to 'enhance Sheriff's Operations … to crack down on unpaid fines and outstanding warrants'.

The deterrent value of ANPR is therefore clear, given its potential to enhance the detection of road traffic offences, parking violations and unpaid fines.

Neither Victorian nor national privacy regulators have examined ANPR. A holistic examination of the national privacy regime by the Australian Law Reform Commission ('ALRC') (2008) referred briefly to the potential of CCTV and ANPR to 'reduce the need for live monitoring of surveillance systems and reduce costs associated with recording irrelevant activity when used with "intelligent software"' (ALRC 2008:414), such as pattern (VLRC 2010:114) or facial recognition technology (Information Integrity Solutions 2008:8). However, this report offered little regulatory guidance for managing data obtained or stored in these systems. A major review of ANPR by a Queensland Parliamentary Committee highlighted the value of automated 'traffic surveillance' to improve police 'operational efficiency', while contributing to improvements in 'public order and public health by way of reduced road crashes' (Parliamentary Travelsafe Committee 2008:1, 16). ANPR is considered valuable when used in conjunction with random breath and drug testing, given the latter is currently unable to detect illicit drugs that might contribute to driver impairment (Wilson 2012). Mobile vehicle tracking can also assist with criminal investigations (VLRC 2010:61) and has been used to seize firearms from known 'gangsters'. Senior police extol the benefits of ANPR in helping to intercept 'the same targets three times in three different unregistered cars … in one night' (Staff Writer 2011).

An investigation by the Victorian Law Reform Commission ('VLRC') (2010) recommended the establishment of an independent body to regulate all forms of electronic surveillance deployed in public places by government authorities and law enforcement agencies. Part of this organisation's mandate would involve receiving periodic reports about the use of ANPR by Victoria Police and other public organisations involved in road traffic control and vehicle licensing; the incremental review of any regulatory requirements; and articulating a reasonable expectation of privacy in public places to ensure the responsible and proportionate use of surveillance remains confined to 'legitimate' public administrative functions. The VLRC did not consider that ANPR contravened restrictions associated with optical surveillance devices, which are not to be used to monitor activity in public spaces (VLRC 2010:114). However, Victoria Police considered any restrictions on the use of tracking devices were 'administratively unworkable' given the need 'to obtain a warrant each time they wish to use ANPR'. Supplementary statements highlighting the value of ANPR for 'emergency services in the case of missing persons' and the contradiction of allowing Victoria's road traffic authority and private 'tollway operators … to continue to use ANPR for road safety and tolling purposes' were also noted (VLRC 2010:114). The VLRC questioned current 'vague and unnecessarily broad' legislation enabling police to deploy tracking devices 'without consent' and capture 'vast amounts of information about individuals who are behaving lawfully', while legitimising 'function creep' and the use of ANPR data for 'unintended purposes' (VLRC 2010:115). Regulatory options included the introduction of warning signs indicating where and when police deployed ANPR, and specific legislation governing the use of ANPR data for law enforcement purposes.

CrimTrac's proposed nationalisation of vehicle registration data can be viewed as part of the ongoing centralisation of Australia's strategic law enforcement priorities since the late 1990s (James and Warren 2010). In 2006, CrimTrac commissioned a scoping study into ANPR based on consultations with representatives from all state police services, the Australian Federal Police and various national criminal intelligence and transportation authorities (CrimTrac 2009a:46). While the final report has not been publicly released (Senate Standing Committee on Legal and Constitutional Affairs 2008), various sources indicate the preference for 'an integrated national ANPR network' (CrimTrac 2009b:30)

with a centralised data management and distribution capacity (Derby 2011:164), or the development of 'common standards' for the 'interoperability' of discrete systems already introduced by Australia's state policing services (CrimTrac 2010:56). The centralised coordination of ANPR data flows promises significant road safety improvements, and efficient interagency cooperation to enhance national security and border control (Information Integrity Solutions 2008). Independent consultations with privacy regulators and various community advocacy groups raised concerns over whether it was 'necessary' to collect information relating to vehicles associated with no previous road traffic or criminal violations, enable such data to be shared on a national basis, or allow for its subsequent de-identification and centralised storage for up to five years. The report ultimately found these concerns did not offset the logical 'business case' favouring ANPR to improve law enforcement efficiency, reduce the cost of criminal investigations, enhance road safety in known accident 'hot spots' and produce financial benefits for all road users through reduced insurance premiums.

Although PbD is not expressly adopted in Australia, Victoria Police must invoke appropriate 'cryptographic controls' for all surveillance technologies and electronic data (CLEDS 2007:48–53). However, in 2010 an independent review found many internal data management policies did not comply with appropriate encryption or security standards (Office of Police Integrity 2010:8). Law enforcement exemptions ensure state and national privacy regulators do not review police information management policies.

The scant attention to the privacy implications of ANPR in Victoria and nationally is disconcerting in light of Queensland's Parliamentary investigation in 2008. This report identified the need for several procedural safeguards, including 'clearly articulated purposes' for the collection, distribution and use of ANPR data; clear restrictions on the agencies and personnel allowed to access personal information; the immediate removal of data relating to vehicles with no offence history; and the introduction of secure data transportation, access, exchange and encryption arrangements. This last recommendation incorporates the logic of PbD within a holistic independent regulatory and complaints structure, with the power to impose 'severe penalties' for data misuse (Parliamentary Travelsafe Committee 2008:21). However, these issues remain unheeded in light of CrimTrac's proposed national approach to ANPR and recent developments associated with Victoria's mobile BlueNet system.

Questioning ALPR/ANPR

The artificial divide between privacy and security (Solove 2011) associated with mobile and fixed ALPR/ANPR systems raises an additional question of whether this technology is effective in reducing road traffic violations. While the efficient recovery of stolen vehicles might reduce insurance premiums for the benefit of all road users, the capacity for increased camera surveillance to alter driver behaviour and improve road safety remains debatable. Of concern is the reliance on questionable data-profiling techniques in deploying ALPR/ANPR at specific locations, during particular time periods or against certain classes of road users considered at risk of causing accidents that might lead to serious injury or death. Harcourt (2007) provides a useful two-phase critique that suitably reveals these limits of ALPR/ANPR technology.

According to Harcourt, the deployment of fixed or mobile ALPR/ANPR systems at particular locations based on higher 'hit rates' compared with other geographic areas constitutes a form of profiling. To justify using camera surveillance and automated data

matching at 'hot spots' or during 'hot times' would involve proof that such deployment will decrease overall levels of prohibited driving behaviour or infractions beyond these locations and times. Attributing longer-term decreases in prohibited behaviour to the use of these technologies, as can be seen in the justifications for ANPR in Australia (Kaila 2012), is also ill-conceived, as such reductions may be due to numerous factors, including changing attitudes toward driving, improved vehicle and road design, and increases in informal forms of regulation (O'Malley 2013). To the extent that ALPR/ANPR is video surveillance, justifying its introduction in line with the Ontario Privacy Commissioner's guidelines requires showing other less intrusive law enforcement technologies have been tried and were found to be ineffective (OIPC 2007). Alternatives to ALPR/ANPR do not appear to have been considered in either Ontario or Victoria. The primary motives for introducing this technology seem to be improved road safety via rapid recovery of stolen vehicles and streamlined enforcement of outstanding warrants and fines for offences likely to be unrelated to driving and traffic control.

Harcourt (2007:23–5) would argue that effectiveness is best judged by considering the comparative 'elasticity' between groups in targeted locations and those in other locations immune from ALPR/ANPR surveillance. If drivers in targeted locations are less elastic in changing their driving behaviour than those in other locations, or if drivers in other locations are more elastic than those in targeted locations, ALPR/ANPR will have no deterrent effect. Disproportionate targeting might even increase aggregate driving violations. This means that using trends in recorded hit rates as the measure for deciding where to locate ALPR/ANPR cameras in the hope of maximising the potential to detect further violations can *increase* the prohibited driving behaviour within the jurisdiction. Harcourt's insightful claim about comparative 'elasticity' has not been considered in relation to any aforementioned road safety initiatives, and depends on the type of behaviour targeted and the use of predictive actuarial methods to decide where, when and which technologies to deploy to help detect these violations.

To offer one of many possible examples, imagine the failure to update annual vehicle registration details as a symptom of disproportionate surveillance targeting motorists in certain low-income areas or resort locations at peak holiday times. Those with prior 'hits' may have comparatively less income, time after work hours or other practical burdens to impede compliance compared with middle-income earners residing in locations where ALPR/ANPR is not deployed. The latter group may recognise their area is rarely targeted for road traffic surveillance and feel freer to let their registrations lapse than previously. Their preparedness to challenge financial penalties or seek concessions to the strict enforcement of licensing violations (O'Malley 2013) reinforces the continuance of profiling in recognised 'hot spots'.

The 'ratchet effect' is an additional self-fulfilling element of law enforcement surveillance. Proportionately higher 'hit rates' in certain communities provide the strategic evidence to justify repeated deployment of ALPR/ANPR in 'hot spots', while other areas remain immune from surveillance (Harcourt 2007:147). Such profiling might legitimise further discriminatory targeting of certain population groups or regions, based on empirical claims that 'unauthorised drivers create extra risks on our roads and are commonly over-represented in road trauma' (Kaila 2012). These patterns are identified in the disproportionate use of mobile vehicle surveillance in some urban enclaves across the United States (Meehan and Ponder 2002; Koper, Taylor and Woods 2013). The fully randomised deployment of mobile ALPR/ANPR systems regardless of location is one possible remedy to enhance the prospect that all drivers in all locations could potentially be

subject to police surveillance. Although randomised spatial deployment is impossible with fixed ALPR/ANPR cameras, Victoria's mobile BlueNet system makes this feasible.

However, when applied to ALPR/ANPR, Harcourt's critique of profiling loses some footing where population management is based on abstracted notions of 'dividualism', 'data doubles' and their assemblage across multiple policing agencies (Haggerty and Ericson 2000) through centrally coordinated information flows via identical or interoperable technologies. If ALPR/ANPR resources are equally distributed geographically and temporally, comparative elasticity is eroded as 'the profile becomes the population' and all road users become subject to ubiquitous surveillance. Harcourt did foresee that each enforcement ratchet would produce fewer differences between 'hits' and 'non-hits'. This reasoning presumes that the rationale for the placement of surveillance technologies requires constant upgrading or randomisation. While Ontario guidelines indicate that police must justify resource deployment, there is no evidence to suggest this is happening. In Victoria, this occurs through periodic road traffic blitzes in certain locations or during holiday periods. These rather loose justifications allow targeted surveillance to become mass surveillance, as per the CrimTrac model. As such, Harcourt's critique may become outmoded before it can be systematically applied to question surveillance practices in contemporary law enforcement.

One key objective of CrimTrac's preference for national ANPR data management involves maximising the potential for rapid automated electronic data sorting. However, this proposal is also subject to resistance from state police. Victoria Police representatives have expressed the preference to retain the ability to select 'operational systems and architecture' that best suit local information and intelligence requirements. Rather than supporting a 'massive national system', this logic favours greater interoperability between discrete or established systems, so data 'can be easily shared between and accessed by other agencies' (Parliamentary Joint Committee on Law Enforcement 2012:5–6). Broader definitions of 'enforcement related activity' to encompass 'surveillance … intelligence gathering activities and other monitoring … protective or custodial activities' (Parliament of the Commonwealth of Australia 2012:58) under proposed amendments to national privacy laws favour both state and national policing, security and safety interests. However, this shift also reinforces ongoing tensions between federal and state power over information management that gradually creep towards nationalisation while encountering new modes of state police resistance. This tension replicates political debates associated with new forms of state surveillance that are commonly challenged by dedicated individuals and interest groups using the very platforms upon which such surveillance depends (O'Malley 2013).

Perhaps the most salient issue challenges arguments that suggest personal information no longer matters to surveillance processes. This claim is significant in relation to the use of technology by police agencies to detect crime and promote road safety in each jurisdiction. Even unified willingness to deploy ALPR/ANPR for improved criminal investigations and streamlined fine enforcement confronts significant legal and cultural distinctions relating to the permissible scope of law enforcement surveillance. While municipal policing in Canada contrasts with Australia's larger state agencies, the purpose of 'law enforcement' is open to constitutional protection and certain presumptions involving reasonable suspicion relating to surveillance in public and private spaces. This issue has far less resonance in Australia, partly due to the longstanding acceptance of ANPR, 'random breath testing' and red light cameras. Hence, the creep of population surveillance is more considerable on Australia's roads. This promises to extend to other classes of road users — motorcyclists — who have traditionally not been legally required to display a front numberplate due to ongoing debates regarding the development of an appropriate and safe mode of attachment. Victoria Police

claim 'almost 20 000 riders who sped past Victoria's front-facing traffic cameras' since 2009 have successfully avoided up to 25 000 unenforceable demerit points and A$4 million in fines (Moor 2013). Therefore, the cultural acceptance of reducing road deaths and injury at all costs through blanket ANPR surveillance is easy to imagine in contemporary Australia.

However, the alternative 'Canadian way' involving PbD is unlikely to curb enthusiasm for the efficiencies promised by ALPR. One contradiction we have noted is that PbD legitimates new mass surveillance practices. This finding has international relevance, as Privacy Commissions face numerous challenges in garnering compliance with privacy protocols, while PbD enables the efficient incorporation of a technical design rubric that accepts the inevitability of more surveillance that happens to play by certain rules. Whether this approach protects individual privacy or promotes greater road safety through the acceptable deployment of new technologies remains as contentious as Australia's pervasive expectation of mass road traffic surveillance and a proposed national ANPR data repository.

Conclusion

New automated law enforcement technologies raise the prospect of expanding electronic surveillance or digital dragnets into the lives of ordinary citizens. Such technologies erode legal requirements for reasonable suspicion that provide due process protections under the criminal law. Indeed, the idea that personal data should only be used for purposes related to its original collection is fading. As digital sorting capacities expand, new laws and technological developments legitimise contentious data-sharing practices among multiple public and private agencies. The schism between regulating individual privacy, criminal enforcement and new securitisation measures continues as the capacity for data sharing now transcends international borders and accepted information privacy and security requirements (Rule 2007). The potential integration of road traffic safety and national security in some contexts is especially contentious for conflating the scales of security and facilitating the expansion of various pre-crime and preventative policing measures, such as enhanced stop, search, identity verification and seizure powers (see Zedner 2009). Additional concerns regarding false positives, data protection and the movement of individuals with no prior criminal history add weight to concerns about the viability of privacy protections associated ALPR/ANPR.

Harcourt's (2007) critique of law enforcement profiling may become weaker in the increasingly dividuised contexts of road traffic enforcement, when 'the profile becomes the population' through the deployment of ALPR/ANPR. Nevertheless, this approach raises the fundamental and frequently avoided question of ALPR/ANPR's efficacy in reducing prohibited behaviours, rather than its widely recognised benefits in enhancing police efficiency. Perhaps of greatest concern is that neither PbD in Canada, nor Australia's distinct lack of privacy protocols for the use of ANPR, prevent the expanded use of these systems or related surveillance technologies in contemporary law enforcement.

Statutes

Charter of Human Rights and Responsibilities Act 2006 (Vic)

Constitution Act 1982 (Can)

Freedom of Information and Protection of Privacy Act 1996 (BC)

Freedom of Information and Protection of Privacy Act 1990 (Ont)

Information Privacy Act 2000 (Vic)

Municipal Freedom of Information and Privacy Protection Act 2007 (Ont)

Personal Information Protection and Electronic Documents Act 2000 (Can)

Privacy Act 1985 (Can)

Privacy Act 1988 (Cth)

Surveillance Devices Act 2007 (NSW)

Surveillance Devices Act 1999 (Vic)

References

Australian Law Reform Commission ('ALRC') (2008) *For Your Information: Australian Privacy Law and Practice* (Report 108) (12 August 2008) <http://www.alrc.gov.au/publications/report-108>

Boutilier A (2013) 'License Scanners: Privacy Chief Wants Ottawa Police to Work With Her', *Metro News* (online), 8 January 2013 <http://metronews.ca/news/ottawa/500995/licence-scanners-privacy-chief-wants-ottawa-police-to-work-with-her/>

Briody M and Prenzler T (2005) 'DNA Databases and Property Crime: A False Promise' (2005) 37(2) *Australian Journal of Forensic Sciences* 73

Brown M, Landsdell G, Saunders B and Eriksson A (2013) '"I'm sorry but you're just not that special …" Reflecting on the "Special Circumstances" Provisions of the *Infringements Act 2006* (Vic)' (2013) 24(3) *Current Issues in Criminal Justice* 375

Butler D (2005) 'A Tort of Invasion of Privacy in Australia' (2005) 29(2) *Melbourne University Law Review* 339

Cavoukian A (2011) 'Find Ways to Deliver Both Security and Privacy', Presentation delivered at the Canadian Society for Industrial Security Annual Meeting, 30 May 2011, IPC <http://www.ipc.on.ca/english/Resources/Presentations-and-Speeches/Presentations-and-Speeches-Summary/?id=1074>

Commissioner for Law Enforcement Data Security ('CLEDS') (2007) *Standards for Victoria Police Law Enforcement Data Security* (July 2007) <http://www.cleds.vic.gov.au/content.asp?document_id=11976>

Cousineau M (2013) 'The Global War on Terror and Automatic License Plate Recognition' (2013) 50(1) *Canadian Review of Sociology* 74

CrimTrac (2008) *Annual Report 07–08* (September 2008) <http://www.crimtrac.gov.au/documents/AnnualReport0708-FullReport.pdf>

CrimTrac (2009a) *Annual Report 2008–09* (September 2009) <http://www.crimtrac.gov.au/documents/Crimtrac_0809_full.pdf>

CrimTrac (2009b) *CrimTrac Overview 2009* (June 2009) Commonwealth of Australia <https://senate.aph.gov.au/submissions/comittees/viewdocument.aspx?id=dd60984f-33e2-4836-85a4-690052ca7914>

CrimTrac (2010) *CrimTrac Annual Report 2009–2010* (September 2010) Commonwealth of Australia <http://www.crimtrac.gov.au/documents/CrimTrac_0910_full.pdf>

Deleuze G (1992) 'Postscript on the Societies of Control' (1992) 61 *October* 3

Denham E (2012) *Use of Automated Licence Plate Recognition Technology by the Victoria Police Department* (Investigation Report F12-04) (15 November 2012), Office of the Information and Privacy Commissioner for British Columbia <http://www.oipc.bc.ca/rulings/investigation-reports.aspx>

Department of Justice (Vic) (2013) 'Automatic Number Plate Recognition' <http://www.justice.vic.gov.au/home/justice+system/sheriffs+in+victoria/automatic+number+plate+recognition>

Derby P (2011) 'Policing in the Age of Information: Automated Number Plate Recognition' in Doyle A, Lippert R and Lyon D (eds), *Eyes Everywhere: The Global Growth of Camera Surveillance*, Routledge, 2011

Diffie W and Landau S (2010) *Privacy on the Line: The Politics of Wiretapping and Encryption*, MIT Press, 2nd ed, 2010

Evans J (2013) 'Police Nab More than 1000 Motorists Using New BlueNet Number Plate Technology', *Herald Sun* (online), 29 January 2013 <http://www.heraldsun.com.au/news/law-order/police-nab-more-than-1000-motorists-using-new-bluenet-number-plate-technology/story-fnat79vb-1226564337115>

Gaumont N and Babineau D (2008) 'The Role of Automatic License Plate Recognition Technology in Policing: Results from the Lower Mainland of British Columbia', *The Police Chief* (online), November 2008 <http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1671&issue_id=112008>

Hamblin A (2013) 'Hi-tech Police Patrol Nabs Offenders', *Geelong Advertiser* (online), 14 January 2013 <http://onsale.geelong.com/articles/2013/01/14/Hi-tech_police_patrol_nabs_offenders/>

Harcourt B (2007) *Against Prediction*, University of Chicago Press, 2007

Harris A and Moor K (2012) '"Cops" Hoon Trap in the Suburbs', *Herald Sun* (online), 2 April 2012 <http://www.heraldsun.com.au/archive/news/cops-hoon-trap-in-the-suburbs/story-fn7x8me2-1226315924326>

Harris K D (2013) *Privacy on the Go: Recommendations for the Mobile Ecosystem* (January 2013) State of California Department of Justice <http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf>

Hier S P and Walby K (2011) 'Privacy Pragmatism and Streetscape Video Surveillance in Canada' (2011) 16(2) *International Sociology* 844

Hooper S-J (2013) 'Leading the Way in Road Policing', *Police Life: The Victoria Police Magazine* (online), Autumn 2013, 14–15 <http://issuu.com/policelife/docs/policelife_autumn2013>

Information and Privacy Commissioner ('IPC') (2003) *Privacy Investigation: The Toronto Police Service's Use of Mobile License Plate Recognition Technology to Find Stolen Vehicles* (29 April

2003) Information and Privacy Commissioner/Ontario <http://www.ontla.on.ca/library/repository/mon/5000/10311696.pdf>

Information and Privacy Commissioner ('IPC') (2007) *Guidelines for Using Video Surveillance Cameras in Public Places* (September 2007) Information and Privacy Commissioner/Ontario <http://www.ipc.on.ca/images/Resources/video-e.pdf>

Information Integrity Solutions (2008) *Privacy Impact Assessment Consultation Paper: Automatic Number Plate Recognition CrimTrac Scoping Study*, June 2008 <http://www.privacy.org.au/Papers/ANPR-Background-Paper.doc>

James S and Warren I (2010) 'Australian Police Responses to Transnational Crime and Terrorism' in Eterno J A and Das D K (eds), *Police Practices in Global Perspective*, Rowman & Littlefield, 2010

Johnson M (2011) 'Status Quo Surveillance — The Legal Framework for Camera Surveillance in Canada' in Doyle A, Lippert R and Lyon D (eds), *Eyes Everywhere: The Global Growth of Camera Surveillance*, Routledge, 2011

Kaila J (2012) 'BlueNet Police Car Can Detect Unregistered Vehicles and Unlicensed Drivers While on the Move', *Herald Sun* (online), 14 December 2012 <http://www.heraldsun.com.au/news/law-order/bluenet-police-car-can-detect-unregistered-vehicles-and-unlicensed-drivers-while-on-the-move/story-fnat79vb-1226536679894>

Koper C S, Taylor B G and Woods D J (2013) 'A Randomized Test of Initial and Residual Deterrence from Directed Patrols and Use of License Plate Readers at Crime Hot Spots' (2013) 9(2) *Journal of Experimental Criminology* 213

King M (2011) 'Tech Could Make Traffic Cops "Twice as Efficient"', *The Barrie Examiner* (online), 13 June 2011 <http://www.thebarrieexaminer.com/2011/06/13/tech-could-make-traffic-cops-twice-as-efficient>

Leman-Langlois S (2008) 'Privacy as Currency: Crime, Information and Control in Cyberspace' in Leman-Langlois S (ed), *Technocrime: Technology, Crime and Social Control*, Willan Publishing, 2008

Lippert R and Walby K (2013) 'Governing through Privacy: Authoritarian Liberalism, Law, and Privacy Knowledge', *Law, Culture and the Humanities* (online), 26 March 2013 <http://lch.sagepub.com/content/early/2013/03/21/1743872113478530.abstract>

McArthur K (2012) *ALPR and Digital Civil Rights* (16 November 2012) Unrest.ca <http://www.unrest.ca/alpr-update-commissioners-investigation-report-released>

Meehan A J and Ponder M C (2002) 'Race and Place: The Ecology of Racial Profiling African American Motorists' (2002) 19(3) *Justice Quarterly* 399

Moor K (2013) 'Motorcyclists are Free to Speed and Dodging Fines without Front Identification', *Herald Sun* (online), 6 May 2013 <http://www.heraldsun.com.au/news/law-order/motorcyclists-are-free-to-speed-and-dodging-fines-without-front-identification/story-fnat79vb-1226635623691>

Murphy P (2010) 'Police Boost Their Spy Equipment', *Herald Sun* (online), 2 December 2010 <http://www.heraldsun.com.au/ipad/police-boost-their-spy-equipment/story-fn6bfkm6-1225964107070>

National Policing Improvement Agency ('NPIA') (2009) *Practice Advice on the Management and Use of Automatic Number Plate Recognition*, Association of Chief Police Officers <http://www.acpo.police.uk/documents/crime/2009/200907CRIANP01.pdf>

New South Wales Law Reform Commission ('NSWLRC') (2007) *Invasion of Privacy* (Consultation Paper 1) (May 2007) New South Wales Law Reform Commission <http://www.lawreform.lawlink.nsw.gov.au/agdbasev7wr/lrc/documents/pdf/cp01.pdf>

Office of Police Integrity (2010) *Information Security and the Victoria Police State Surveillance Unit* (February 2010) IBAC <http://www.ibac.vic.gov.au/docs/default-source/opi-parliamentary-reports/information-security-and-the-victoria-police-state-surveillance-unit---feb-2010-.pdf?sfvrsn=4>

O'Malley P (2010) '"Simulated Justice": Risk, Money and Telemetric Policing' (2010) 50(5) *British Journal of Criminology* 795

O'Malley P (2013) 'The Politics of Mass Preventive Justice' in Ashworth A, Zedner L and Tomlin P (eds), *Prevention and the Limits of the Criminal Law*, Oxford University Press, 2013

Palmer D and Warren I (2012) 'Tecnología de Vigilancia y Controles Territoriales: Gobernanza y el Pulso de la Privacidad' ('Surveillance Technology and Territorial Controls: Governance and the "Lite Touch" of Privacy'), 217 *Novatica* 217 (May–June 2012) 15

Palmer D, Warren I and Miller P (forthcoming a) 'Privacy, Dataveillance and Crime Prevention' in Michael K and Abbas R (eds) *Encyclopedia of Social Network Analysis and Mining* ('ESNAM'), Springer

Palmer D, Warren I and Miller P (forthcoming b) 'ID Scanners and Überveillance in the Night Time Economy: Crime Prevention or Invasion of Privacy?' in Michael K and Michael M G (eds), *Überveillance and the Social Implications of Microchip Implants: Emerging Technologies*, IGI Global, Hershey

Parliament of the Commonwealth of Australia (2012) Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (23 May 2012) <http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fems%2Fr4813_ems_00948d06-092b-447e-9191-5706fdfa0728%22>

Parliamentary Joint Committee on Law Enforcement (2012) *Gathering and Use of Criminal Intelligence* (27 September 2012) Parliament of Australia <http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;adv=yes;orderBy=customrank;page=0;query=anpr;rec=0;resCount=Default>

Parliamentary Travelsafe Committee (Qld) (2008) *Report on the Inquiry into Automatic Number Plate Recognition Technology* (Report 51) (September 2008) Queensland Parliament <http://www.parliament.qld.gov.au/documents/committees/TSAFE/2007/anpr_technology/anpr_report.pdf>

Rule J B (2007) *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience*, Oxford University Press, 2007

Senate Standing Committee on Legal and Constitutional Affairs (2008) 'CrimTrac' (Question 105) (20 October 2008) Commonwealth of Australia, Canberra <http://www.aph.gov.au/~/media/Estimates/Live/legcon_ctte/estimates/bud_0910/ag/QON_105_CRIMTRAC.ashx>

Solove D J (2011) *Nothing to Hide: The False Tradeoff between Privacy and Security*, Yale University Press, 2011

Staff Writer (2011) 'Mobile Automatic Number Plate Recognition Cameras Targetting Gangsters', *Herald Sun* (online), 4 November 2011 <http://www.heraldsun.com.au/news/victoria/snapping-up-suspect-vehicles/story-fn7x8me2-1226185131059>

Victorian Law Reform Commission ('VLRC') (2010) *Surveillance in Public Places* (Final Report 18) (1 June 2010) <http://www.lawreform.vic.gov.au/projects/surveillance-public-places/surveillance-public-places-final-report>

Wilson L-A (2012) 'Exploring Illicit Drug Use and Drug Driving as Edgework' (2012) 24(2) *Current Issues in Criminal Justice* 223

Zedner L (2009) *Security*, London, 2009