

Ensuring Compliance with the **Australian Privacy Principles:**

Responsible Use of Facial Recognition Technology in Hotels & Clubs



Purposes of FRT?

Regulatory goals under consideration across Australia for FRT:

- ✓ Self-Exclusion
- ✓ Third-party Exclusion
- ✓ Anti-Money Laundering
- ✓ Anonymous Harm minimisation



Computer Vision is the specialist field interprets images and video for use as computer input.

Executive Summary

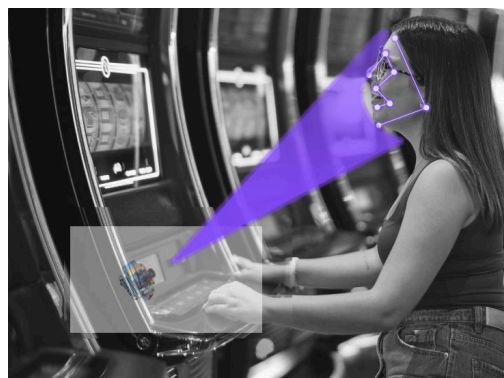
Face Recognition technology (FRT) holds promise for public safety and operational efficiency. However, its deployment—particularly in sensitive environments such as hotels, clubs, and gaming venues—requires stringent adherence to privacy obligations. This whitepaper outlines how Xailient ensures full compliance with the Australian Privacy Principles (APPs) under the Privacy Acts.

Through a privacy-by-design approach, privacy impact assessments, ethical AI governance, and secure, transparent data handling, Xailient's solutions are architected to uphold the rights of individuals while providing high-value operational capabilities.

Monitoring games, rather than entire venues, constrains the scope of FRT systems to players at the time of play.

State of the Art - FRT inside Every Game

Recent advancements in technology make it practical to install FRT cameras in each Gaming Machine and to recognize customers in real-time. This provides the opportunity for a reduced scope of monitoring, enhancing the general interest in privacy because cameras are only monitoring players seated at games, not all customers.



Low-cost retrofit cameras with on-board FRT are being deployed into EGM globally.

Deidentified Face Recognition Technology (FRT) can preserve the privacy of gaming patrons, enabling anonymized tracking until regulatory thresholds justify action.

About Xailient

Xailient is an Australian provider of FRT headquartered in NSW. Xailient exports our technology globally and has customers in residential security, corporate enterprises, and casino gaming. We engage closely with outside thought leaders in “Responsible AI” to guide our work and contribute our voice to this important global trend. Our mission is to make these technologies safe, for individuals, organizations, and the public, and our team is dedicated to advancing cutting-edge technology that embodies industry-leading standards in AI supervision and privacy compliance.

Mission Driven Partnership to Reduce Harm

Xailient is a global leader in making accurate, real-time FRT low-cost and privacy-safe. Some of our customers use their face to unlock their homes. Through integration into Konami’s SYNKROS™ we have reversed this process to lock Game Machines digitally.

This partnership opens a more targeted solution to the objectives of self-exclusion, third-party exclusion, harm minimisation, and anti-money laundering. Xailient’s privacy-safe FRT limits the scope of data collection and AI processing, protecting the public. Konami’s SYNKROS provides a wide array of alerts and automated actions, providing regulators with fine-grained controls. Together, these provide the most effective and least intrusive option for safely and securely monitoring Casinos, Hotels and Clubs.

This solution can operate automatically, or by notifying venue staff, or both.



Purpose is a critical element of modern privacy governance. Former practices of vacuuming up data under one justification and reusing that data in an unrelated purpose are no longer acceptable, and do not comply with the APPs.



Genuine Consent is an emerging global standard for individual consent. It requires the subject to be informed about, and to understand, the terms and purpose of their consent. Genuine Consent must be voluntary, specific, current, and revocable.

1. Introduction to the Australian Privacy Principles (APPs)

The 13 Australian Privacy Principles form the foundation of privacy law in Australia (see sidebar). While all apply, in practice the most relevant APPs for Face Recognition in hospitality venues include:

- APP 1: Open and transparent management of personal information
- APP 2: Anonymity and pseudonymity
- APP 3: Collection of solicited personal information
- APP 4: Collection of unsolicited personal information
- APP 5: Notification of data collection
- APP 6: Use and disclosure
- APP 8: Cross-border disclosure
- APP 11: Security of personal information
- APP 10, 12 & 13: Quality of, access to and correction of personal information

Balancing privacy and State and Federal Authorities' interests in data and data collection is incorporated into the APPs. Where possible, the Principles direct that the least invasive means be used to fulfil a regulatory purpose.

Furthermore, the Principles can and have been interpreted as requiring that organisations use the most privacy-preserving technology available – it is not acceptable to deploy obsolete technology when more privacy-safe techniques are on option. For example, techniques in encryption, de-identification and decentralisation can enhance solutions whilst delivering on the regulatory purpose. Xailient's technology incorporates the state-of-the-art to advance the privacy interest.

Hierarchy of Express & Implied Consent

One method to minimise the privacy impact is to restrict the FRT system scope such that it monitors only the Gaming Machines.

This provides policy makers with new choices to balance objectives and privacy. For example, a customer might be interpreted as providing implied consent to FRT checking if they sit at a Gaming Machine, and would only be recognised if they had previously given express consent for the purpose of self-exclusion.





As a result, the minimum number of persons are subject to FRT, and the FRT itself is minimised, whilst achieving the regulatory purpose.

Understanding the Australian Privacy Principles





The 13 Australian Privacy Principles form the foundation of privacy law in Australia. They regulate the collection, use, storage, and disclosure of personal information, including biometric data like face images. These fit into 4 broad categories:

AUSTRALIAN PRIVACY PRINCIPLES




THE COLLECTION, USE AND DISCLOSURE OF PERSONAL INFORMATION (APP 1,2,3,4,6)

 OPEN AND TRANSPARENT MANAGEMENT OF PERSONAL INFORMATION	This ensures entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date privacy policy
 COLLECTION OF SOLICITED PERSONAL INFORMATION	This ensures entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date privacy policy
 DEALING WITH UNSOLICITED PERSONAL INFORMATION	This ensures entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date privacy policy
 USE OR DISCLOSURE OF PERSONAL INFORMATION	This ensures entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date privacy policy



AN ORGANIZATION OR AGENCY'S GOVERNANCE AND ACCOUNTABILITY (APP 5,7,8,9)

 NOTIFICATION OF THE COLLECTION OF PERSONAL INFORMATION	Outlines when and in what circumstances an entity that collects personal information must notify an individual of certain matters
 DIRECT MARKETING	An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met
 CROSS BORDER DISCLOSURE OF PERSONAL INFORMATION	Outlines the steps an entity must take to protect personal information before it is disclosed overseas
 ADOPTION USE OR DISCLOSURE OF GOVERNMENT RELATED IDENTIFIERS	Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual

INTEGRITY AND CORRECTION OF PERSONAL INFORMATION (APP 2,10,11)

 ANONYMITY AND PSEUDONYMITY	Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.
 QUALITY OF PERSONAL INFORMATION	An entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.
 SECURITY OF PERSONAL INFORMATION	An entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorized access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.

THE RIGHTS OF INDIVIDUALS TO ACCESS THEIR PERSONAL INFORMATION (APP 12, 13)

 ACCESS TO PERSONAL INFORMATION	Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.
 CORRECTION OF PERSONAL INFORMATION	Outlines an entity's obligations in relation to correcting the personal information it holds about individuals.

PENALTIES FOR NON-COMPLIANCE:

Under the draft bill, the maximum penalty of \$2.1 million for serious or repeated breaches of privacy will increase to not more than the greater of \$10 million, or three times the value of any benefit obtained through the misuse of information, or 10 per cent of the entity's annual Australian turnover.

2. Xailient's Technology: Privacy-By-Design

Xailient's Face Recognition architecture was built with privacy as a first-order principle. This is evident in key fundamental design decisions:

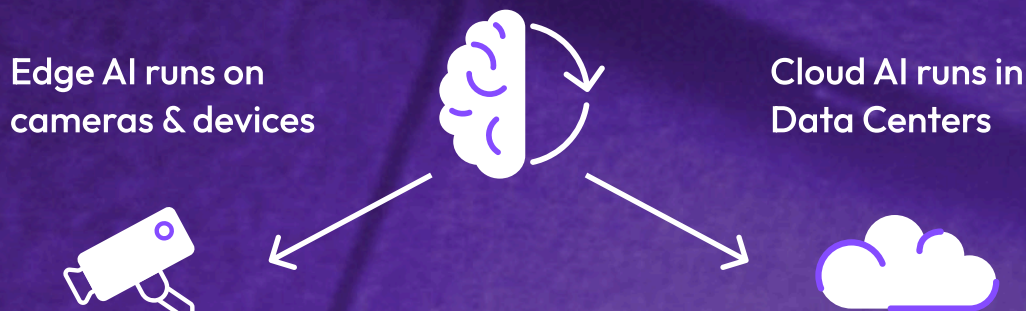
- Purpose Limitation: FRT is restricted to the purposes disclosed to the individual—typically patron self-exclusion enforcement. (APPs 3 & 6)
- Edge Processing: All face detection and recognition occur on local devices and is performed without collecting images, minimizing the scope of collection (in line with requirements of APP 3), preventing inadvertent collection of bystanders (APP 4), and recognition is restricted to matching against a pre-registered set of individuals.
- Pseudonymisation: Individuals are represented via deidentified digital tokens or pseudonyms (APP 2).
- No Image Retention: The system does not store facial images unless explicitly required for audit purposes or law enforcement cooperation, or as a result of an explicit self-exclusion registration (APPs 3 & 11).
- Consent-aware Operation: Use of the system is configurable to require informed, opt-in consent, aligned with APPs 3 & 5. This is supported by signage, public notices, and digital policy availability.
- Auditable and manageable: The system has secure methods for investigating reported errors and correcting or removing personal information. (APPs 10-13).

What is Edge AI?

Edge AI is the industry term for AI that processes data at the source, rather than in a centralized location. The term is contrasted with Cloud AI, which operates in data centers. Edge AI reduces the need to transmit data and wait for a response, leading to cost efficiencies, speed and reliability improvements, and gains in cybersecurity and data privacy.

Many jurisdictions have ruled that operating Edge AI does not constitute 'data collection' for legal purposes. This is significant for Computer Vision, because images and video can contain data that is subject to privacy regulations or other laws.

Edge AI analyzes data at the source, and can be configured to delete images in real-time. For example, Edge AI FRT can watch for excluded patrons and alert security staff when a known subject attempts entry, while all other patrons will be ignored and their images discarded.



What is Computer Vision?

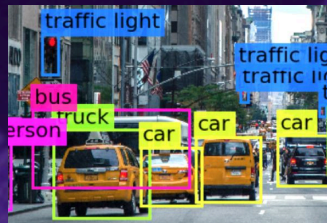
Computer Vision is software that interprets images and video for use as digital input. Images are easily transmitted, stored and displayed for human observation, but Computer Vision is needed for any measurement or automation tasks.

Digital images (and video) must be analyzed by Computer Vision to determine if, for example, an image includes a person. Diversity in camera angles, distances, and lighting; and in human attire, pose, and appearance make the process challenging for computers. Machine Learning processes and the AI revolution have dramatically advanced the field of Computer Vision.

The most common types of Computer Vision AI are:



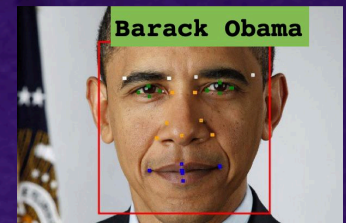
Classification - makes determinations about the entire image, for example 'cat', 'dog', or 'none'.



Detection & Localization - provides details about specific object types and where those objects are within an image. Often referred to as 'Detection'.



Character Reading - reads numbers, letters and/or symbols. Often referred to as "OCR", for Optical Character Reading, or ALPR for "Automated License Plate Reading".



Face Recognition - analyzes an image of a face for the purpose of matching against one or more other face images. Often referred to as Face Recognition Technology or (FRT).

3. Oversight tools: Governance and Ethical Implementation

Xailient's management tools provide governance and supervision over FRT services. These enforce responsible use policies across deployments.

- **Data Minimisation and Auditability and Reporting:** All recognition events are logged with metadata but without retaining sensitive image data, supporting transparency (APP 1) and enabling post-incident reviews without compromising privacy.

Policy Configuration Tools: Xailient customers can define data retention limits, deletion schedules, and review workflows—embedding APP 10 and 11 compliance directly into their operations.

FRT System Quality & Duty of Care

Xailient's solution includes ongoing review of FRT results after deployment, using a combination of human and AI supervision, extending the spirit of APP 10 (Quality).

Our system is remotely updateable, extending the spirit of APP 13 (Correction of personal information). We have extended this to updateability of the FRT itself, so that individuals are correctly recognized even as they age and change.

We believe that the individuals rights under APP 10 and 13 take on a greater meaning when considering the public at large. This integrated auditing and improvement includes ongoing proactive assessment and reduction of bias.

4. APP Alignment in Practice

APP	Compliance Mechanism
APP 1	Public-facing Privacy Policy, available signage and Privacy Impact Assessments (PIAs)
APP 3	Solicited personal data (facial biometrics) only collected with legal basis (consent or legal requirement)
APP 5	Notices at entry points, digital privacy statements, and training for staff on proper disclosures
APP 6	Data only used for explicitly stated purposes: excluded patrons, harm minimization, and (subject to regulator policy) anti-money-laundering
APP 8	No cross-border transmission; all processing occurs within Australia
APP 11	Encryption at rest and in transit; deletion protocols; data minimisation by default
APP 12/13	Individuals may request access to or correction of data held, managed through venue-specific channels or state based monitors

5. Independent Oversight and Regulatory Alignment

FRT systems in hotels and clubs must balance the principal social benefits against the community's right to privacy.

- Transparent impact assessments
- Public consultation
- Restricted data collection to patrons seated at Electronic Game Machines

6. Use Case: Patron Exclusion Without Broad Surveillance

One of the key benefits of Xailient's approach is its ability to detect banned patrons without scanning or identifying every customer. Unlike legacy CCTV-based analytics:

- Selective recognition is used only when a patron matches a ban list (i.e., is already subject to regulatory compliance processes).
- Restricted Zone of surveillance, cameras are installed in the Electronic Game Machines (EGMs) and monitor the seated patron. Bystanders and other venue visitors are not subject to FRT.

This avoids indiscriminate surveillance and supports compliance with proportionality and necessity principles under privacy law. This use case illustrates best practice under APP 6 (Use and Disclosure) and aligns with both the spirit and the letter of the Privacy Act.

7. Data Lifecycle and Security Controls

Security under APP 11 is maintained through:

- Zero image collection, unless opted-in with lawful basis.
- Encrypted communication protocols
- Granular role-based access within admin tools
- Automatic data deletion and retention policy enforcement

Venues and solution partners can demonstrate proactive risk mitigation and control over data integrity.

Conclusion: Compliance with Confidence

Privacy, ethics, and Face Recognition can co-exist through:

- **Secure Privacy-by-Design**
- **Strong operational governance**
- **Ongoing regulatory engagement**

Xailient is a leading example of how technology can align with the Australian Privacy Principles, ensuring public trust while delivering effective and lawful outcomes.

About Xailient

Xailient is the world leader in privacy-safe artificial intelligence solutions for computer vision applications. Our AI software enables real-time object detection, facial recognition, and other computer vision tasks and complies with privacy and AI regulations in over 80 jurisdictions globally. Xailient's patented technologies drive transformation across various industries by enabling devices to **See What Matters.**