Facial Recognition Technology

Discussion Paper
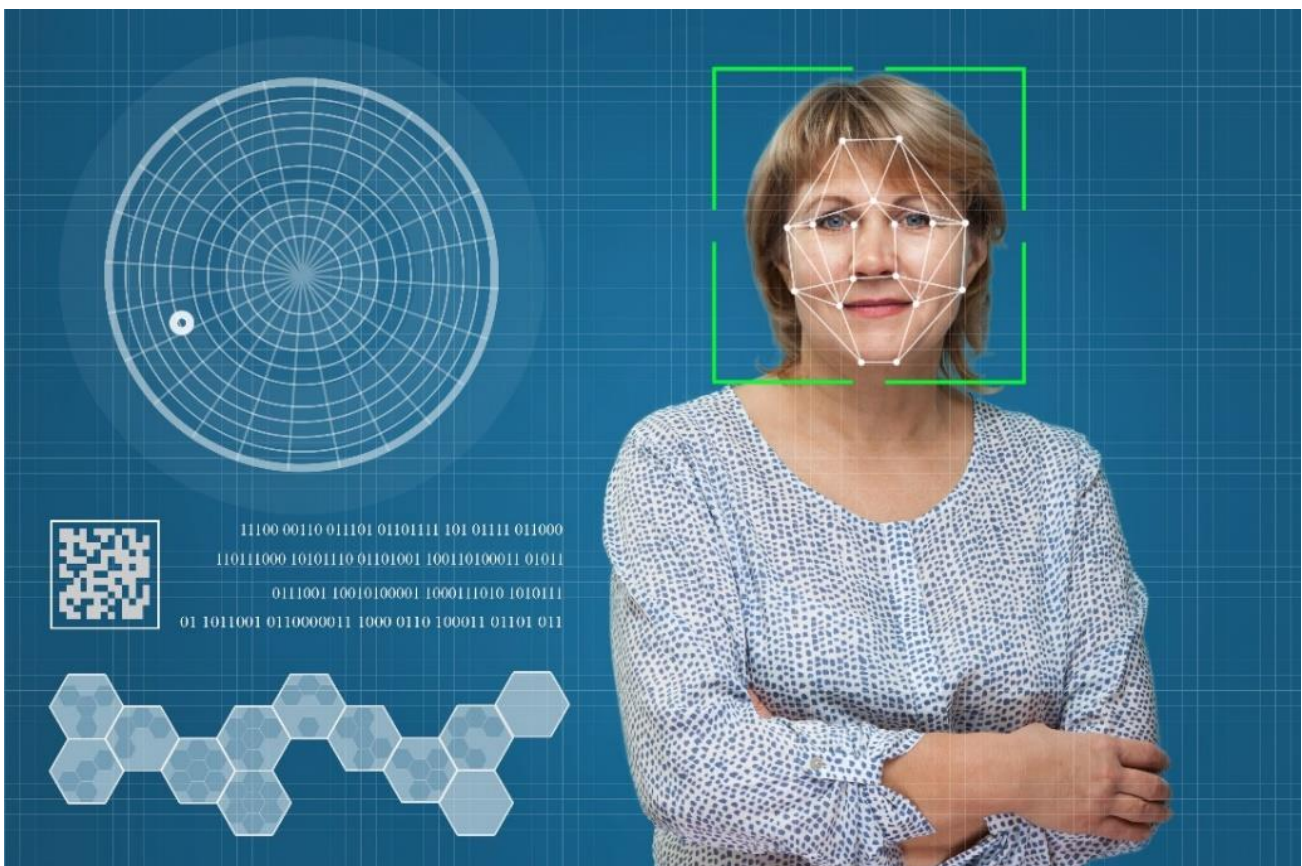
Wesley Public Affairs & Advocacy

February 2023

Contents

1   Executive Summary

Facial Recognition Technology (FRT) is a component of a surveillance system matching images of faces to reference databases.

In the context of the gambling industry in NSW, FRT is most often discussed as a tool to detect people who are self- or venue-excluded, in order to prevent them entering or to remove them from the premises. Significant privacy concerns and error rates are sufficiently troubling that the Australian Human Rights Commission has called for a moratorium on the use of FRT in policing and law enforcement situations until appropriate legislation is in place[1].

FRT is also used to detect cheating, to surveil staff to prevent theft, and as part of the data collection system venues use to build more detailed customer profiles for marketing purposes. FRT is combined with Artificial Intelligence (AI), CCTV, and Near Field Communication (NFC) devices to form an intelligence ambience in many venues, with a key use of this data being to induce people to gamble more and longer than they intended.

It is used in casinos in Macau, Nevada, and possibly in Australia, to detect how an individual behaves to keep them at a game longer than they planned, and to reduce their gaps in gambling by allowing customers to order food or drink without leaving the table or machine.

Although the data FRT systems help create is protected in general terms by basic Australian privacy laws, in practice, the issues of consent, data usage, third party access, privacy and security are not currently well articulated in legislation in NSW[2].

A survey by CHOICE found 76% of customers in a non-gambling retail setting were not aware their images were being captured; 78% were concerned about the storage of their data; 75% were concerned companies might use that data for marketing purposes and 83% believed retailers should properly inform customers about their use of FRT[3]

FRT is not a gambling harm minimisation tool.

At best, FRT is a mechanism to assist a venue in upholding its obligations under (self) exclusion agreements to help keep excluded people away from gambling opportunities. In this role, it may help prevent further harm to people who have already been significantly harmed by gambling. FRT cannot prevent harm from initially occurring and if anything, in the way it can currently be used, actually promotes harm by potentially prolonging the exposure of people to gambling beyond their means through targeted marketing and engagement tactics.

---

[1] Human Rights and Technology Report, AHRC, 2021 Recommendations 19-21: Facial recognition & biometric tech | Human Rights and Technology
[2] 21 Aug 2019 Facial recognition: ten reasons you should be worried about the technology (theconversation.com); 27 Sept 2022 Model law proposed to control 'Wild West' of facial recognition technology in Australia - ABC News
[3] June 2022 CHOICE survey: CHOICE reveals Kmart, Bunnings and The Good Guys are using facial recognition technology on unsuspecting customers

1.1   Recommendations

1. In almost every situation, the use of a mandatory harm prevention cashless card would achieve a better exclusion and enforcement outcome than FRT, and without any invasion of privacy.
2. No FRT should operate in NSW pubs or clubs until a "model law" is enacted in NSW[4].
3. So that customers can give informed consent at gambling venues to the capture and use of their images, there should be prominent signage, regular announcements, and in the case of clubs, front desk staff telling customers FRT is operating on the premises.
4. Legislation related to the use of FRT should protect human rights, as recommended by the Australian Human Rights Commission.
5. The collection, use and disclosure of data from FRT in gambling venues should be explicitly regulated and protocols approved by an independent agency, for instance the Information and Privacy Commission (NSW).
6. FRT should not be counted as a harm minimisation measure. It may, however have a role in assisting exclusion operations.
7. Venues should explicitly be restricted from using FRT or other surveillance devices to amass data about their customers.
8. Any data or metadata derived from surveillance should be held in databases managed and operated independently from venues and government.
9. Significant penalties for using FRT for anything other than an approved purpose related to Responsible Conduct of Gambling (RCG) should be put in place.
10. FRT data use for law enforcement purposes should require a warrant.
11. In the event that a third-party exclusion system is established, a system should be in place to manage access if there is a need to demonstrate to the independent third-party authority a person's gambling behaviour, through images captured by FRT

---

[4] Davis et al 2022 Facial Recognition Technology - https://www.abc.net.au/news/science/2022-09-27/facial-recognition-technology-model-law/101474010

2   Discussion

2.1   Glossary

- AI – Artificial Intelligence
- AML – Anti money laundering
- APP – Australian Privacy Principles
- CTF – Counter terrorism financing
- FRT – Facial recognition technology
- OAIC – Office of the Australian Information Commissioner

Wesley Mission does not have access to staff in venues who install, operate, interact with or maintain FRT systems. This discussion paper relies on information in the public domain.

We also acknowledge many venues have AML/CTF reporting obligations, which may require record keeping as mandated by AUSTRAC, and venues should be more vigilant in enforcing self-exclusion deeds. Our concerns about FRT should not be taken as barriers to the gambling industry being compliant in these two key areas.

Gambling harm prevention means more than honouring a deed of self-exclusion from a person who has been significantly harmed by gambling. Measures should be able to prevent people becoming so harmed they feel they need to self-exclude. **If the only measure a venue implements is FRT directed at excluded people, they are not acting to reduce harm.**

2.2   What is facial recognition technology?

FRT uses a camera and software to

- Identify there is a face in an image
- Compare the face to a reference image
- Either verify identity (one-to-one matching) or identify an individual (one-to-many matching)

FRT can be used to unlock a smart phone or perform immigration checking (one-to-one matching of one face, usually in optimal lighting and minimal movement, against a known single image). It is also used to check if a person in a club or pub is on an exclusion register (one-to-many), where the image captured is usually taken under suboptimal lighting, the subject is moving, and the database contains multiple potential matches.

There is a known racial bias in FRT – it works best for white adult men, and worst for black or Asian women[5]. False positives and false negatives mean either people who are not excluded could be asked by staff to leave, or people who should be subject to intervention can gamble without detection.

In the US, the Electronic Privacy Information Center obtained FBI data showing the FBI's system had a margin of error of 20%[6].

Any positive identification of a face usually then has to be checked by a staff member.

Beginning in 2015, studies have shown human operators also make errors. These can be as high as 50%, even among experienced operators. Highly trained operators were able to reduce

---

[5] 2022 Johnson, T. et al Facial recognition systems in policing and racial disparities in arrests; 2020 Albiero, V. et al Analysis of Gender Inequality in Face Recognition Accuracy; 2020 Najibi, A. Racial Discrimination in Face Recognition Technology

[6] At Facial Recognition Databases Hearing, Congress Attacks FBI (nbcnews.com)

errors to around 30%[7]. Some individuals are 'super-recognizers', having an ability to be accurate that is stable over time. Such individuals are around 2-3% of the population[8], which suggests staff in pubs and clubs who are employed for other qualifications and skills are unlikely to be 'super-recognizers' and more likely to be making errors.

2.3   Data protection and privacy

Before considering ways FRT might be used in NSW gambling contexts, it is necessary to review the legislative protections on privacy. This section of the discussion paper is based on the HWL Ebsworth Lawyers publicly available paper *Facial Recognition Technology and the Law[9]*.

2.3.1   Biometric information

There are thirteen Australian Privacy Principles (APP), in Schedule 1 of the Commonwealth Privacy Act 1988. The APP do not generally apply to an organisation with a turnover of less than $3million, which may exempt some smaller pubs and clubs.

Under Australian privacy laws, biometric information is considered to be personal information. Although not defined by the Privacy Act or the APPs (which are technology neutral) it is likely that an image and metadata about that image which can be used to validate an individual's identity will be biometric information.

Biometric information used for "automated biometric verification" or "biometric identification" or "biometric templates" is considered *sensitive information* (as a technical term) for the purposes of the Privacy Act and the APPs. Images collected by FRT cameras are verified by software, in an automated fashion, and are used for either identification in the usual sense and/or form a biometric template, which is defined as a mathematical or digital representation of a person's biometry. This makes the image captured by an FRT system "sensitive information" under the Privacy Act and the APPs. This means biometric information, as a form of 'sensitive information' is subject to a higher level of privacy protection than other personal information.

For example, APP 3 provides an entity covered by the APP may only solicit and collect biometric information if the information is "reasonably necessary for one or more of the entity's functions or activities", if it has been collected by "lawful and fair means" and the person consents to the collection of that information (unless an exception applies).

2.3.2   Consent

The general principle is as biometric information is 'sensitive information', customers whose images are captured by FRT should give express consent to the collection of their image in advance. Customers should also be adequately informed before giving consent. To give fully informed consent, the customer would need to understand not just that their image is being collected, but also have full information about the use and disclosure of that image and any data connected to it.

Given biometric data is considered to be sensitive information for privacy law purposes, there are also safeguards around its use and disclosure following collection. APP 6 requires the data acquired by FRT only be used for the primary purpose of installation – that is, if FRT is installed to aid in exclusions as its primary purpose, the data cannot be used for marketing purposes unless consents are obtained. If a venue decides to use its FRT system to amass data for marketing, then it is likely to have to engage in much more extensive consent collection than is currently the case.

---

[7] White 2015 "Error Rates"
[8] 2020 Dunn et al UNSW "Face Test: a screening tool for super-recognizers", PLoS ONE
[9] (14 June 2022 Facial Recognition Technology and the law - HWL Ebsworth Lawyers)

The issue of consent, exemptions to the need to obtain consent, and the ways in which FRT data in particular can be used and disclosed is currently being considered by regulators. This includes the circumstances in which FRT data can be shared with the police[10]. Only recently, Adelaide City Council has halted sharing data with the Police from its council CCTV system until privacy concerns are addressed[11].

The Australian Information Commissioner in 2021 considered cases where facial images or FRT is involved[12].

More recently, CHOICE referred Bunnings, Kmart and the Good Guys to the OAIC over their use of FRT[13]. These retailers have turned off their FRT systems while these privacy related investigations are underway. All stores had small print signage near the front door explaining there was 24-hour CCTV coverage including FRT. In a statement, Bunnings said they used their system to undertake a one-to-many match against their own data base of customers who had been excluded due to "incidents of concern" in their outlets. The Good Guys said their use was ""strictly for the purposes of security and theft prevention and managing/improving customer experience at our stores"[14].

It is this last use which most concerns Wesley Mission – managing or improving customer 'experience' is not related to enforcing self-exclusion or stopping money-laundering. It could be a marketing exercise, which should require full, informed consent by all customers.

2.3.3   Exemptions

There are some reasonable exceptions to requiring consent from the subject when capturing images. In the context of pub and club gambling, this would include where there is reason to believe unlawful activity or serious misconduct, such as money-laundering, is taking place. In certain circumstances where the Police believe unlawful activity may be occurring, they may collect sensitive information without obtaining consent. However, and this will depend on the existing legislation in NSW, recording biometric information about a person because they "might" do something in the future is not necessarily a reason to be exempt from consent requirements[15].

Wesley Mission strongly believes a person who has taken out a self-exclusion deed and then subsequently enters a venue from which they have excluded themselves, should not be treated as if they are engaged in unlawful activity or misconduct. Use of the FRT system to enforce exclusion does not exempt venues from the obligation to obtain consent from all customers.

Wesley Mission also argues implied consent still requires both a person is adequately informed about not only the collection of their biometric data, but also the uses to which it will be put. It is also not true consent if the person has little reasonable choice other than to move to an area under FRT surveillance.

---

[10] Nowra Council sharing CCTV footage with Nowra Police: SF v Shoalhaven City Council [2013] NSWADT 94 before S Montgomery.

[11] 10 Nov 2021 Facial recognition technology put on hold in Adelaide amidst privacy concerns - ABC News

[12] Commissioner initiated investigation in to Clearview AI, Inc (Privacy) [2021] AICmr 54 (14 October 2021) link - use of facial images collected from social media; Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021) link - use of FRT of customers participating in an in-store survey

[13] 29 Sept 2022 CHOICE raises concern over Bunnings, Kmart and the Good Guys use of facial recognition technology - ABC News

[14] 15 June 2022 Bunnings, Kmart and The Good Guys using facial recognition technology to crack down on theft, Choice says | Facial recognition | The Guardian
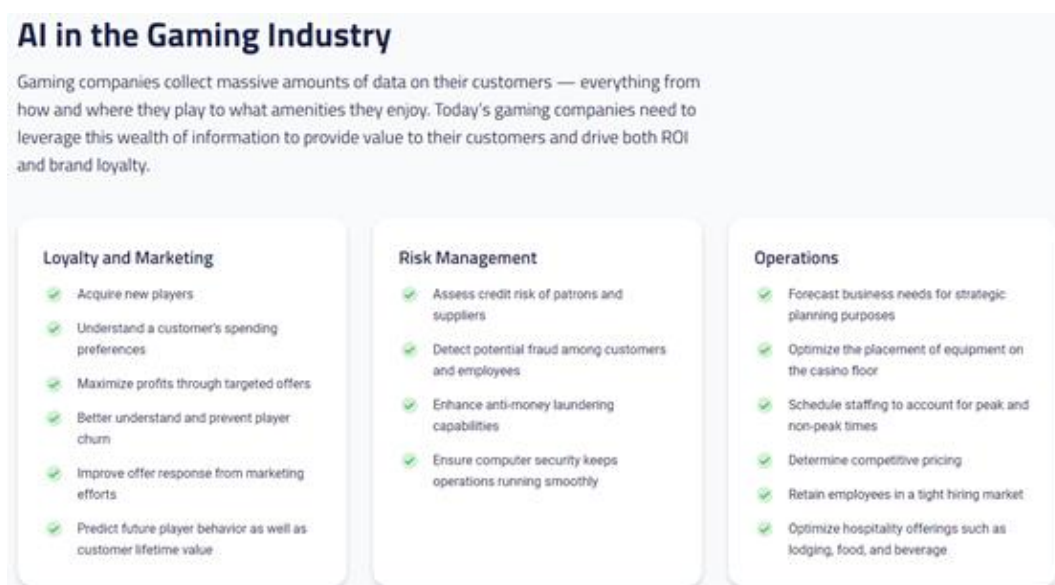
[15] **Caselaw relevant to the SA Surveillance Devices Act:** *Nanosecond Corporation Pty Ltd v Glen Carron Pty Ltd (2018) 132 SASR 63* (Nanosecond)

If FRT is to be used to counter money laundering, more detailed information about the mechanism must be made publicly available. If it involves a live feed to the Police, as in cases of Council CCTV, this should trigger public discussion and consultation before any legislative changes. The impact of the NSW *Surveillance Devices Act* would also need to be considered.

Wesley Mission argues a mandatory harm prevention cashless system would achieve the same effect, but without breaches of privacy. We have outlined our suggested design features for this system in this discussion paper.

2.4 How it is used in the casino gambling industry

Casinos employ significant levels of surveillance and data collection in order to monitor staff, legitimately guard against cheating and to learn about and influence what their customers do. This system benefits from two modern phenomenon - 'surveillance realism' and 'digital resignation' - where people assume corporations and/or governments use technology to gather data about them in ways which are ubiquitous and impossible to avoid[16].

AI in the Gaming Industry

Gaming companies collect massive amounts of data on their customers — everything from how and where they play to what amenities they enjoy. Today's gaming companies need to leverage this wealth of information to provide value to their customers and drive both ROI and brand loyalty.

Loyalty and Marketing	Risk Management	Operations
✓ Acquire new players	✓ Assess credit risk of patrons and suppliers	✓ Forecast business needs for strategic planning purposes
✓ Understand a customer's spending preferences	✓ Detect potential fraud among customers and employees	✓ Optimize the placement of equipment on the casino floor
✓ Maximize profits through targeted offers	✓ Enhance anti-money laundering capabilities	✓ Schedule staffing to account for peak and non-peak times
✓ Better understand and prevent player churn	✓ Ensure computer security keeps operations running smoothly	✓ Determine competitive pricing
✓ Improve offer response from marketing efforts		✓ Retain employees in a tight hiring market
✓ Predict future player behavior as well as customer lifetime value		✓ Optimize hospitality offerings such as lodging, food, and beverage

Industry trade papers are clear that actions to prevent churn (players leaving a game or even the casino) and to "improve offer responses" or gambling more, are some of the key uses of AI[17].

Naturally, casinos and gambling machine operators do not make information about the integration of FRT into their systems easily available, and in part this is due to the legitimate use of surveillance to guard against cheating and theft. However, using trade announcements, some concerning innovations can be verified. Konami is a major manufacturer of electronic gambling machines. They have integrated FRT into individual machines, rolling this out in Las Vegas since 2019[18]. Patrons must first explicitly agree to register their photo, and contact details, with the casino using this system, although it is presented as a system to guard against machine tampering or to detect people on exclusion registers. To identify people who are tampering with a machine, however, the AI software associated with the FRT must learn the normal behaviour of a gambler, in order to determine unusual behaviour. The system could also be programmed to detect boredom or some other negative (from the perspective of the casino)

---

[16] Dencik, L. & Cable, J. 2017 "The advent of surveillance realism: public opinion and activist responses to the Snowden Leaks"; Selwyn, N., O'Neill, C., Smith, G., Andrejevic, M. & Gu, X. 2021 "A necessary evil?"; Draper, N. A., & Turow, J. 2019 "The corporate cultivation of digital resignation"
[17] Machine Learning and AI in Casinos and Gaming | DataRobot
[18] Major casino game company will add facial recognition, H. Samsel, Security Today, 29 October 2019

emotion and allow messaging to be sent to the machine or the gambler's phone to encourage them to continue gambling[19].

This interaction is part of the Konami system, which now includes machines that greet customers who login on the machine, and can personalise messages based on historical data and loyalty indicators[20]. Similar interactions are being included in table games in casinos, allowing the identification of regular customers linked to their known food and beverage preferences, so that gamblers need only raise a hand to have their favourite drink delivered and automatically charged to their tab[21]. Digitally enabled gambling chips feed into this system[22].

Star Casino in Sydney introduced FRT in 2019[23]. The casino detected a croupier stealing chips using their standard CCTV system, but argued they needed to upgrade their system, which integrates with motion sensors, ID scanners, number plate recognition software, mobile phone and other ambient surveillance and AI systems operating in the complex, including their non-casino venues and hotels.

2.5   How it is used in NSW pubs and clubs

NSW pubs and clubs have changed their attitude to FRT significantly since September 2020. When then-Gaming Minister Victor Dominello announced a consultation draft of the *Gambling Harm Minimisation Bill,* which focussed on self and third-party exclusion, the industry responded negatively to the mention of FRT as one of the possible technologies they could employ. The industry announced they were "deeply concerned by the potential impact and cost of the draft legislative changes" and "the government's intended implementation would create unnecessary red tape and place a significant compliance burden on venues."[24]

The industry also warned they could not afford to implement FRT and that "we [the AHA] don't believe our patrons want to be monitored through facial recognition each and every time they catch up with mates at the pub."[25]

The then-Gaming Minister's suggested alternative, a cashless card, received similar negative responses from the industry and its supporters[26]

In October 2022, ClubsNSW and the AHA announced they would be rolling out their own FRT system to every club and pub in NSW. We are not aware of any public and independent evaluation, nor does it appear to be adequately covered by legislation. To support the roll-out, the Minister for Hospitality and Racing, Kevin Anderson, introduced a very broad but ill-defined governance framework in a Bill to modify the *Registered Clubs Act*, but which did not apply to pubs. Minister Anderson stated, in introducing the Bill, FRT "could only be used for gambling harm minimisation or to identify people suspected of committing a serious offence such as money laundering". But there were no such restrictions in the Bill, which referred to guidelines which do not exist[27]. In response to proposed cross-bench amendments, the Bill was withdrawn[28].

---

[19] Casino Marketing: The Leap from Email to SMS | mobileStorm
[20] Facial recognition and AI coming to Vegas casinos- Associated Press, 4-5 January 2020
[21] Liu, M.T., Dong, S. & Zhu, M. "The application of digital technology in gambling industry",
[22] Macau casinos utilizing AI, facial recognition – Asia Times
[23] Casino Upgrades Surveillance, Casino News Daily 11/3/2019
[24] 25 Sept 2020 Pokies venues could ban problem gamblers reported by family members under proposed NSW legislation - ABC News
[25] Cash ban as gambling card to overhaul $6b pokie industry in NSW (smh.com.au)
[26] 4 Oct 2020 Push for cashless poker machines in NSW catches clubs by surprise (smh.com.au);Early opposition from ALP, SFF and industry to card: 7 Oct 2020 NSW pokies gambling card could devastate pubs, clubs: Michael Daley (smh.com.au)
[27] Business racing to use facial recognition technology, raising concerns the law is too slow to catch up | Privacy | The Guardian 23 Oct 2022
[28] 1 Nov 2022 Gambling: NSW government to abandon clubs reform bill after crime commission report (smh.com.au)

At the time, ClubsNSW reported nearly 100 clubs already had FRT in operation. The then-CEO of ClubsNSW, Josh Landis, said it had proven effective in identifying and stopping self-excluded patrons from using gambling machines[29]. We are not aware of any evidence or data presented to demonstrate these claims of effectiveness. Trade papers also reported the system had been trialled in six pubs, although again, no evidence of the nature of the trial or its evaluation is publicly available[30].

Statements from ClubsNSW and the AHA provide conflicting information on the use of the system. While it is clear the FRT system will be linked in some way to the existing ClubsNSW Multivenue Self-Exclusion system, that exclusion register does not currently cover every gambling club or pub in NSW. In an early example of mission creep, pubs have suggested they may use FRT to track people excluded from venues for disorderly conduct[31].

2.5.1 What we know of the way FRT is marketed to clubs and pubs

FRT and surveillance tech companies often publish advertorials in The Drop, a key industry e-Magazine.

When urging venues to better operate AML/CTF programs, which of course is necessary, they promote FRT because it would allow suspicious behaviour to be assessed – which can only be done if the footage is kept and analysed. They suggest "you can keep track of patrons who frequent your venue and identify which of them could potentially be engaging in illegal activities"[32]. It is no doubt true keeping accurate records which might later be used by AUSTRAC would be in the public interest, but it is unclear to Wesley Mission how this could be done by staff who are not properly trained within the framework of the Privacy Act or APPs, nor is it clear venue staff have a role to play in law enforcement by attempting to predict who might be about to commit a crime.

Advertorials also claim FRT assists venues to "identify and remove persons who have been suspended, banned or self-excluded from their premises, so there is a lawful basis for such an implementation. **In addition, the collection of faces is reasonably necessary for venues to perform everyday activities and operations** (our emphasis).[33]" Wesley Mission suggests this interpretation of the APP might need testing against the Privacy Act and APPs, particularly around the need to collect biometric data for "everyday activities" especially if those everyday activities are marketing related.

Despite the claims of suppliers of FRT and other devices, Wesley Mission continues to have concerns about how the *NSW Surveillance Devices Act (SDA) 2007* interacts with various gaming machine, liquor licensing and casino laws to allow the use of surveillance devices. Given installing FRT can cost a venue as little as $80 a month, this technology is within the reach of every venue and the legal basis must be better defined[34].

Clubs giving endorsements to Exact Technologies as suppliers of surveillance systems include Panthers Entertainment Group, the Canterbury League Club, the Campbelltown Catholic Club, Wenty Leagues, Liverpool Catholic Club, Castle Hill RSL, and The Star[35].

Most concerningly, FRT suppliers, although using wording in their advertorials matching the requirements of the APPs, such as "the singular purpose is to prevent breaches of self-exclusion

---

[29] 19 Oct 2022 NSW clubs to introduce facial recognition technology in bid to stop problem gambling | 7NEWS

[30] Clubs and pubs join forces on facial recognition - Club Management 19 Oct 2022

[31] 28 Oct 2022 ClubsNSW suggests use of facial recognition could go beyond identifying problem gamblers | Gambling | The Guardian

[32] Using facial recognition for your AML/CTF programs - The Drop

[33] May 2021 Facial recognition for clubs & pubs: Your Top 10 Questions answered - The Drop

[34] May 2021 Facial recognition for clubs & pubs: Your Top 10 Questions answered - The Drop

[35] Projects – Exact Technologies – accessed 13/3/2023

agreements"[36], also point out to venue management that FRT can help with "enhanced customer service – especially your VIP member programs"[37].

Wesley Mission is concerned there is no independent oversight or evaluation of the industry developed FRT system. There does not appear to be a legislative framework requiring, for example, the Privacy Commissioner to be satisfied the protocols in place for collection, analysis, storage and deletion would protect privacy and ensure the system is used for the singular purpose of excluding people already on a register in the same way that the South Australia system requires the Commissioner for Liquor and Gaming to approve systems.

2.6 How it is used in other Australian States

2.6.1 South Australia

In 2020, SA announced FRT must be introduced if a pub or club has more than 30 machines and any of them have note acceptors. The casino also must use FRT. The industry in SA moved quickly to implement both technologies. Venues which are not legally obliged have also installed FRT. Detailed guidelines have been published which restrict the use of FRT to exclusion purposes only[38].

Key points include:

- Systems and system providers must be approved by the Liquor and Gaming Commissioner before deployment
- Systems must be able to communicate with the exclusion register (barring data in SA terminology) but cannot access that system until proof of engagement with a gambling venue is provided
- Data cannot be stored or exported offshore
- Data cannot be used in other applications
- Data from the FRT or exclusion register cannot be shared with anyone other than the gambling venue which engages the systems provider
- The Commissioner must be notified of the staff at a venue who will access the system
- Any device which receives alerts from the system about patrons in a venue must be at the venue
- Devices which receive alerts must be positioned so that the public cannot access them or see the screen

Section 5.8 of the guidelines states

"While the use of facial recognition technology is a mandatory requirement for certain licence holders, it is not meant to be a total replacement for the management of barred persons, but rather a valuable tool to assist licensees with their responsible gambling obligations."

2.6.2 Tasmania

The Tasmanian government announced in September 2022 it would accept the recommendation of its Liquor and Gaming Commission and introduce a mandatory cashless

---

[36] Facial recognition – Privacy, data protection & human rights - The Drop
[37] Facial recognition – making it work with your systems for your members - The Drop
[38] SA Consumer and Business Services Gambling Administration Guidelines: FRT System providers July 2021

card rather than FRT[39]. The Commission had undertaken an inquiry to investigate the extent to which technological solutions could minimise gambling harm[40].

The Commissioner's recommendations were based on

- FRT being a tool for venues to manage for the small number of people who, having self-excluded, then enter venues
- FRT "does not have broad scope as a tool for minimising harm from gambling, rather it could be considered an additional tool to mitigate already existing harm."
- FRT does not prevent harm for people who have not self-excluded

If implemented, the Tasmanian Commissioner recommended the SA model should be followed, preceded by trials and extensive staff training.

Tasmania has a planned timeframe of implementation for their Player Card Gaming system by the end of 2024, assisted by the fact Tasmania only has 2,323 poker machines in pubs and clubs[41]. Their casinos already operate cashless gambling.

2.7   Other evidence around FRT in gambling harm contexts

The National Strategy to Reduce Gambling Harms in Great Britain commissioned an extensive review of prevention and education measures[42]. FRT was mentioned once, as a possible way venues could help enforce self-exclusion. It was not included as a harm minimisation tool.

2.8   International concerns around FRT in public and "third" spaces[43]

The UK has a large, well-known CCTV system being converted to an FRT system. UK civil liberties groups are concerned about the use of the system for policing and other purposes. As in Australia, the legal basis for the use of data derived from FRT, and the nature of any consent in the system, is tenuous.

In the Face Off (2018) report, it was noted the UK Metropolitan Police had a 2% accuracy rate for identification, although none of the people "identified" were in fact wanted criminals[44]. 102 innocent people were incorrectly identified. South Wales police had a 9% accuracy rate but stored the biometric data on 2,451 incorrectly identified people for 12 months.

The Urban Agenda for the EU released a report noting the legislative weaknesses in many European countries around the deployment of FRT in public places[45]. As in other reports, consideration was given to the necessity of gathering the information, the lawfulness of doing so and the issue of proportionality. That is, deciding whether the public interest in gathering data outweighs the presumption of privacy in public places. The report recommended more specific legislation around data protection, and to clarify the existing exemptions from EU privacy laws

---

[39] Announcement by Premier Jeremy Rockliff and Deputy Premier Michael Ferguson: Nation-leading card-based gaming with pre-commitment a first in Tasmania - Premier of Tasmania
[40] Tasmanian Liquor and Gaming Commission report to the Treasurer: TLGC Report to Treasurer - Investigation of harm minimisation technologies.PDF (treasury.tas.gov.au)
[41] Tasmanian Gaming and wagering industry data: Gaming and Wagering Industry Data | Treasury and Finance Tasmania
[42] Hilbrecht, M. (Ed.). (2021). Prevention and Education Evidence Review
[43] As just one example of the global discussion around the potential for serious misuse of FRT, this international conference held in September 2022 at University of NSW: FACIAL RECOGNITION IN THE MODERN STATE | UNSW Allens Hub; see also the UK Centre of Data Ethics and Innovation Snapshot Paper – Facial Recognition Technology, 2020 Snapshot Paper - Facial Recognition Technology - GOV.UK (www.gov.uk)
[44] Big Brother Watch: Defending Civil Liberties, Protecting Privacy
[45] Lequesne Roth, C. 2021 New Surveillance Technologies in Public Spaces, Urban Agenda for the EU

that are being used to justify CCTV. In particular, the report recommended real-time FRT be prohibited due to the potential use of profiling on discriminatory grounds.

In 2021 Amnesty International launched a global campaign against mass surveillance including FRT[46]. Although the context of these bans is different from pub and club gambling – tracking of protests or the targeting of individuals by law enforcement agencies – FRT in community venues acts to normalise the use of biometric data collection and increase the sense of "surveillance resignation".

2.9   Risks

If FRT is introduced, a key concern is where data is stored and how long it is kept. This exposure to the risk of hacking was highlighted in 2022 with two major data leaks. Customers of Optus were surprised to learn the amount of data kept by the company on file after identity had been verified[47]. Similarly, the Medibank leak exposed poor data management practices[48]. Other similar issues with data management are inevitable when personal data is stored.

An anonymous submission to the Crown Casino (Melbourne) Royal Commission related to the potentially illegal sharing of personal data about a customer by Crown with other casinos through the "Casino Surveillance Network"[49]. The person concerned has lodged a complaint in Queensland around the legitimacy of their exclusion from a non-Crown casino.

Casinos in the US often have systems which the manufacturers claim are NDAA (*National Defence Authorization Act*) compliant[50]. The NDAA prohibits the use of surveillance systems from some (mainly Chinese) manufacturers due to risks of the government of the PRC requesting the data, as the discussion around Huawei has shown. The US ban extends to components manufactured by the listed companies. The ban technically only covers federal government agencies, or federal government grants (i.e. they cannot provide funds to a third party to purchase surveillance if the technology comes from companies on the banned list).

It is relevant because in several US states, surveillance is a regulatory requirement. It may become relevant in Australia if the federal government makes security decisions about providers of technology.

---

[46] Amnesty International and more than 170 organisations call for a ban on biometric surveillance - Amnesty International

[47] Optus data breach: everything we know so far about what happened | Optus | The Guardian

[48] More Medibank customer data released onto dark web. Has everything now been released? - ABC News

[49] Submission 36 Anonymous.pdf (rccol.vic.gov.au)

[50] What is NDAA Compliance and Does My Business Require It? (2krew.com)

3   References

Albiero, V. et al 2020 Analysis of Gender Inequality in Face Recognition Accuracy, Proceedings of the IEEEE/CVF Winter Conference on Applications of Computer Vison (WACV) 2020.

Davis, N., Perry, L. and Santow, E. 2022 Facial Recognition Technology: Towards a model law; Human Technology Institute, The University of Technology, Sydney.

Dencik, L. & Cable, J. 2017, The advent of surveillance realism: public opinion and activist responses to the Snowden Leaks, International Journal of Communications,11, 763-781.

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. New Media & Society, 21(8), 1824–1839. https://doi.org/10.1177/1461444819833331

Dunn, J. D. et al 2020 UNSW Race Test: A screening tool for super-recognizers, PLoS ONE 15/11 eo241747.

Face Off: the lawless growth of facial recognition in UK policing, May 2018, Big Brother Watch.

Hilbrecht, M. (Ed.). (2021). Prevention and Education Evidence Review: Gambling-Related Harm. Report prepared in support of the National Strategy to Reduce Gambling Harms in Great Britain. Greo: Guelph, Canada. https://doi. org/10.33684/2021.006

Human Rights and Technology Report, AHRC, 2021 Recommendations 19-21: Facial recognition & biometric tech | Human Rights and Technology.

Johnson, T. et al 2022 Facial recognition systems in policing and racial disparities in arrests, Government Information Quarterly, 39/4, 101753.

Lequesne Roth, C. 2021 New Surveillance Technologies in Public Spaces: Challenges and Perspectives for European Law at the Example of Facial Recognition, Urban Agenda for the EU/Security in Public Spaces.

Liu, M.T., Dong, S. & Zhu, M. "The application of digital technology in gambling industry", Asia Pacific Journal of Marketing and Logistics, 33/7, 1685-1705.

Najibi, A. 2020 Racial Discriminiation in Face Recognition Technology, Blog Science Policy, Harvard University Racial Discrimination in Face Recognition Technology - Science in the News (harvard.edu).

Selwyn, N., O'Neill, C., Smith, G., Andrejevic, M. & Gu, X. 2021 "A necessary evil? The rise of online exam proctoring in Australian universities", Media International Australia, 2021.

White, D. et al 2015 Error Rates in Users of Automatic Face Recognition Software, PLoS ONE 10/10.

Get involved

To volunteer, donate or leave a gift in your Will
visit wesleymission.org.au

Wesley Mission
220 Pitt Street, Sydney NSW 2000
PO Box A5555, Sydney South NSW 1235
(02) 9263 5555
communications@wesleymission.org.au
wesleymission.org.au

CEO and Superintendent: Rev Stu Cameron
ABN 42 164 655 145   Wesley Mission is a part of the Uniting Church in Australia.

Do all the good you can because every life matters