Office of the Information Commissioner
Queensland

152

SUBMISSION TO LAW, JUSTICE AND SAFETY COMMITTEE

Inquiry into alcohol-related violence in Queensland
(December 2009)

CONTENTS

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 12 Universal Declaration of Human Rights[1]

BACKGROUND

The Queensland Office of the Information Commissioner (**OIC**) is an independent statutory authority accountable to the Queensland Parliamentary Law, Justice and Safety Committee. Under the *Information Privacy Act 2009* (Qld) (**IP Act**) OIC has performance monitoring and support functions. These statutory functions include

> *leading the improvement of public sector privacy administration in Queensland by taking appropriate action to*
>
> *(i)promote understanding of and compliance with the privacy principles; and*
>
> *(ii)provide best practice leadership and advice, including by providing advice and assistance to relevant entities on the interpretation and administration of [the Information Privacy Act].*

In Interim Report Number 73 concerning its Inquiry Into Alcohol Related Violence, the Law, Justice and Safety Committee commented on networked ID Scanning Devices at 6.5.stating

> ***6.5 Networked ID Scanning Devices***
>
> *Further inquiries will be made into the possibility of the introduction of a system of ID scanners which could be networked to allow venues within a precinct to share information, including scans of patrons' ID and CCTV images. This would aid venues to effect bans where patrons have caused a disturbance or are unduly intoxicated.*
>
> *Some positive anecdotal evidence has been provided from venue owners and managers and police that this technology has had an impact in reducing the level of alcohol-related violence in licensed venues. This has been attributed to the fact that patrons know that their identification details have been collected by the venue and will be provided to police if an offence is committed.*
>
> *An important issue raised with a system of networked ID scanners relates to privacy, in particular the collection and storage of this sensitive information. The committee recognises that the safety of patrons and the protection of their identity documents are paramount. These issues need to be closely considered before any recommendation can be made on this matter.*

While OIC's jurisdiction does not extend to the private sector, including most licensed premises, the IP Act does apply to Queensland government agencies affected by alcohol related violence and accordingly, this submission aims to assist the Committee in its considerations by providing advice on the privacy implications for the Queensland community arising from the use of Identification Scanning (**ID Scanning**) and Closed Circuit Television (**CCTV**) by licensed premises.

This submission does not represent the views or opinions of the Queensland Government.

[1] UN GAOR (1948).

KEY POINTS RAISED IN THE SUBMISSION

- The use of ID Scanning and CCTV by licensed premises with a turnover of over $3 million may breach Commonwealth privacy principles. This is a matter for the federal Privacy Commissioner.
- The use of ID Scanning and CCTV by licensed premises with a turnover of less than $3 million amounts to arbitrary interference with a person's privacy and people are entitled to protection of the law from it. Such protection does not presently exist.
- The advice of the Office of the Information Commissioner is that fundamental human rights, including privacy rights should not be eroded by the use of CCTV and ID scanning in selected licensed premises when:
    - only some licensed premises are currently regulated by the *Privacy Act 1988 (Cth)*
    - alcohol is not the cause of violence
    - some licensed premises are known to be more violent than others and at particular times
    - alcohol related violence occurs in many other public and private places apart from licensed venues and ID scanning and CCTV would not be a proportionate policy response to the general problem
    - the privacy rights of a large proportion of the population are interfered with because of the behaviour of a few evidence based best practice harm minimisation is not in place
    - all available strategies (that do not breach fundamental human rights) to reduce violence in and around licensed premises are yet to be implemented in Queensland
    - the deterrence effect of ID scanning and CCTV has not been established while it is clear that the predominant purpose for the collection of personal information by licensed premises is for their own 'law enforcement' purposes and as the all seeing eye for law enforcement by police
    - erroneous community beliefs about alcohol contribute to the problem
    - current planning, liquor licensing and price regulation/taxation laws contribute to the problem
    - work remains to be done in assisting licensed premises resolve the fundamental conflict between their financial interests and the responsible service of alcohol,
    - the drinking culture remains largely untouched and largely supported by planning and liquor licensing approaches
    - there are other more targeted techologies around that may not be as intrusive of human rights, such blood alcohol testing being made available in licensed premises so patrons can choose to reliably measure their blood alcohol content and the new DNA-style spray that leaves a colourless unique mark on targets that remains visible for 6 weeks under a UV light.

THE COMMONWEALTH PRIVACY JURISDICTION

The Commonwealth *Privacy Act 1988* applies to the private sector excluding businesses with a turnover of less than $3 million. If a licensed premise has an annual turnover of more than $3 million, it may fall within the coverage of the Commonwealth *Privacy Act 1988*. Patrons who transact with licensed premises that have an annual turnover of less than $3 million have no privacy protections whatsoever. These premises are able to collect, manage, use and disclose the most sensitive and intimate of their patron's personal information for any purpose the premise considers appropriate.

For those licensed premises with a turnover of more than $3 million, application of the privacy principles is mandatory with recourse to seeking a waiver of the privacy principles from the Commonwealth Privacy Commissioner where necessary.

The 'small business exemption' was initially brought in because the compliance costs for small business were considered prohibitive. Some businesses dealing in personal information (residential tenancy database operator, for example) or with sensitive information - health providers - do not fall within the small business exemption. It is optional for a small business to opt in to coverage. Currently 184 businesses have chosen to opt in.

The small business exemption has a potentially large coverage. It is estimated that 94% of Australian businesses fall under this exemption - in 2007 there were 1,890,213 businesses with an annual turnover of less than $2 million. It would be relevant to the Committee's considerations to ascertain from the relevant Queensland government authority the percentage of licensed premises which have a turnover of less than $3 million.

Huge advances in e-commerce have been made in the last 20 years (since the Commonwealth *Privacy Act 1988* was first enacted). Any small business can now compile, on the simplest of laptops, a vast store of their customer's personal information. On average 20% of all privacy complaints falling outside of the jurisdiction of the *Privacy Act 1988* concern the small business exemption. On a 'positive side' the threshold figure - $3 million - has over this period been lowered in real terms.

The small business exemption is mainly confined to Australia - the UK, Canada and NZ do not have this exemption. There have now been five inquiries (including the latest ALRC one) looking at the small business exemption. Each one to date has resulted in the position of not 'overburdening/over-regulating small business'. This position is supported by the Commonwealth Privacy Commissioner.

The ALRC could not be less equivocal on its position on the small business exemption, stating "...the exemption for small business is neither necessary nor justifiable." The ALRC's recommendation 39-1 recommended the total removal of the small business exemption in the Privacy Act.

The recent Australian Government's response to the ALRC's report is two-fold. On 14 October 2009 the government released a 'first-stage response' addressing 197 of the report's 295 recommendations. Recommendation 39-1 is one of the unaddressed recommendations. At present there is no indication when the 'stage two response' will be released.

Other relevant 'stage two recommendations' include:

- proposals to clarify or remove certain exemptions from the *Privacy Act 1988* - including the small business exemption and employee records
- introducing a statutory cause of action for serious invasion of privacy
- serious data breach notifications
- handling of personal information under the *Telecommunications Act 1997*.]

With respect to the privacy principles, the *Information Privacy Act 2009* (Qld) and the *Privacy Act* 1988 (Cth) contain substantially similar privacy principles. For the Committee's information, the federal Privacy Commissioner has recently launched an investigation into a proposal by Brisbane nightclubs to use digital fingerprint scanners in order to compile a 'ban-list' of patrons considered by the premises as being 'anti-social'.[2] The federal Privacy Commissioner noted[3]:

> *A potential issue is that, once information is digitized, it makes it much easier for that information to be used for other purposes that you may not have consented to.*

RECENT HIGH COURT CASES ON LIABILITY

The following summaries of recent High Court cases are highlighted for the Committee's attention. While they primarily concern the licensee's liability for individual patron behaviour, the judges make relevant comment on liability for injury to third parties and community values. The factual situations also provide a potent reminder that there are severe restrictions on the ability of strategies such as networked ID scanning and CCTV to prevent 'anti social', 'violent' behaviour and reduce the general impact of intoxification on third parties, the community and public services.

Cole v South Tweed Heads Rugby League Football Club Limited [2004] HCA 29

On 26 June 1994 Ms Cole was injured when she stepped out into the path of a car after spending most of the day drinking at the respondent Club. At some point in the afternoon, the Club had stopped serving alcohol to Ms Cole but she apparently continued to drink alcohol purchased and supplied to her by friends. In the late afternoon, Ms Cole had, in no uncertain terms refused the Club's offer of a courtesy bus home or to call her a taxi. Ms Cole left in the company of two 'sober' friends but was hit by the car 50 minutes after leaving the club. Ms Cole was in a state commonly described as 'legless' and, on appeal, no liability was held by the car driver who was not in a position to avoid Ms Cole. The sole issue before the High Court was Ms Cole's claim that the Club was responsible for her inability and therefore liable for her injuries. Ms Cole's blood alcohol level was 0.24 (just under 5 times the legal limit). In a 4-2 judgment the High Court did not agree.
Gleeson CJ stated:

> *Again, as a general rule a person has no legal duty to rescue another. How is this to be reconciled with a proposition that the respondent had a duty to protect the appellant from the consequences of her decision to drink excessively? There are many forms of excessive eating and drinking that involve health risks but, as a rule, we leave it to individuals to decide for themselves how much they eat and drink. There are sound reasons for that, associated with values of autonomy and privacy;*

---

[2] *'Nightclubs fingered by privacy watchdog'*, report by Julian Bajkowski of the Australian Financial Review dated 7 December 2009.
[3] Ibid.

and

> *The consequences of the appellant's argument as to duty of care involve both an unacceptable burden upon ordinary social and commercial behaviour, and an unacceptable shifting of responsibility for individual choice.*

In a dissenting judgment McHugh J (with whom Kirby J agreed) stated:

> *Upon these facts, the inference is irresistible that, by early afternoon, liquor supplied by the Club had reduced Mrs Cole to such a physical and mental state that there was a real risk that she would suffer harm of some kind. The inference is also irresistible that the more she drank the more opportunities there were that she would suffer harm and the greater the likelihood that the harm would be serious. If the Club ought to have foreseen that her consumption of alcohol had reached a point that further alcohol might expose her to an alcohol-induced risk of injury, it does not matter whether she purchased the further alcohol she drank or whether her companions purchased the alcohol that she drank. The Club owed her a personal duty not to expose her to the risk of injury and, by directly supplying her, or by permitting her companions to supply her, with further alcohol, the Club breached the personal duty of care that it owed to her.*

Kirby J commented on his (majority) colleagues' opinions - *The withered view of community and legal neighbourhood propounded by Gleeson CJ and Callinan J is one that I would reject.*

CAL No 14 Pty Ltd v Scott [2009] HCA 47

On 24 January 2002 Mr Shane Scott was drinking at the Tandara Motor Inn, Triabunna, Tasmania. Mr Scott, concerned about the possibility of police breathalyser units, arranged to have his motorcycle placed in the Motor Inn's secure lockup and left the keys with the licensee on the understanding that he would call his wife, Mrs Sandra Scott to pick him up later that evening. In the event, Mr Scott refused the licensee's offer to call Mrs Scott on several occasions - the licensee did not know Mrs Scott's telephone numbers - and instead, Mr Scott demanded the return of his motorcycle and keys insisting 'he was alright to drive'. (Note that the earlier deterrence effect of random breath testing had worn off) Mr Scott crashed his motorcycle 700 metres from his home and died. Mr Scott's blood alcohol level was 0.25 (5 times the legal limit).

The issue before the High Court was whether the licensee had breached a duty of care to Mr Scott by returning the motorcycle and the keys?

The unanimous decision (5 judges) of the High Court said that there was:

- No duty of care
- No breach of a duty
- No causal link between the breach and Mr Scott's death.

The conclusion of the High Court was:

> *The conclusion is that, save in exceptional circumstances, publicans owe no duty of care to their customers in relation to how much alcohol is served and the consequences of serving it says nothing about whether publicans owe a duty to third parties who may be damaged by reason of the intoxication of those customers.*

Haynes J stated:

> *...persons in the position of the Proprietor and the Licensee owe no general duty of care at common law to customers which requires them to monitor and minimise the service of alcohol or to protect customers from the consequences of the alcohol they choose to consume.*

In Queensland, the *Liquor Act 1992* confers statutory duties and vicarious liability for certain matters on licensees. It states a licensee must:

- behave responsibly in the service, supply and promotion of liquor
- not engage in any practice or promotion that may encourage rapid or excessive consumption of liquor
- engage in practices and promotions that encourage the responsible consumption of liquor; and
- provide and maintain a safe environment in and around the licensed premises.

Licensees, particularly of the larger venues, legitimately raise issues about their ability to monitor the number of drinks patrons consume, their inability to judge when people are intoxicated because of the individual effects of alcohol intake; and their inability to know how much alcohol a person has already consumed over what period of time before the person enters the premises. The purpose of networked ID fingerprint scanning and CCTV is not to support responsible service of alcohol but to identify people primarily for law enforcement purposes and exclude people from premises for up to five years after some form of anti social conduct has occurred. There is no hard evidence that ID scanning provides a deterrent effect such that it improves the safety of the environment. There are other less invasive actions that could be taken to ensure licensees do provide responsible service of alcohol in a safe environment.

ALCOHOL AND VIOLENCE

There are many available resources on alcohol and violence. The International Center for Alcohol Policies is a not for profit organisation based in the USA supported by major producers of alcoholic beverages. The Committee is referred to ICAPs 'Blue Book' and a 2008 publication entitled "Alcohol and violence: Exploring patterns and responses" commissioned by the International Center for Alcohol Policies, available online at www.icap.org.

ICAPs conclusions are that

- the vast majority of drinking episodes does not lead to violence and most violence does not involve drinking
- Violent incidents involving alcohol also involve harmful or abusive drinking.

These conclusions appear to suggest that policy responses directed at all patrons are not proportionate to the problem (ie targeted policy solutions are suggested) and that it might be more effective for licensed premises to develop strategies focussed harmful and abusive drinking rather than on individual violent patrons.

In a more recent review of evidence in the paper entitled "The Role of Drinking Patterns and Acute Intoxification in Violent Interpersonal Behaviours", Kenneth E Leonard arrives at the following conclusions:

- it is not so much that alcohol causes aggression, as that aggressive people drink
- aggression may be exacerbated by alcohol in people who are Type 11 alcoholics or have with frontal lobe dysfunction.
- there are entrenched beliefs about alcohol causing aggressiveness but in people referred for problem drinking after a violent incident, analysis of **pre-drinking** motivations shows this was not the case.

To illustrate this insight the author quotes one of the sample:

> *Usually, when you go for a night out [drinking], you have two things in mind that you want: either you pull a bird [get a woman to sleep with you] or you get into a good punch up. The thing is though, if you pull a bird first, you don't take her home and beat her up, do you?*

Leonard quotes Critchlow[4], a leading expert in the psychology of drinking behaviour, who summarises the accumulated evidence about alcohol and violence as:

> *On a cultural level it seems to be the negative consequences of alcohol that hold most powerful sway over our thinking. Because alcohol is seen as a cause of negative behaviour, alcohol-related norm violations are explained with reference to drinking rather that the individual. Thus, by believing that alcohol makes people act badly, we give it a great deal of power. Drinking becomes a tool that legitimates irrationality and excuses violence without permanently destroying an individual's moral standing or the society's system of rules and ethics (Critchlow, 1986, p761)*

- Such an association of alcohol and violence does not operate in violence-repressing cultures.
- Male violence is triggered by public contests of honour or reputation
- In many societies around the world, heavy drinking is strongly associated with masculinity
- Where there is no expectation of violence, violence will not occur with any amount of alcohol. If there is an expectation, there is a high probability it will occur.
- In violence reinforcing cultures where there is an association of alcohol with masculinity, there is a far greater likelihood of incidence of alcohol related violence. In such cultures the drinking environment becomes the proving ground for male status.
- Several scientists have suggested that manipulation of these environments can reduce the incidence of violence
- The key environmental variables that escalate drunken aggression are noisy, cramped and badly maintained venues and venues in which tolerance or expectation of violence is the norm and in which social rules are not clear.
- Male propensity for aggression cannot be changed. There is no comment in the study of the increasing involvement of young women in anti-social behaviour. What can be changed are beliefs about alcohol, social responses to

[4] Critchlow, B. 1986. "The powers of John Barleycorn: Beliefs about the effects of alcohol on social behaviour", *American Psychologist, 41,* p761

violence and aggression in drinking environments and the drinking environment itself.

ID SCANNING

> *Raymond tells his partner, Lesley, that he is working behind at the office. Lesley is good friends with Joseph, a worker at Raymond's local bar - the Terminus Hotel. Lesley texts Joseph who accesses the hotel's computer system and then texts Lesley back with the information that Raymond entered the Terminus Hotel at 5.30 pm and a quick cross- check of the hotel's CCTV monitor shows he is currently drinking in the hotel's beer garden.*

ID Scanning is the process of electronically reading and storing proof of identification documents (**ID**). A modern ID scanner is capable of reading both sides of the ID and they can scan a wide variety of IDs. The scanned data can be uploaded as an image or used to automatically populate text fields in, for example, a database. The extracted data can be exported to other applications, such as Word or Excel, or communicated by way of an e-mail attachment or by posting it to the Web. Information captured by ID scanners may be stored on a single computer, standalone server, or shared across a networked system.

A 'top of the range' scanner costs $10,000[5]. One system, already in common use in Australia[6], is the idEYE; it scans a patron's ID and takes a real-time photograph of the patron. A recent development is the additional capture of a patrons' fingerprint[7], and to have the scanned ID interface with CCTV surveillance and biometric recognition software[8].

While biometrics has strong benefits in the areas of verification and identification of individuals, its use to date has been mainly in the areas of homeland security. For example, the US-VISIT (United States Visitor and Immigrant Status Indicator Technology) is biometric system used by US immigration. It cannot be legitimately argued that licensed premises need a similar level of sophisticated identification system to deal with persons simply wanting to drink in licensed premises.

The use of biometrics technology in Australia has to date been regulated under a code of conduct which industry can voluntarily adopt. While privacy considerations are fully built into the self regulatory scheme[9], it remains one that licensed premises can simply choose not to adopt.

Claimed benefits relating to ID Scanning

The following benefits are commonly claimed to result from ID Scanning:

- ability to verify the patron is the required age to enter the licensed premise
- easier detection of fake IDs
- easier detection of improper use of someone else's ID

---

[5] '*Up to six fake IDs confiscated every night.*' report by Alison Sandy of the Courier Mail dated 17 November 2009.
[6] For instance in Mackay – '*ID scanning cuts night-life violence*' report on abc.net.au/news dated 19 August 2009 and '*Northbridge introduces new ID scanning Software*', report by Scott-Mitchell on outinperth.com/news dated 16 October 2009.
[7] '*Brisbane nightclubs to introduce fingerprint scanning*' report by Sophie Elsworth in the Courier Mail dated 23 November 2009.
[8] '*Clubbers, prepared to be scanned*' report by Katherine Feeney in the Brisbane Times dated 21 November 2009
[9] The Biometrics Institute (Australia) offers Privacy Impact Assessment (PIA) and Audit Services to its members to assist them to make informed decisions on the management of the privacy issues associated with biometrics. See http://www.biometricsinstitute.org/displaycommon.cfm?an=1&subarticlenbr=113

- a formal record of the patron's attendance at the licensed premise
- ease of transmission of information concerning patrons between licensed premises; and
- deterrence of undesirable behaviour.

One of the fundamental privacy principles provides that personal information should only be collected for a lawful purpose directly related to a function or activity of the collecting entity, and that only necessary personal information should be collected. There are good public health (and other) policy reasons to support licensees in the responsible service of alcohol, in particular to prevent the serving of alcohol to minors. This has been the historical reason for licensed premises to check IDs as a condition of entry and concerns the first three dot points above. The checking of IDs for this purpose does not of course entail the collection and other use of personal information. To sell alcohol in a safe environment licensed premises do not need a formal record of a patron's attendance at the licensed premise, or to transmit the information concerning patrons between licensed premises. ID scanning 'deterrence effect' is not evidence based. The main use of personal information collected appears to be for it to be passed onto policy to assist in the identification of offenders and as such contributes to an all seeing eye capacity for QPS. This is demonstrated by the examples given by licensees who have existing computerised systems and CCTV on the way in which they have used the information collected.

While a patron can be fined for being under-age in licensed premises, the reality is that the fines imposed on the premises are ten times those imposed on an individual. As such, there is a significant benefit for the licensed premise being able to accurately establish the age of people seeking to enter the premise. However, the efficacy of an ID scanner for the purposes of age and identity verification is not absolute in that:

- A sophisticated forgery may still pass scrutiny by an ID Scanner.
- An ID Scanner will not detect a government-issued ID which has been fraudulently obtained.
- The ID Scanner will not detect that someone has presented another person's government-issued ID as their own, for example a sibling with a strong resemblance. Even if – as with the idEYE – a real time photograph is taken of the person presenting the ID the deception will not be apparent at the scan unless:
    - the photograph is cross-matched with the image on the ID,
    - the quality of both is high; and
    - the cross matching is very sophisticated.

Even if an ID scanner should prove more effective in detecting forged IDs than human senses, this function does not require storage of information taken from the ID. Capture of every patron's ID information is not necessary in order to verify their age. Manual inspection or scanning only of the ID will allow a patron's age to be verified from the ID document. Moreover, there is a need to conduct age verification by sighting ID for only a small percentage of patrons.

The underlying premise behind ID Scanning is that anti-social behaviour in licensed premises is solely the fault of the patron and accordingly, control of the patron will deliver a safer premise. The control is achieved through licensed premises:

- knowing who their patrons are and their personal details including home addresses
- watching what their patrons do at all times
- removing some patrons from accessing their services for indeterminate time periods.

Not all licensed premises have the same issue with anti-social behaviour. While it is commendable that licensed premises are looking for solutions to anti-social behaviour in venues, an escalating 'law enforcement' approach will not resolve the drivers of alcohol related violence. The use of ID Scanning is very intrusive and may result in antisocial behaviour shifting to other locations. By focussing on the patron, attention is deflected away from the licensed premises' inability to resolve the conflict between the profitability of supplying large volumes of alcohol and the responsible service of alcohol, their and liquor licensing's responsibility for an environment conducive to alcohol misuse and bad behaviour, and the community's responsibility for its culture around violence, masculinity and drinking.

Policy options that encourage licensees to otherwise focus on providing a safe environment without the need to compromise fundamental human rights should be developed. For example, the names of the most violent licensed premises are published in NSW.[10] This has been credited for a downturn in the number of reported incidents. The NSW Police Commissioner Mr David Owens considers that a combination of tougher police enforcement of incidents, restrictions on opening hours and the "shaming" of pubs by publicly listing their assault rates' has had a significant effect on the number of incidents.[11] This approach is consistent with the Right to Information reforms where government agencies use information strategically to activate the community in resolving issues and to dampen demand on their resources.

The success appears to have resulted from a working partnership between the community and the licensees. Commissioner Owens states[12]:

> *"The community is actively working with us to say, 'We don't want anti social behaviour, we don't want drunks punching on in the streets outside our premises, inside our licensed premises,'*

Ms Sally Fielke, the Australian Hotels Association Chief Executive has claimed:[13]

> *"We would attribute [the decrease in the number of incidents] to the hard work that licensees have put in in terms of being extra vigilant on staff training, additional responsible service of alcohol measures and other proactive initiatives.*

None of the 'successful' mechanisms cited by Ms Fielke involves compromising the privacy of patrons.

---

[10] See - 'Revealed: the most violent pubs and clubs' a report by Matthew Moore, Sydney Morning Herald 11 March 2008.
[11] '*NSW to stay tough on pub violence*' report by Stephanie Gardner, AAP, 5 November 2009.
[12] Ibid.
[13] Ibid.

Claimed benefits relating to a deterrence factor

A common argument for the introduction of ID Scanning is that it makes the licensed premise safer for the patrons.[14] Patrons are advised that scanning of IDs is undertaken in order to better protect them. It is claimed that ID Scanning has a significant effect on the behaviour of the patrons in the licensed premise. For example, it is asserted that the use of ID scanners in Geelong nightclubs is responsible for a reduction in alcohol-related crime. The Home House nightclub has reported one incident of assault in a year compared with four incidents per weekend the previous year[15]. Importantly there is no information about whether the problem shifted to another location by people being deterred from entering that particular club and choosing to drink elsewhere and in locations where incidents may be less likely to be reported to police.

Senior Sergeant Mick Searle of the North Queensland police stationed in Mackay has stated:

> *In a lot of cases people are now realising that, 'hang on a sec, they know who I am' which means that they then think twice about committing some act of violence or antisocial behaviour against another patron. Which means that the venue is safer for everyone inside them and we get the people that don't want to adhere to that sort of code of behaviour, well they don't go in.*[16]

The deterrence effect of 'being known' assumes that aggressive patrons who decide to enter a licensed premise

- care
- have been fully informed of the possible uses by police of the information collected
- do not become disinhibited or more impulsive after imbibing alcohol and
- that patrons retain the cognitive reasoning capacity to remember ID scanning is in place, consider it and rationally decide to walk away before an incident escalates. It requires a person to think 'This person has done something with which I do not agree and while my immediate response would be to hit them, I will not act on this impulse because I will then be held personally responsible for that action.' It is not a given that a person whose cognitive reasoning is adversely affected by alcohol will be capable of this reasoning.

There is another evidence based reason for patrons not going into clubs with IC scanning. That evidence is discussed under the heading 'Community attitude to ID scanning'.

On a practical basis, the use of ID Scanning alone does not allow a licensed premise to 'know who you are'. The ID Scanner will create a record of who *enters* a licensed premise at a given time, but, unless the patron also 'scans out', it will not provide a reliable indicator of who was *in* the licensed premise at a given time. Nor, should undesirable behaviour occur within the licensed premise, will it allow the identification of those involved in the behaviour. Identification would still need to be carried out manually, and, if the licensed premise deemed it appropriate, its records on the identified individuals updated to reflect their behaviour. Realistically it seems unlikely that a licensee could physically restrain an anti-social or violent person to take their

[14] Ibid.
[15] Op cit at 2.
[16] Ibid.

fingerprint or physically take their ID from them to confirm their identity at the time of an incident.

In order for an licensed premise to 'know who you are' ID scanners must be combined with a real-time photograph of the patron taken when they enter, and CCTV systems recording what occurs in the licensed premise. Should undesirable behaviour occur, the CCTV footage can be cross-referenced with the entry photograph—either manually or, if the CCTV footage is of the necessary quality, through facial recognition software. The cross matching will in turn be matched to the scanned ID, which will reveal, depending on the form of ID scanned, the residential address of the individuals involved.

Casablanca owner Sarosh Mehta provided a real life example of this potential:[17]

> *A couple of weeks ago we had an issue, the police came the guy did a runner.*
>
> *We had him on the CCTV...but because we also had his real time photo and ID information we were able to hand the authorities the data they needed to chase him down the next day.*

Incidents such as show that it is not so much the claimed deterrence benefit of ID scanning that interests licensees but that the real purpose in collecting the information is for and on behalf of the police.

Licensed premises are not free to take the law into their own hands. Law enforcement and investigation is not a function of a licensed premise – this is the function of Queensland's law enforcement agencies, such as the Queensland Police Service (QPS) or the Office of Liquor and Gaming. The privacy principles specifically permit the passing of personal information to enforcement agencies, so it would not be a breach of the privacy principles to provide the QPS with personal information if it was needed to enforce the law. However, the privacy principles do not permit a licensed premise to collect personal information just in case it needs to give that information to QPS. The only personal information which can be collected is that which is needed for a legitimate purpose of the licensed premise.

Claimed benefits arising from the circulation of personal information between licensed premises

> *Josephine presents her ID to enter a bar in Townsville with some work colleagues after attending a conference but she is denied entry. The door staff advise her that five months ago she got into a heated argument with the bar staff of a tavern in Brisbane over short-changing and she was subsequently placed on a 'ban list'. This is the first time Josephine is aware that this information concerning her exists. Josephine further contends that the record has incorrectly been linked to her as she has never even visited the tavern as it is located in the opposite side of the city to where she lives and socialises.*

Another argument for ID Scanning is the ease with which it will allow licensed premises to exchange ID data. Again, it is claimed that this will increase patron safety. Bree Maddox, owner of the Court Hotel in Northbridge, Perth has stated:[18]

> *'What happens is that if someone is removed because of unacceptable or violent behaviour it basically means that they can't walk down the street get into another venue.'*

[17] Op cit at 4.
[18] Ibid.

A reduction in the opening hours will also achieve a similar outcome without offending fundamental human rights.

ID Scanning allows the simple and easy compilation of patron lists, complete with patron profiles. The obvious outcome of such lists is the creation of a 'ban list' or 'blacklist'. As this information is electronic, it can easily—in some cases, instantaneously—be provided to other licensed premises. A simple keystroke could implement a 'banned from one, banned from all' practice. Licensees freely acknowledge that the creation of a blacklist is one of the purposes of ID Scanning.[19] One timeframe suggested for keeping a person's name on a blacklist is five years.[20]

Before any government endorsement into such information sharing practices can be considered, there are several essential questions which must be answered:

- Where will the transfer of personal information stop? Will it be limited only to the personal information of those who have been found guilty of a crime or misdemeanour in a licensed premise, or will it extend to anyone that has committed a crime or misdeamour or to anyone the licensed premise would rather not have in their premises?
- Will patrons be blacklisted for behaviour that is not criminal in nature?
- Who will decide whether a misdeamour is serious enough to warrant blacklisting?
- How will the identity of the person be confirmed?
- Will the length of the ban be proportionate to the seriousness of the anti-social behaviour?
- Will it be shared only between licensed premises owned by the same legal entity, or between all other licensed premises, regardless of who owns them, including restaurants?
- Will police be able to access the information when investigating the whereabouts of interested persons, establishing alibis in unrelated crimes, including using licensed premises databases of fingerprints as an extension of police records?
- Will it be shared between interstate licensed premises? Internationally?
- What safeguards will surround the sharing?
- What mechanisms will be put in place to ensure the information is accurate and up to date?
- What training will be provided to licensed premise employees to ensure all personal information is handled appropriately?

[19] '*Nightclub blacklist*' report by Nicole Carrington in the City News dated 26 November 2009.
[20] Ibid.

- To whom can a patron complain if they find themselves unjustly placed on a blacklist, perhaps because someone used a fraudulently obtained government ID which the ID scanner was unable to detect?

- What mechanisms will there be for a person to challenge their placement on a 'ban list'?

The blacklist allows licensed premises to act as judge and jury, imposing 'sentences' at the list compiler's discretion. Inclusion on a blacklist could, and likely would, occur without the patron's knowledge or consent and there appears to be no right of response to, or review of, being placed on a blacklist. If a person has no way to know they've been blacklisted until they are refused entry, they would have no way of exercising a right of response or review even if one existed.

The licensed premise's profile of a patron, and any blacklist on which their name appears, is the patron's personal information. The privacy principles explicitly provide that an individual has a right to access their personal information and, if they believe it to be wrong—inaccurate, incomplete, misleading or out of date—to seek amendment to correct the record. If licensed premises introduce such information sharing and profiling activities, they must also introduce procedures to allow patrons to seek access to, or amendment of, their personal information, and to deal responsively with such requests.

Community attitudes towards ID Scanning

The use of ID Scanning by licensed premises may not only infringe privacy and other fundamental human rights, it could also adversely impact on the licensed premise's business. A 2007 survey conducted by the Commonwealth Office of the Privacy Commissioner found that, while 80 percent of people thought it acceptable to *show* their ID, *82 percent considered it unacceptable that their ID be recorded as a condition of entry onto licensed premises.*[21] It can be presumed that the community's negative reaction to fingerprint scanning will be similarly strong.

Those concerned with the rapid spread of ID scanners in licensed premises raise the point that such scanning effectively tracks both a person's movements and their social associations and interactions during what is purely a leisure activity.[22]

It is a fundamental privacy principle that the collection of personal information is not an 'unreasonable intrusion into the personal affairs of a person'. Australia is not a society where citizens are required to carry ID papers at all times and to produce those papers on demand. (For the convenience of patrons, some NSW licensed premises are offering to microchip patrons.) Nor is Australia a society which expects citizen movements will be tracked at all times. From the results of the Privacy Commissioner's survey, it seems reasonable to extrapolate that the majority of people consider a beer at a hotel on the way home is 'nobody's business but theirs'.

The ID scanner creates a record that the patron is not physically at their residence. Cross-checking of the scanned ID may reveal that other adults who live at the same address are also in the licensed premise. This information could be used to determine that a given residence was empty and likely to remain so for a portion of the evening, making the residence a target for thieves.

---

[21] *Community Attitudes to Privacy*, August 2007, Office of the Privacy Commissioner at page 79.
[22] 'A farewell to the era of anonymous drinking' article by Jem Matzan dated 9 January 2008 available at www.thejemreport.com

What the ID data reveals about the emptiness of a residence is not the only information valuable to criminals. The ID data itself is an extremely valuable resource for identity theft. For example, a driver's licence (often the primary form of identification) contains:

- full name
- photograph
- signature
- addresses – both current and potentially past
- unique government identifier—licence number
- date of birth
- height.

In addition, a driver's licence contains wholly irrelevant, potentially highly sensitive, personal information which is of no legitimate interest to those who operate licensed premises, such as what vehicles a person is licensed to drive and whether or not they are an organ donor.

It would be a significant concern if licensed premises, including those with a turnover of less than $3 million are able to introduce ID Scanning as an entry requirement, without being required by law to take steps to address both the potential risks of storing such information and the legitimate privacy concerns of their patrons. If a policy decision was made to endorse the introduction of ID scanning, licensed premises should be required by law to introduce clear, comprehensive, and effectively communicated procedures which set out how the ID data will be handled, stored, used and disclosed, and staff must be trained in those procedures.

Patrons must be given sufficiently detailed collection notices, so they are fully informed of what the licensed premise will do with their information and why the licensed premise wants it. If licensed premises claim to collect personal information for the safety of patrons, there should be an evidence base for this claim, past anecdotal information from industry and police. Adequate security safeguards must be introduced to prevent unauthorised access, use or disclosure of the scanned data, particularly while that data is being transferred.

Privacy Considerations

The procedures should be readily available on request, and they must, at the least, address the following key considerations.

Need for ID Scanning

> The community accepts that there is a need to verify age in relation to activities which have a mandated minimum age requirement. Viewing appropriate ID and assessing its bona fides are considered by the general community to be reasonable actions for a licensed premise to take *in relation to those persons for whom their age is uncertain.*[23]

[23] Ibid.

There may be an argument that this assessment can be more accurately and speedily done electronically rather than manually. However, where an ID is not a forgery but rather has been obtained by fraudulent means, it is arguable that humans are better than machines at detecting the fraud. For example, an ID scanner will not be able to detect that a woman has presented with her sister's (genuine) driver's licence[24], but an experienced bouncer, observing the woman, may be able to detect the woman's nervousness and so subject the ID to closer scrutiny.

A licensed premise must be able to justify why it needs to go beyond simply viewing ID. As soon as the ID is scanned and that data is kept, the transaction between the patron and the licensed premise is no longer anonymous. It should be borne in mind that, for the majority of patrons, their age and their behaviour on the licensed premise is not of concern. Yet these patrons are being asked to potentially surrender their privacy. In the absence of any criminal imputation, these patrons are being asked to provide their ID data, and in some circumstances, fingerprints and photos, and trust that this information is necessary to enable the transaction and that it will be kept safe. The licensed premise should explain the *benefits to the patron* of their personal information being collected.

Once the purpose is fulfilled, the data should be deleted by the licensed premise. Unless the data is required for a legitimate secondary purpose–such as provision to the Queensland Police Service for the purposes of law enforcement–the data should at least be de-identified, and ideally destroyed, after 24 hours.

Collection

Fundamental to the privacy principles is the requirement that a person be told why their personal information is needed, what it will be used for, and to whom it will be given. The organisation must have a definite, legitimate use for the information and only information relevant to that purpose should be collected. If the licensed premises were to scan a person's driver's licence as a whole, it would capture personal information that is of no conceivable use to it – such as the person's organ donor status.

The collection must not employ 'unfair means'. Accordingly, the licensed premise must involve the individual in the scanning process and the scanning process must be transparent and honest.

Security

> *So they will scan your ID, take your photo and fingerprints. That's a high risk of identity theft. How secure will the information be and who will control it? By the time you get home someone will already have punched out a few fake drivers licenses in your name etc and rolled your house whilst you're at the pub.*[25]

[24] It is relatively easy for a person, using someone else's identity documentation, to obtain a government-issued identity card. See *Student reveals how easy it was to get fake ID*, report by Alison Sandy of the Courier Mail dated 17 November 2009.

[25] Anonymous comment posted online in response to 'Brisbane nightclubs to introduce fingerprint scanning' report by Sophie Elsworth, in the Courier Mail dated 23 November 2009.

Personal information is commercially valuable; collections of personal information even more so. The more extensive the collection, the more is it worth. It is common sense that the greater the value of something, the greater the protections which must be applied to it. Licensed premises which scan and store patron IDs, especially where this is done in conjunction with photographs and fingerprints, are collating an extensive library of patrons' personal information, of value for both lawful and unlawful purposes.

The information is also potentially vulnerable to internal manipulation and abuse, for example, it may be beneficial to Mr X for the local club's records to show that he arrived at a particular time on a specific night. If there are no safeguards in place to prevent unauthorised alteration of the data, and no audit function which will show who accessed it and when, Mr X could effectively 'rent an alibi' from a willing club employee.

Licensed premise instigating ID Scanning must be required to take all necessary steps to ensure the integrity and security of the scanned data through robust measures such as:

- limiting access
- instigation of audit trails
- firewalls
- data encryption; and
- holding data only for a limited time.

Disclosure

> *Awesome Alcohol has introduced a new 'alcopop'. It puts on a promotion at the Terminus Hotel between 7pm and 9pm each night for a week. How successful is the promotion with the target 20-30 year old demographic? The data from the ID scanners can be used to gauge that success. Did the patrons approve their data to be used for marketing purposes? They wanted nothing more than to have a drink with a friend before going out to dinner – what was once a simple, anonymous everyday occurrence has resulted in them being the focus of behavioural targeting.*

The privacy principles require an entity which is collecting personal information to tell individuals to whom it will be disclosed. If an entity later discovers it needs to legitimately disclose it to someone else it can rely on the disclosure exceptions. These exceptions are generally disclosures which people could reasonably anticipate. For example, disclosure is authorised by law, required for an ongoing enforcement investigation, or necessary to prevent a loss of life.

But how many people would be aware that a licensed premise may give their information to the police even when they have not been involved in an incident? Personal information is able to be provided to police for the purposes of investigating a potential unlawful activity. For example, the police are interested in Person A. They are also interested in Person B. They are particularly interested in whether Person A and Person B are working together on an unlawful activity. Why not check whether Person A and Person B have been present in the same licensed premise at around the same time? If law enforcement agencies were given remote access to

licensed premise databases, this could be done without ever leaving the office.

People may also not be aware that it is permissible for an organisation to give or sell their collections of personal information for the purposes of direct marketing (albeit with limited conditions). The mere action of dropping into your local hotel for a quick drink on a Friday night after work can, because your ID was scanned by the hotel, be the prompt for a marketing campaign targeted at you and your home.

As a matter of sound business practice, the licensed premise should take reasonable steps to make the patrons aware of any intended use of their personal information by the premise for marketing purposes. The premise should also provide the option for patrons to opt out of marketing and promotional campaigns.

CLOSED CIRCUIT TELEVISION (CCTV)

CCTV is a system which allows the capture of images and video footage on a closed loop which is accessible only by persons directly connected to the loop. A typical CCTV system includes one or more cameras linked to a 'control room'—a centralised area which allows monitoring and management of the camera systems.

Proliferation

CCTV is now a ubiquitous surveillance tool, used by government and private sector alike. Generally, government sector CCTV is directed towards the security and safety of public spaces and crime prevention. Private sector CCTV is generally used to secure and observe privately owned spaces. Despite its proliferation, CCTV is a relatively recent phenomenon. In 1960 the first two public CCTV cameras were erected on a temporary basis in Trafalgar Square in London to assist the monitoring of crowds during a state visit. Today the UK is potentially the most 'watched country in the world'[26] having an estimated 4.3 millions cameras – one for every 14 persons – with London having a million cameras alone[27].

Closer to home, Australia has to date had a more modest love affair with the CCTV camera. In 2005, Sydney had only 7,000 CCTV cameras[28]—approximately one camera for every 600 persons. Brisbane City Council currently operates 56 CCTV cameras in and around the Queen Street and Fortitude Valley malls and a scant 100 cameras across the rest of Brisbane, monitoring roadways, Council buses and Council car parks.[29]

Among state governments, the Queensland State Government is a notably strong supporter of CCTV systems. The then Department of Local Government, Planning, Sport and Recreation administered the Security Improvement Program (SIP), which offered grants to local councils of up to fifty percent of licensed premise costs for CPTED (Crime Prevention through Environmental Design) to assist local government

[26] It is estimated that one-fifth of all CCTV cameras world-wide are in the UK - http://www.caslon.com.au/privacyguide20.htm.
[27] '*Big Bother. How a million surveillance cameras in London are proving George Orwell wrong.*' Article by Jamie Malanowski in Washington Monthly November/December 2009 at pp. 11-16.
[28] '*CCTV and other visual surveillance*' a Caslon Analytics privacy guide available on www.caslon.com.au/privacyguide
[29] Figures taken from http://www.brisbane.qld.gov.au/BCC:BASE::pc=PC_68 dated 1 October 2009.

security initiatives. The initiatives included 'the provision of surveillance equipment in malls and other public places'[30].

However, the use of CCTV in Queensland will likely continue to grow, particularly as technology advances in this area. As recently as 1 December 2009 Police Commissioner Bob Atkinson revealed a plan to use unmanned surveillance aircraft on a '24/7 basis' to monitor Queensland traffic.

Community attitudes towards CCTV

Studies[31] and surveys[32] show that, generally, the community supports the use of CCTV as a means of preventing crime and social disorder in those areas where there is a 'legitimate expectation of public observation'. The community sensibly accepts that they can be observed by any number of people in public spaces, such as a public mall, and that CCTV surveillance is just another observer. Accordingly, the community may be more accepting of CCTV in large licensed premise's which have a public space feel but less accepting in the small corner bar, and far less accepting of surveillance in a toilet area. Research into the public acceptance of CCTV in licensed premises and an evidence base should inform any policy response.

Effectiveness of CCTV in preventing crime

There are dozens of CCTV cameras at Sydney Airport, but despite this 'high security', a man was killed in broad daylight a few weeks ago. If having CCTV around doesn't stop murder, what can it actually do?[33]

It is often presumed that CCTV prevents crime and social disorder by acting as an effective psychological deterrent to potential offenders. While the community supports CCTV as a crime prevention tool *in principle*, it does not consider that CCTV does in fact have a significant effect on crime prevention. [34]

Research supports this perception. The '*Crime and CCTV in Australia: Understanding the Relationship'* report concluded that CCTV is effective at *detecting* violent crime, and/or may result in increased reporting, as opposed to *preventing* any type of crime. The study also concluded that the 'human factor' remains a strong influencing factor in CCTV's effectiveness in detecting criminal activity:[35]

Findings from the observational study indicated that the effectiveness of CCTV may be very much dependent on a whole range of issues but in particular the monitoring strategies adopted by camera operators... Although it was anticipated that most surveilled incidents would be initiated by the camera operators themselves, it was determined that approximately half resulted from the police requesting specific surveillance of a person or incident. The observational study also suggests 7 of the 51 arrests were the direct result of the camera network with remaining arrests attributable to police communication and simultaneous detection.

---

[30] Security Improvement Program Guidelines page 1 available on http://www.localgovernment.qld.gov.au/Funding/Previousfundingprograms.aspx

[31] Such as '*Crime and CCTV in Australia: Understanding the Relationship'* by Helene Wells, Troy Allard and Paul Wilson of Faculty of Humanities and Social Sciences, Bond University, 2006.

[32] *Community Attitudes to Privacy*, Office of the Privacy Commissioner, August 2007.

[33] Comment by person identified as 'Frank' cited in '*How good are CCTV cameras at preventing crime?'* article by Maryke Steffens dated 15 April 2009 at www.abc.net.au/science/articles.

[34] In '*Crime and CCTV in Australia: Understanding the Relationship'* 93.5% of persons surveyed supported the use of CCTV to prevent crime but only 46% considered that it actually prevented crime. Op cit at 14 at page 51.

[35] Ibid at page 13.

As noted earlier in this submission, one immediate benefit of CCTV for licensed premises is the capacity to, after an incident has occurred, pick out of the crowd those who were involved and, in conjunction with ID Scanning, identify them and their domestic addresses.

In addition, CCTV has the following claimed benefits:

- monitoring employee behaviour
- protection and security of assets – property and equipment
- provision of evidence in criminal and civil actions in the courts or in other disciplinary proceedings
- resolution of issues and complaints.

Addressing privacy issues

The Terminus Hotel has a CCTV system. The manager of the hotel has compiled some of the footage into a 'most embarrassingly drunk patron' video, and it is regularly shown to hotel employees for their amusement on work social occasions. Maree, one of the hotel employees, 'borrows' the compilation to show her friends, one of whom recognises herself in the video.

The following measures should be put in place to protect the privacy of persons recorded by CCTV.

- The recording of images should be undertaken fairly and lawfully.
- The cameras should be in plain view and their use should be brought to the attention of patrons by way of signs placed at the entry to the licensed premises and in the areas they are used.
- The recorded images should only be used for the purpose for which the CCTV system was installed, unless the footage is required by a law enforcement agency. While it would be tempting to use the footage for staff training or marketing purposes, it was not collected for these purposes. An exception to this would be the training of staff in the use of the CCTV system.
- The CCTV system should only be used to identify incidents occurring within a defined operational area, and it should not to be used to record outside this area. For example, even though a licensed premises camera may have the capacity to record a person walking down the street, this area is a public place and the licensed premise has no business recording within this space.

Information concerning the CCTV should be made available to patrons at the point of capture, including:

- who owns and operates the CCTV system
- when the system operates
- rights of patrons to access the footage
- any policy governing the use of CCTV, including security and access by employees and police
- the period of retention of the footage and the method of destruction or disposal of old footage; and

- the mechanism for dealing with inquiries and complaints concerning the CCTV.
- The use of CCTV in conjunction with ID scanning, real time photographs, biometric and facial recognition software and what this capability enables the licensed premises to do and to what use they might put the aggregated data.

At the very least, the information above should be available upon request. Accordingly, in the first instance, the licensed premise's employees and contracted staff should be able to answer inquiries concerning the CCTV system with more detail than that which is made automatically available. Other than in exceptional circumstances, it is not sufficient for inquiries to be referred elsewhere, to persons who are not present in the premises or who are not available at that time.

Before the licensed premise uses the personal information recorded by the CCTV, it should be required to ensure the information is accurate. For example, if the licensed premise provides footage of an incident to the police, it should ensure that the footage is only of that incident on the relevant date.

The licensed premise should restrict access to the control room and to the recorded footage. There should be a clear audit trail for access to the footage. Showing the footage to, for example, select staff members for their amusement and enjoyment, must be absolutely forbidden and attract strict sanctions should it occur.

If the licensed premise considers the footage should be released to the public for a beneficial purpose, for example, to obtain the public's assistance in identifying the alleged perpetrator of a crime, the licensed premise should consult with the Queensland Police Service on the footage's release.

When providing a patron with access to the footage, the licensed premise should bear in mind that other patrons may be captured on the footage and it would be a breach of their privacy to disclose their images to another person.

CONCLUSION

Requiring ID Scanning, photography and fingerprint collection before allowing entry to, and widespread use of CCTV surveillance in, licensed premises are significant incursions into the privacy of individuals. The majority of patrons in licensed premises are and will continue to be law-abiding persons engaged in a commonplace leisure activity. ID Scanning and CCTV surveillance indiscriminately captures the law-abiding of-age patron, by far the majority, as it attempts to detect the minority of patrons engaging in inappropriate actions, social misbehaviour or criminal acts.

The community generally recognises that enforcement of the law should be undertaken by the relevant enforcement agency and that it is not always entirely compatible with privacy. Law enforcement officers, such as the police, have special rules in the privacy principles when conducting investigations. However, even with these special rules, law enforcement agencies are not permitted to compile dossiers of personal information on law-abiding citizens. They must have at least a reasonable suspicion that the person in question is involved in a crime. If police officers were to stop persons in the street who were engaged in ordinary, lawful, day-to-day activities and obtain the person's information 'just in case' they ever committed a crime there would be public outcry, even with the oversight to which police are subject. Yet, if licensed premises begin using ID scanners and taking photographs and fingerprints as a condition of entry, especially in conjunction with

CCTV, this is effectively what they are doing: compiling a dossier on law-abiding patrons, 'just in case' they do something wrong.

It is claimed that significant benefits flow from the use of ID Scanning and CCTV in licensed premises. The benefits may not necessarily be those that are claimed, the claimed benefits may not be accurate or likely, and they may not necessarily be those which benefit the patrons. Regardless, the claimed benefits must be carefully assessed for accuracy and the actual benefits and their extent identified. Those benefits must then be weighed against the benefits of alternative policy options and the detriment that is the surrender of patrons' anonymity and all its attendant risks.

There is a near certainty that abuses will occur in respect to licensed premises' extensive library of patrons' personal information. That potential can be minimised with the implementation of stringent privacy safeguards but, as with many of these protections, the safeguards are only effective if the individuals managing and using the systems understand and utilise them, and are given no opportunity to circumvent them. And, where there is no oversight, there may be little to no motivation to utilise such safeguards in the first place.

While licensed premises appear eager to introduce the full panoply of ID Scanning and surveillance, it appears the community does not support its use. Accordingly, unless patrons can be assured that their personal information will be respected, protected and used only for the reasons they were *told* it would be used, licensed premises may find that, instead of protecting their clients, they end up driving them elsewhere.