

28 September 2023

Russell Hooper
Director, Policy – Gaming and Liquor
Integrity, Regulation and Legal Services
Department of Justice and Community Safety

By email only: gamingandliquor@justice.vic.gov.au

Submission in response to the proposed Casino Control Regulations 2023 and Regulatory Impact Statement

Thank you for the opportunity to comment on the proposed Casino Control Regulations 2023 (**proposed Regulations**) and associated Regulatory Impact Statement (**RIS**).

The Office of the Victorian Information Commissioner (**OVIC**) has combined oversight of freedom of information, privacy and information security, administering both the *Freedom of Information Act 1982* (Vic) and the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**). OVIC has an interest in this consultation as it relates to collecting, storing, using and disclosing personal information of individuals.

This submission provides comments in relation to specific areas of the proposed Regulations and RIS that relate to information privacy and security. The comments reflect OVIC's expectations of Victorian public sector organisations regulated under the PDP Act. However, OVIC notes that the Federal *Privacy Act 1988* (Cth) (**Federal Privacy Act**) will apply to the casino operator's handling of personal information.

Identification

Method for identity verification

OVIC notes regulations are required to prescribe what the casino operator must do to verify a person's identity to give effect to the CLARC Act reforms. These reforms require the casino operator to verify a person's identity before issuing a player card or paying out winnings or accumulated credits.

Options 1 and 2 outline different levels of identity verification, built on the reference case. In addition, option 2 would require the casino operator to record details of one identification document that must be used when collecting winnings above \$1000. This would require the casino operator to record the specific details of the identification presented upon signing up for a player card, which would need to be updated if that document expired.

OFFICIAL

From a privacy perspective, Option 1 (which is the option set out in the proposed regulations) is preferred, as it involves the collection and use of fewer identification documents compared to Option 2.

Option 1 involves the collection of certain personal information (name, residential address, date of birth), and the requirement to verify this information by sighting, in person, an Australian Government Entity photo identification or an international passport and one form of photographic identification (these may be the same documents).¹ The casino operator must take all reasonable steps to confirm the validity of the document/s presented.

Option 2 would require individuals' identities to be verified by a 100-point ID check, and for details to be recorded of one of the forms of identification to be used when collecting winnings over \$1,000. If 100-points of ID is not required to verify identity, and given that the RIS notes that the recording of details of an identity document will have minimal impact on preventing money laundering, then this is likely to result in the overcollection of personal information and increases the risk of scope creep (using information collected for one purpose for a different and unrelated purpose). It also increases the administrative burden on the casino operator to protect more identity documents.

OVIC notes the method for verifying identity should, to the extent practicable:

- collect and store the minimum amount of personal information;
- take a risk-based approach to identity verification, determining the level of assurance of identity required for the relevant activity;
- be able to be audited by an external party such as the Victorian Gambling and Casino Control Commission (VGCCC);
- be flexible and able to adapt to new technologies or methods for identity verification; and
- be consistent with other Australian frameworks or guidelines for identity verification.²

OVIC notes that Option 1 and proposed regulation 23 would require the casino operator to have an identity verification policy, fulfilling the policy objective. This policy would outline how it will collect and validate personal information for identity verification purposes and must be approved by the Victorian Gambling and Casino Control Commission (VGCCC). This would allow the VGCCC to help ensure privacy risks are considered and addressed.

Facial recognition technology

OVIC is concerned that the proposed Regulations mention 'facial recognition technology' (FRT) under subregulation 25(5). This suggests the casino operator may use FRT for identity verification purposes.

¹ For example, regulation 12 of the proposed Regulations in relation to identity verification for issue of player cards.

² These principles are consistent with the guiding principles in section 42 of the *Service Victoria Act 2018* (Vic) for making and using the Service Victoria [Identity Verification Standards](#).

OFFICIAL

OVIC strongly suggests that FRT should not be used to verify player identity, and that the reference to FRT be removed from the proposed Regulations. Given the VGCCC will be required to approve the casino operator's identity verification policy, OVIC suggests that using FRT should not be considered 'reasonable steps the operator will take to verify a person's identity'.³

The biometric information collected by FRT is a form of 'sensitive information' under the Federal Privacy Act. This means organisations who must comply with the APPs can only collect biometric information in limited ways (with the applicant's consent and if the information is reasonably necessary for one or more of the entity's functions or activities).⁴

While OVIC understands the use of FRT could be considered reasonably necessary by some people in order for the casino operator to verify player identity, there will likely be issues around consent. For consent to be valid, the individual must have the capacity to give consent, and the consent must be voluntary, informed, specific and current. By allowing the casino operator to use FRT to verify player identity, the player has no real choice but to consent to the collection of their biometric information if they want to attend the casino.

The use of FRT by the casino operator could result in the overcollection of personal information and create a risk of scope creep, where the FRT may subsequently be used for purposes beyond player identity verification. For example, tracking individuals' behaviour by monitoring and checking biometric information for surveillance that is not proportionate to maintaining security at the casino.⁵

FRT may also inadvertently identify individuals with assumed identities such as undercover law enforcement officers, VGCCC staff, or victim survivors of family violence. Identifying these individuals would impact the VGCCC's ability to effectively regulate the casino operator and may have an impact on the safety and security of police or other individuals.

In addition to these privacy issues, OVIC notes that FRT has limited utility because:

- it can only match a person's face to the image on their identity document;
- it will not always be able to correctly match a person's face to their identity document, particularly if there are factors such as poor lighting present;
- it can be less effective on different ethnic groups;
- it may inadvertently identify undercover officers or the VGCCC staff, thereby impacting their ability to effectively regulate the casino operator; and

³ See regulation 23 of the proposed Regulations.

⁴ The *Privacy Act 1988* (Cth) applies to the casino operator because it is a body corporate with an annual turnover of more than \$3,000,000.00 (section 6C and section 6D of the *Privacy Act 1988* (Cth)).

⁵ For example, the Office of the Australian Information Commissioner found the collection of facial images by 7-Eleven while surveying customers about their in-store experience interfered with customer's privacy by collecting sensitive biometric information that was not reasonably necessary for its functions and without adequate notice or consent.

- it has been shown to have limited benefit towards reducing gambling harm.⁶

Carded play

Player cards

OVIC understands the proposed Regulations must require player cards to be linked to the individual's identity and collect the minimum information specified in the reference case for carded play.⁷

OVIC is concerned that Options 1 and 2 for carded play would require an image of the individual to be included on their physical player card and stored electronically to allow casino staff to ensure the player card is only used by the individual to which it is linked. OVIC understands the purpose of this but recommends that player cards do not include the individual's photo on the physical card because, if lost, any person who finds the player card would be able to identify the player and their status as a gambler at the casino due the image on the card.

Furthermore, OVIC notes that it may not be necessary to include a photo on the physical card given the card would be linked with the player's individual account. This means the casino operator could refer to the electronic image of the player when verifying that the card is being used by its registered player.

Information and security

A large amount of transactional data will be collected through the player cards. OVIC is concerned that this would effectively create a honeypot of information about individuals in a sensitive setting, linked to the personal information on their player account.

OVIC notes there must be a high level of security over the data in the player account, the player card, and any database sitting behind them.

As Options 1 and 2 for carded play would require the amount of loyalty credits redeemed through play at table games and gaming machines to be collected through player cards, there is likely to be some interaction between the casino operator's loyalty scheme and player cards. OVIC is concerned the casino operator may use the existing loyalty scheme's system for the collection and use of player information for carded play. This creates a risk of scope creep, where the information collected for carded play may subsequently be used for the loyalty scheme without the casino operator obtaining meaningful consent from the individual. In addition, loyalty schemes are often run through third party marketing software. The use of the loyalty scheme's database for carded play may risk the information collected for carded play being inappropriately disclosed to third parties. Disclosing player card information to third parties may also increase the risk of data breaches.

⁶ For example, in the Tasmanian Liquor and Gaming Commission's report to the Treasurer on their investigation of harm minimisation technologies, they recommended against FRT because it was not effective for the wider prevention of harm in gaming venues in Tasmania, but rather effective only for a small subset of people that self-exclude from gaming venues and only if privacy issues could also be addressed.

⁷ See the reference case for carded play at 4.5.2 on page 39 of the Regulatory Impact Statement.

OFFICIAL

OVIC recommends that the proposed Regulations require the casino operator to use separate databases for carded play and the loyalty scheme, to mitigate the risks of scope creep and disclosure of player information to third parties without meaningful consent.

OVIC also recommends that player information should be regularly deleted when no longer needed and if a player requests that their account is deleted (subject to any other obligations to retain data). Player information that is not regularly deleted when no longer necessary, or held for long periods of time, increases the risk of a data breach. This may be unintentional (for example, a data leak) or intentional (for example, the casino operator is subject to a hack due to the data they hold). Deleting personal information when it is no longer required is consistent with privacy law.⁸

Collection notice requirements

OVIC is pleased to see the proposed Regulations will require the casino operator to provide notice of certain information to individuals before collecting their information to verify their identity.⁹ The proposed Regulations would also require the casino operator to provide this information in other ways, such as ensuring the notice is available electronically, in a range of languages and in an Easy Read format.¹⁰

OVIC considers that these additional requirements will assist individuals to make an informed decision about whether they wish to provide their personal information to the casino operator attend the casino.

Information protection offences

OVIC is pleased to see the proposed Regulations will introduce an offence for the access, use or disclosure of identity verification information for non-regulatory purposes.¹¹ The RIS notes non-regulatory purposes includes targeted advertising, direct marketing, and loyalty schemes.¹² This helps to enhance privacy protections by prohibiting the access, use or disclosure of personal information collected for identity verification purposes for secondary unrelated purposes.

If you would like to discuss this submission, please do not hesitate to contact me directly or my colleague Jenna Daniel, Senior Policy Officer at jenna.daniel@ovic.vic.gov.au.

Yours Sincerely



Rachel Dixon

Acting Information Commissioner

⁸ For example, see Australian Privacy Principle 11.2 in the Federal Privacy Act and Information Privacy Principle 4.2 in the PDP Act.

⁹ See regulation 25(3) of the proposed Regulations.

¹⁰ See regulation 25(4) of the proposed Regulations.

¹¹ See regulation 25 of the proposed Regulations.

¹² On page 77.