novática
Revista de la Asociación de Técnicos de Informática

Novática, founded in 1975, is the oldest periodical publication amongst those specialized in Information and Communications Technology (ICT) existing today in Spain. It is published by **ATI** (*Asociación de Técnicos de Informática*) which also publishes **REICIS** (*Revista Española de Innovación, Calidad e Ingeniería del Software*).

<http://www.ati.es/novatica/>
<http://www.ati.es/reicis/>

ATI is a founding member of **CEPIS** (Council of European Professional Informatics Socities), an organization with a global membership of above 200,000 European informatics professionals, and the Spain's representative in **IFIP** (International Federation for Information Processing), a worldwide umbrella organization for national societies working in the field of information processing. It has a collaboration agreement with **ACM** (Association for Computing Machinery) as well as with **AdaSpain**, **AI2**, **ASTIC**, **RITSI** and **Hispalux** among other organisations in the ICT field.

Editorial Office, Advertising and Madrid Office
Plaza de España 6, 2ª planta, 28008 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Layout and Comunidad Valenciana Office
Av. del Reino de Valencia 23, 46005 Valencia; Tlfn. 963740173 <novatica_prod@ati.es>
Accounting, Subscriptions and Catalonia Office
Via Laietana 46, ppal. 1ª, 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>; <novatica.subscripciones@atinet.es>
Aragon Office
Lagasca 9, 3-B, 50006 Zaragoza Tlfn./fax 976235181 <secreara@ati.es>
Andalucía Office <secreand@ati.es>
Galicia Office<secregal@ati.es>
Advertising Plaza de España 6, 2ª planta, 28008 Madrid.
Tlnf.914029391; fax.913093685 <novatica@ati.es>
Legal deposit: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Cover Page: Dancing House - Concha Arias Pérez / © ATI
Layout Design: Fernando Agresta / © ATI 2003

Special English Edition
2012/2013 Annual Selection of Articles

summary

Surveillance Technology and Territorial Controls: Governance and the 'Lite Touch' of Privacy

Darren Palmer[1], Ian Warren[2]
[1]Chair Australian Surveillance Studies Group, Criminology, School of Humanities and Social Sciences, Deakin University, Geelong (Australia); [2]Senior Lecturer in Criminology, Australian Surveillance Studies Group, School of Humanities and Social Sciences, Deakin University, Geelong (Australia)

<{darren.palmer,ian.warren}@deakin.edu.au>

Abstract: *The considerable growth of surveillance technologies, dataveillance and digital information processing has occurred across many domains, including the night-time economy. We explore a particular technology (ID scanners) and the connections between this form of surveillance and associated database construction with the broader use of new forms of territorial governance. In turn, we argue that privacy, at least in the context of Australia, has limited influence on the use of new and untested surveillance technologies in contemporary law enforcement. In part, this is due to the construction of current Australian privacy laws and oversight principles. We argue this in itself does not solely account for the limitations of privacy regimes, as recent Canadian research demonstrates how privacy regulation generates limited control over the expansion of new crime prevention technologies. However, a more telling problem involves the enactment of new laws allowing police and venue operators to exclude the undesirable from venues, streets and entertainment zones. These developments reflect the broader shift to governing through sub-sovereign territorial controls that seek to leverage many current and emerging surveillance technologies and their normalisation in preventing crime without being encumbered by the niceties of privacy law.*

Keywords: *Alcohol, Antisocial Behaviour, Crime Prevention, Economy, ID Scanners, Night-time, Privacy.*

Authors

Darren Palmer is an Associate Professor in criminology at Deakin University, Geelong, Australia. He is a co-editor of *Crime and Justice: A Guide to Criminology* (2012) and *The Global Environment of Policing* (2012); co-author (with Ian Warren) of *Global Justice: Theories, Practices and Impediments* (2013), a forthcoming chapter (with Ian Warren) 'Re-territorialising Urban Governance in Australia' in R Lippert and K Walby eds. *Policing Cities: Urban Securitization and Regulation in a 21st Century World*, and currently preparing a manuscript on ID scanning in the Night Time Economy (with Ian Warren and Peter Miller).

Ian Warren is a Senior Lecturer in criminology at Deakin University, Geelong, Australia. He has written extensively on various important social issues relating to crime, drug law enforcement, surveillance and regulatory control. Most recently, he has been involved in a major research examining the use of ID scanning technologies to prevent violence and anti-social behaviour in Australian licensed venues.

1. Introduction

A quick glance at most privacy legislation indicates personal information provided for a business or commercial purpose must be provided to law enforcement authorities upon request. In the case of Australia, this information must be provided to these authorities for 'the prevention, detection, investigation, prosecution or punishment of criminal offences or breaches of a law' ([1], Schedule 1). This broad and ill-defined exemption indicates that the protection of personal information is secondary to the demands of criminal law enforcement, evidence gathering, the prevention of crime and the goal of community protection [2][3][4].

Privacy law potentially mediates the schism between surveillance, reactive criminal detection and crime prevention. However, the example of Australia indicates the reality of privacy law as a substantive mediating force against the growing tendency to use surveillance technologies in contemporary criminal justice is much less clear.

For two decades privacy scholars have outlined the social benefits of taking privacy more seriously [5][6]. All Australian state and federal jurisdictions have robust legal structures enabling Privacy Commissioners to work with private industry and oversee the development of codes of practice relating to the collection, storage and accurate maintenance of personal information for business purposes. Human rights instruments also contain specific references to privacy that are enforceable against state Parliaments, courts, tribunals and relevant statutory authorities. For example, as long as there are no competing national laws that enable government intrusions into the private domain, Victorian law confers two main rights to privacy on all individuals that are enforceable against public authorities operating within that state:

a) [The right] not to have his or her privacy, family, home or correspondence unlawfully or arbitrarily interfered with; and
b) [The right] not to have his or her reputation unlawfully attacked ([7], section 13).

These principles focus mainly on intrusions into the private home, with the emphasis on personal reputation being more akin to the power of defamation law to prevent unnecessary snooping and gossip about personal activity. However, any untoward intrusions that occur beyond the private or personal realm remain beyond these legal protections. Nevertheless, the ability to access goods and services, or the adoption of new technological strategies in public and semi-public spaces remains a growing facet of contemporary life [8], with the nexus between safety, security and information privacy extending well beyond those rights protected by most current Australian laws.

Australian state and federal privacy legislation allows concerned citizens to question the measures adopted by private businesses to solicit or maintain personal information for the provision of goods or services [1][9]. Regardless of how frequently these measures are activated by concerned citizens, any personal legal rights to privacy or any codes of practice developed between private industry and designated Privacy Commissioners do little to erode the function creep of new technologies in the delivery of commercial or governmental services.

Growing demands for providing quicker and more efficient ways of delivering services to ordinary citizens [10][11] also extend to the law enforcement field, where police agencies increasingly rely on new technologies to enhance their investigative, crime prevention or mass surveillance capacities. For example, road traffic control is one area of law enforcement that has become so dependent on new surveillance technologies that the administration of fines and other punishments for problematic driving is almost fully automated. This form of simulated justice [12] comes at considerable cost, particularly when police managers or operational personnel fail to adapt conventional modes of enforcement to ensure new technologies are deployed according to accepted due process requirements [13].

> "The example of Australia indicates the reality of privacy law as a substantive mediating force against the growing tendency to use surveillance technologies in contemporary criminal justice is much less clear"

A recent Ombudsman's report examining the implementation of new data management systems in several Victorian government departments is particularly critical of the lack of coordinated leadership behind the deployment of many technological initiatives in contemporary public administration [14].

A crucial example involves the protracted efforts to upgrade the Victoria Police crime database. The report identified considerable financial waste stemmed from the absence of clear managerial oversight of the implementation of this important upgrade. More importantly, this lack of a strategic long-term vision meant that any new data management and dissemination strategies were adopted without adequate consideration of the future objectives of the organisation. The report concluded that the Victoria Police was clearly unwilling to adapt its 'business processes to fit the new system', because it was preoccupied with making 'the system fit Victoria Police's [existing] processes' ([14], p. 66). The end result was the ultimate abandonment of the database upgrade after five years of preliminary work and the expenditure of tens of millions of dollars. The cause of this wastage was simple: Victoria Police had not 'defined and set a clear vision for modern policing out to 2030', established clear business requirements, adequately planned for organisational transformation from a paper-based organisation to an electronic organisation or established clear ownership and accountability for organisational transformation ([14], p. 66).

The sense of mistrust associated with these large-scale publicly funded databases filters into the routine uses of new technologies to supplement conventional operational policing activities. Here, extensive reforms to the criminal law introduce lower legal thresholds to combat minor forms of crime or antisocial behaviour [15], which fuel more intrusive forms of mass surveillance in both public and semi-public spaces. These developments can have several negative social impacts [16][17]. While much has been written about the contemporary 'reflex application of the criminal law … to deal with complex social problems' ([18], p. ix), the use of technology by police or private agencies, such as open space CCTV systems or mobile phone tracking devices in large privately owned shopping malls, increases the scale of dataveillance in contemporary life. This in turn helps to normalise the use of questionable information technology and data mining practices for fairly routine low-level law enforcement activities.

The power of existing privacy laws to contain both the nature of such information gathering and the desirable uses of personal data is limited in two ways.

First, there is little scope for privacy law to allow citizens to collectively challenge the growing function creep of new surveillance technologies employed by police, other government departments or private businesses. As with many other areas of law, the right to correct an actual or suspected privacy breach can only be determined after an aggrieved person has detected a suspected violation by providing sufficient evidence of harm to convince a court or other official body that legal intervention is required. This 'back-end' process is partially tempered by Australian Privacy and Information Commission structures, which enable the development and implementation of codes of practice to prevent breaches of agreed standards by private businesses or local governments. These processes are yet to be researched in depth in Australia. However, emerging research into similar oversight methods in Canada indicates that extremely diverse standards of information management are developed for the administration of open space CCTV networks, which undermines consistency in the application of privacy law. Moreover, Commissioners routinely prioritise public safety over individual or collective privacy interests when developing methods of overseeing the operation of these systems and related data access, storage and maintenance protocols [19].

Second, these processes are fuelled by the express exemption under Australian privacy law regarding crime. This crucial term has yet to be scrutinised in detail by Australian courts. The complex relationship between crime prevention [20], technology and privacy adds weight to Hier and Walby's [19] concerns regarding the value of current privacy laws in protecting the community from the expanded uses of intrusive surveillance technologies or the data they generate. As Solove [21] indicates, the emotive nature of crime and security debates establishes an uneven playing field where the privacy interests of few are considered to unnecessarily compromise the safety of the majority. Solove's concern is that the failure to equate privacy with greater security means that in any debate between these two important social concerns, security and community protection will always win. This means privacy rights run the risk of dissolving as more surveillance technologies permeate the contemporary crime prevention landscape, even if, as the Victorian example indicates, both the high- and low-end uses of these forms of dataveillance are not necessarily matched by shifts in the prevailing enforcement philosophies that inform their deployment.

One area where these debates are prominent is within the management of the contemporary night-time economy. In recent decades law enforcement agencies, often working alongside community groups and venue proprietors, have faced growing pressure to strategically identify and prevent the risks of collective violence, antisocial behaviour and disorder in and around licensed venues [22]. This push has generated extensive reforms to enable increased surveillance of those participating in the night-time economy, along with a greater range of fines and other punishments for more trivial forms of unruly behaviour. The following discussion builds on our extensive research into the use of computerized ID scanning in the Australian night-time economy by challenging the common assumption that new surveillance technologies automatically make the night-time economy safer or easier to manage. More importantly, information privacy law appears largely incapable of preventing the normalization of this form of surveillance. This trend is especially problematic when viewed in conjunction with the introduction of zonal banning laws aimed at removing disorderly people from individual venues, nightclub precincts or designated zones incorporating the central business districts (CBDs) of Australia's urban and regional cities.

2. ID Scanning, Function Creep and Privacy in Australia

Mandatory patron ID scanning has become an increasingly popular method of attempting to minimise the prospect that disorderly or violent people will enter nightclubs or entire entertainment precincts in many Australian cities. This technology enables proprietors to take a digital image of a patron's identification document and a photograph or biometric identifier, such as a fingerprint, prior to allowing entry into a venue licensed to sell alcohol. The person's identity can then be instantly matched with manual records entered into the database that alert door staff about patrons who have been banned from

> "The person's identity can then be instantly matched with manual records entered into the database that alert door staff about patrons who have been banned from the venue"

the venue. As a recent Victorian report on *Surveillance in Public Places* indicates, one major casino in Melbourne has deployed: "*… [i]dentification scanners [to] record the image and written details on an individual's driving license or other identity card, including their name and address. Facial recognition software scans patrons' faces as they enter the nightclub and matches those images against a database of photos. In this way the software can be used to identify patrons who have been previously banned from a venue. The software can be shared among venues*" ([23], p. 40).

Unlike some United States jurisdictions [27] where ID scanners have been specifically endorsed in state liquor licensing laws, many systems in Australia have been adopted at a piecemeal level at the discretion of individual venue operators. However, at least two regions in Australia have seen a more formal approach to the use of ID scanners alongside several additional measures aimed at combating alcohol-related harm.

In March 2010 the Queensland Parliament Law, Justice and Safety Committee released an extensive report outlining 'best practice' in the management of alcohol supply within that state. The report emerged from concerns that Australia's historical 'knock 'em down' attitude towards alcohol consumption and mateship, had given way to: "*… a growing culture of [binge] drinking to harmful levels, without any pride or self-respect. Vomiting, falling over, and creating a nuisance in public are not seen as shameful but to some are badges of honour. A lack of self-respect and respect for others seems entrenched*" ([24b, p. i).

A series of public hearings, venue site visits by Committee members and written submissions by various 'stakeholders', including liquor industry representatives, legal services, youth advocacy groups and education providers, generated an extensive report examining the causes of alcohol-related violence and offered several proposals to improve venue amenity, transport, responsible service of alcohol guidelines and the use of surveillance technologies to manage behaviour in the night-time economy. A total of sixty-eight recommendations were proposed, ranging from formal amendments to criminal and summary offence laws, to the more stringent implementation of national public health programs targeting young people in schools and other community settings.

The final report recognised that ID scanning had been adopted by a number of venues throughout Queensland and in several cases was successfully '*used in conjunction with CCTV images to identify offenders*' ([24b], p. 24). In some 'high risk areas' where more than one premises had deployed this technology, system networking allowed a quick and easy method of determining that a patron banned from one premises should not be allowed entry into another. Various organisations, including the Queensland Police Union of Employees and the Liquor Hospitality and Miscellaneous Union, supported this technology due to its potential to deter troublemakers and enable police to efficiently identify those engaging in violent or antisocial behavior.

The following submission from the Chief Executive of the Queensland Hotels' Association aptly captures the positive view of this technology: "*We have introduced ID scanning where the appropriate form of ID is scanned at the point of entry, and that acts as a clear deterrent to patrons who might otherwise be intending to get up to no good. People know that, if their identity is held in a safe computer and if they create harm or create violence or break the law, those people who are authorised to access the hard drive, being the Police Service, will be able to track them down*" [24b, p. 25).

However, a lengthy submission from the Queensland Information Commissioner raised several concerns over the desirability of extending the use of ID scanners pending the development of agreed information management standards, or more detailed discussion of their legal implications under current Queensland and national privacy legislation. Two main concerns informed this submission. The first involved reservations about the causal link between alcohol and violence in the public imagination. This had the potential to place undue reliance on ID scanning as a quick and effective 'technological fix' [25] to the problem of drinking culture, at the expense of other less intrusive harm minimization strategies. The second relates to the use of dataveillance to achieve substantive improvements in social order. Not only is the deterrent effect of ID scanning difficult to establish, but real concerns also surround the monitoring of *all* venue patrons through such technology. This means that 'the collection of personal information by licensed premises' is more likely to involve questionable forms of dataveillance, with ID scanners becoming '*the all seeing eye for law enforcement by police*' ([24b], p. 25).

While Queensland has not been plagued by the same difficulties surrounding the adoption of new law enforcement technologies that were identified by the Victorian Ombudsman [14], the relatively unquestioned acceptance of ID scanning technologies, either with or without an appropriate trial or adequate consideration of their privacy implications, presents numerous problems. Importantly, many other situational and supply-based policy interventions can have a meaningful impact in altering negative drinking cultures. Nevertheless, despite these concerns the final report recommended licensees trading after midnight should be encouraged to install ID scanning systems with 'due regard to privacy issues and matters of natural justice' ([24b], p. 27).

Neither the report nor the government's formal response clarifies the specific implications of the terms 'due regard' or 'natural justice'. It was suggested venues should receive discounted licensing fees for installing ID scanners, but this proposal was ultimately abandoned with the Queensland government introducing a 'new more secure, more durable and more reliable driver license card' in 2010 ([26], p. 5). More problematically, this example illustrates how Australian governments appear willing to override key issues relating to information privacy given the seemingly more pressing demands of combating alcohol-related disorder through expanded and untested surveillance measures. Interestingly, the Committee's interim report recognised both 'the safety of patrons and the protection of their identity documents are paramount' and strongly cautioned against the widespread use of networked ID scanning until these issues were adequately addressed ([24a], p. 8).

The mandatory adoption of ID scanning in the 'high risk' venues trading after 1.00 am in the Victorian city of Geelong followed a slightly different trajectory. In response to several widely publicised violent crimes in the city's nightclub precinct during late 2006, police, venue proprietors, the local council and concerned citizens used a voluntary Liquor Accord to reform the night-time economy within the 2.5 square kilometre CBD. This region contains up to ten licensed hotels that are popular amongst the local population, large numbers of university students and holidaymakers venturing to Victoria's coastal resorts during the summer months [28]. Key

> "Neither the report nor the government's formal response clarifies the specific implications of the terms 'due regard' or 'natural justice'"

stakeholders involved in the Geelong Liquor Accord agreed to pilot ID scanners at ten venues between May and November 2007. However, neither the initial pilot, nor the formalisation of this technology as a mandatory condition of entry into all high-risk venues under the revised Accord that was released in November 2007 met with any substantial public debate [28].

As with the earlier introduction of CCTV, there was no attempt to develop legal regulation and deliberation processes for determining authorization and appropriateness of the use of ID scanners (for a contrasting example see [29] on the legal regulation of CCTV in Spain).

The most significant event occurred after November 2007 and involved reforms to Victoria's liquor licensing laws that introduced an expanded banning order procedure originally applying to ten designated areas across the state including the Geelong CBD. Section 148B of Victorian *Liquor Control Reform Act* [40] now enables police to implement a zonal ban preventing a person from entering a designated area for behaviour considered to 'give rise to a risk of alcohol-related violence or disorder'. The bans apply to relatively minor public drunkenness or obscene language offences, or more serious assaults, sexual assaults and unlawful weapons offences occurring within the zone ([40], Schedule 2).

All of these behaviours were already prohibited under existing state criminal laws. When coupled with a short-term ban, a person is subject to a $500 fine and must immediately leave the designated area for up to 72 hours unless they live or work within the zone. Failure to comply with the ban carries additional fines and the prospect of an extended banning order, which can also be imposed as a punishment for any serious offences committed 'wholly or partly in a designated area' attracting a maximum imprisonment term of less than 12 months. In these cases, police, the Office of Public Prosecutions or a court must be satisfied the extended order '*may be an effective and reasonable means of preventing the commission … of further specified offences in the designated area*' ([40], s. 148I(1)(c)).

Available data indicates that in the first six-months of operation, the Victoria Police used these banning powers sparingly. From December 2007 to 30 June 2008, 129 bans were issued to 128 'unique persons', with one person being banned on two occasions. All bans were implemented in Melbourne CBD and surrounding declared areas, where there are far greater concentrations of nightclubs than the less populated Geelong zone. Only six per cent of people receiving bans in this initial period were women, while 66 per cent were in the 20-29 year age category. A further 22 per cent were under 20 years of age, while 9 per cent were between 30 and 39 years of age ([30], p. 9).

Periodic government media releases on official websites or in Victorian newspapers reveal that between December 2007 and January 2010, police issued 2,492 short-term banning notices. Around 95 per cent of bans were directed at men, with 2,144 orders issued in the Melbourne CBD ([30], p. 9) [31].

After a change of government in December 2010, this banning regime was expanded to cover several additional public order offences, while increased fines now accompany on-the-spot bans and subsequent breaches of short- or longer-term banning orders. In addition, the banning powers now apply to three new designated areas [32] and further provisions enable police and all venue managers and their security staff in Victoria to impose a graded series of bans ranging from one to six months for various alcohol-related offences occurring in or near individual venues. These 'barring orders' attract fines of up to $2000 if a banned person is detected within 20 meters of the venue where the order applies ([40], s. 106).

The methods for enforcing either short-terms bans issued by police, venue operators and security personnel, and the extended bans imposed by a magistrate's court, are not stated within the relevant legislation. While available data indicates only sixteen bans have been imposed in Geelong between December 2007 and December 2009 ([30], p. 9), the relatively systematic introduction of ID scanners amongst the high-risk venues in this city provides an enforcement template for other designated areas to follow. Enhanced information networking between venues also now makes the task of enforcing bans and increased fines for these low-level liquor violations in the Geelong designated area potentially much easier.

However, questions regarding data security and information privacy remain squarely outside the official discourses that support these new surveillance measures. Of particular concern is the lack of agreed protocols that enable patrons to enter a venue in the Geelong CBD without having their identity scanned. The common practice is to insist that ID scanning is a mandatory requirement before entry is permitted. If patrons decline this requirement, they are routinely told '*… its for security … (w)e just say it's the law*' ([33], p. 22).

The philosophy underpinning this approach is simple. Venue managers believe ID scanners are a valuable method of promoting venue safety by allowing security personnel to 'quickly identify [troublesome patrons] and ban them' ([33], p. 22). Any countervailing concerns over information privacy, data security or police access to scanned information are secondary to the overriding belief that ID scanners can efficiently identify patrons banned from venues deploying this technology, or that they are a valuable deterrent against troublesome or underage patrons attempting to enter any licensed premises within the Geelong CBD.

3. Conclusion

Like many other forms of dataveillance, ID scanners contribute to new forms of 'particularized' citizenship that can compromise universal or rights-based access to government and private services ([10], p. 731). While such measures can enhance community safety, they can also exacerbate social 'segmentation' when supplemented by 'multiple hybrid, civil, contractual, and administrative' legal requirements aimed at regulating a growing number of 'irregular citizens' or 'antisocial youth' ([17], p. 389; 394-397).

There are numerous unknown questions surrounding how police manage and use the data obtained from participating nightclubs in the Geelong CBD to help enforce Victoria's banning regime. Data security, the manual entry of a banned designation and protocols over information sharing, all of which are subject to many legally enshrined privacy controls, remain to be clarified given the overriding importance of promoting safer night-time economies through more intrusive forms of computerised surveillance.

The Queensland report also advocated replicating the Victorian legislative model by introducing the '*power for police to ban trouble patrons from entertainment precincts for 24 hours' and allowing 'courts to issue a banning order where there is persistent alcohol-related*

> "While individuals might be able to bring a legal challenge under the Victorian *Charter of Human Rights and Responsibilities Act*, these provisions relate to personal breaches rather than the processes that lead to the adoption of new surveillance technologies"

offences committed by a person, or where a person commits a serious offence in or around licensed venues' ([24b], p. 23).

This effectively means individuals are increasingly subject to surveillance through their 'digital footprints' and personal 'trust profile(s)' ([10], p. 730), which police and venue operators monopolise through 'exclusive [digital] knowledge' sharing about troublesome persons and their activities ([34], p. 59). Both the Queensland and Geelong examples indicate local and state governments are more than willing to concede that privacy protection is an outlying concern that can be dealt with after these processes are introduced.

Moreover, the firms that manage the installation and maintenance of this technology are able to '*share a banned list of troublemakers – whether that listing is local, statewide or national*' [35]. This raises additional concerns that such forms of computerised surveillance know few geographic boundaries.

The urgency of promoting increased safety in the night-time economy means the impact of problematic 'back end' assemblages involving scanned personal data is only challengeable through administrative, rather than criminal law. Privacy and natural justice processes involve establishing whether the use of these technologies conforms to agreed minimum standards, rather than a detailed assessment of the impact of this 'surveillance creep' ([36], p. 181) on individual or collective citizen rights.

While individuals might be able to bring a legal challenge under the Victorian *Charter of Human Rights and Responsibilities Act*, these provisions relate to personal breaches rather than the processes that lead to the adoption of new surveillance technologies. Privacy law can enable citizens to review and correct personal information stored in any venue database if there has been an error in recording a ban applying to a particular venue or designated zone. Broader constitutional arguments regarding freedom of movement have yet to be raised under current Victorian human rights law, but remain an obvious site for further investigation given the potential social impacts of these zonal prohibitions [37].

Most problematically, these forms of surveillance are inadvertently validated under conflicting legal regimes that 'erode privacy rights, create new forms of inequality, and lack mechanisms of accountability' ([38], p. 6). This is particularly concerning given that any determination of whether a person should be banned from a particular venue or designated zone involves highly discretionary judgments by police, venue operators and private security personnel.

Through an emphasis on increased security, crime prevention and greater community protection, these novel and untested forms of computerised surveillance do compile more detailed and potentially accurate information on people and their activities both within and across Australian state borders. However, when combined with expanded legal powers, such as the Victorian banning provisions, these new forms of simulated surveillance [39] and justice [12] question the value of information privacy law in establishing appropriate information collection and data management strategies before these technologies become normal facets of social life.

The political tendency to introduce and endorse these technologies without adequate public debate is arguably fuelled by the current legal exemption of crime under contemporary Australian privacy law. By conferring few rights to enable citizens to directly challenge the adoption of these security technologies, privacy law inadvertently vests enormous trust in police and other commercial service providers to appropriately manage their deployment. As the recent inquiry in Victoria illustrates, there is serious doubt over whether such trust is deserved.

References

[1] *Information Privacy Act*, Victoria, 2000.

[2] W. Schinkel. Prepression: The actuarial archive and new technologies of security. *Theoretical Criminology*, 15(4): 365-380, 2011.

[3] C. Osmond. Anti-social Behavour and its Surveillant Inter-assemblage. *Surveillance and Society*, 7(3-4): 325-343, 2010.

[4] S. Thompson, G. Genosko. *Punched drunk: Alcohol, surveillance and the LCBO, 1927-1975*, Blackpoint, Nova Scotia: Fernwood Publishing, 2009.

[5] D. Lindsay. An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law. *Melbourne University Law Review*, 29(1): 179-217, 2005.

[6] G. Greenleaf, N. Waters, L.A. Bygrave. Implementing privacy principles: After 20 years its time to enforce the Privacy Act. *University of New South Wales Law Research Series*. <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=987763> [Accessed on 2 November 2010].

[7] *Charter of Human Rights and Responsibilities Act*, Victoria, 2006.

[8] J.B. Rule. *Privacy in Peril: How We are Sacrificing a Fundamental Right in Exchange for Security and Convenience*. New York, NY: Oxford University Press, 2007.

[9] *Privacy Act*, Commonwealth, 1988.

[10] A. Lips, B. Miriam J.A. Taylor, J. Organ. Identity management, administrative sorting and citizenship in new modes of government. *Information, Communication & Society*, 12(5): 715-734, 2009.

[11] G. Greenleaf. Access all areas: Function creep guaranteed in Australia's ID card bill (no. 1). *Computer Law & Security Report*, 23(4): 332-341, 2007.

[12] P. O'Malley. Simulated Justice: Risk, Money and Telemetric Policing. *British Journal of Criminology*, 50(5): 795-807, 2010.

[13] P.K. Manning. A View of Surveillance. En *Technocrime: Technology, Crime and Social Control*, S. Leman-Langlois (ed.). Cullompton UK: Willan Publishing, 2008.

[14] Victorian Ombudsman. *Own Motion Investigation into ICT-Enabled Projects*. Melbourne, Vic: Victorian Government Printer, 2011. http://www.ombudsman.vic.gov.au/resources/documents/Investigation_into_ICT_enabled_projects_Nov_2011.pdf [Accessed on 9 March 2012].

[15] R. Matthews. Beyond 'so what?' criminology: Rediscovering realism. *Theoretical Criminology*, 13(3): 341-362, 2009.

[16] A. von Hirsch, A.P. Simister (eds). *Incivilities: Regulating offensive behavior*. Oxford, UK: Hart Publishing, 2006.

[17] L. Zedner. Security, the state, and the citizen: The changing architecture of crime control. *New Criminal Law Journal*, 13(2): 379-403, 2010.

[18] N. Des Rossiers, S. Bittle. Introduction. En *What is Crime? Defining Criminal Conduct in Contemporary Society*, Law Commission of Canada (ed.), Vancouver: UBC Press, 2004.

[19] S.P. Hier, K. Walby. Privacy Pragmatism and Streetscape Video Surveillance in Canada. *International Sociology*, 26(6): 844-861, 2011.

[20] A. Sutton, A. Cherney, R. White. *Crime Prevention: Principles, Perspectives and Practices*. Melbourne, Vic: Oxford University Press, 2008.

[21] D.J. Solove. *Nothing to Hide: The False Tradeoff Between Privacy and Security*. New Haven, CT: Yale University Press, 2011.

[22] P. Hadfield, S. Lister, P. Traynor. This town's a different town today: Policing and regulating the night-time economy. *Criminology and Criminal Justice*, 9(4): 465-485, 2009.

[23] Victorian Law Reform Commission (VLRC). *Surveillance in public places final report*, no. 18. Melbourne, 2010. http://www.lawreform.vic.gov.au/sites/default/files/Surveillance_final_report.pdf

[24a] Law, Justice and Safety Committee. *Inquiry into alcohol-related violence, Interim report,* no. 73, Brisbane, Qld: Government of Queensland, 2009.
[24b] Law, Justice and Safety Committee. *Inquiry into alcohol-related violence,* no. 74, Brisbane, Qld: Government of Queensland, 2010. <http://www.aic.gov.au/crime_types/violence/alcohol%20and%20drug%20related%20violence.aspx> [Accessed on 3 June 2010].
[25] B. Bloomfield. In the Right Place at the Right Time: Electronic Tagging and Problems of Social Order/Disorder. *The Sociological Review*, 49(2): 174-201, 2001.
[26] Queensland Government. *Queensland Government Response to Law, Justice and Safety Committee's Report into alcohol-related violence*. Brisbane, Qld. Government of Queensland, 2010. <http://www.parliament.qld.gov.au/documents/committees/LJSC/2009/alcohol-related-violence/responseReport74.pdf> [Accessed on 12 March 2012].
[27] J.T. Cross. Age Verification in the 21st Century. Swiping Away your Privacy. *The John Marshall Journal of Computer and Information Law*, 23(2): 363-410, 2005.
[28] D. Palmer, I. Warren, P. Miller. ID scanning, the media, and the politics of urban surveillance in an Australian regional city. *Surveillance and Society*, 9(3): 293-309, 2012.<http://library.queensu.ca/ojs/index.php/surveillance-and-society/article/view/aussie_regional>. [Accessed on 30 March 2012].
[29] G.G. Clavell, L.Z. Lojo, A. Romero. CCTV in Spain: An empirical account of the deployment of video-surveillance in a Southern-European Country. *Information Polity*, 17: 57-68, 2012.
[30] M. Tesoriero. Securing our Streets. *Police Life: The Victoria Police Magazine (The Public Safety Edition)*, Melbourne, Vic: Victoria Police Media and Corporate Communications Department, 2010. <www.police.vic.gov.au/retrievemedia.asp?Media_ID=56600>, pp. 8-9. [Accessed on 12 March 2012].
[31] J. Dowling. Police issue record number of banning notices. *The Age*, 26 enero de 2010, <http://www.theage.com.au/national/police-issue-record-number-of-banning-notices-20100125-muhi.html>.
[32] M. O'Brien. Tough new laws to tackle drunken louts. State government of Victoria Media release, 1 March 2011. <http://www.premier.vic.gov.au/wp-content/uploads/2011/03/110301-OBrien-Tough-new-laws-to-punish-drunken-louts-PDF-41KB.pdf>. [Accessed on 12 March 2012].
[33] D. Palmer, I. Warren, P. Miller. ID Scanners in the Australian Night-Time Economy. *IEEE Technology and Society Magazine*, 30(3): 18-24, 2011.
[34] D. O'Connor, W. De Lint. Frontier government: The folding of the Canada-US border. *Studies in Social Justice*, 3(1): 39-66, 2009.
[35] N. O'Brien, E. Duff. You want a drink? Give us your fingerprints. *Sydney Morning Herald*, 30 Jan. 2011. http://m.smh.com.au/entertainment/restaurants-and-bars/you-want-a-drink-give-us-your-fingerprints-20110129-1a8x3.html. [Accessed on 9 March 2012].
[36] D. Murakami Wood. The Surveillance Society: Questions of History, Place and Culture. *European Journal of Criminology*, 6(2): 179-194, 2009.
[37] K. Beckett, S. Herbert. *Banished: The New Social Control in Urban America.* New York, NY: Oxford University Press, 2010.
[38] K.D. Haggerty, R.V. Ericson. The New Politics of Surveillance and Visibility. En *The New Politics of Surveillance and Visibility*, Kevin D. Haggerty and Richard V. Ericson (eds), Toronto: University of Toronto Press, 2006.
[39] W. Bogard. Welcome to the Society of Control: The Simulation of Surveillance Revisited. En *The New Politics of Surveillance and Visibility*, Kevin D. Haggerty and Richard V. Ericson (eds), Toronto: University of Toronto Press, 2006.
[40] Liquor Control Reform Act. Victoria, 1998.