Verkada

Facial Recognition Technology in Australia and New Zealand: A Privacy-Conscious Approach

Overview

Balancing Security with Privacy Expectations

Facial Recognition Technology (FRT) is increasingly sought after to help retailers and other organizations reduce theft, ensure staff safety, and streamline investigations. Yet across Australia and New Zealand (ANZ), shifting regulatory frameworks have left many businesses uncertain about how to proceed.

Verkada's approach puts privacy at the center by empowering customers to deploy FRT responsibly and selectively without compromising on safety or operational effectiveness.

Navigating an Evolving Legal Landscape

Across ANZ, privacy laws governing FRT are evolving:

- In Australia, facial geometry is classified as sensitive biometric data and is subject to strict regulation. Consent is generally required unless an exception applies, (e.g., prevent imminent and serious harm to life, health or safety, or unlawful activity).
- New Zealand does not currently mandate consent for biometric collection, but a draft biometric code is expected in 2025, signaling a shift towards increased scrutiny.

A clear takeaway from recent high-profile inquiries is that the way organizations go about their implementation matters. Transparency, proportional use, and operational rigor are key to deploying FRT in a way that earns trust and stands up to scrutiny.

Common Use Cases Addressed

- Retail shrinkage and repeat offenders: Real-time alerts and video evidence improve intervention and prosecution.
- Staff and customer safety: Support a safer in-store environment amid rising aggression and theft.
- Investigations and oversight: Reduce time spent locating footage, and ensure policy-aligned use through audit logs.

Principles of Responsible FRT Deployment

Verkada supports organizations in aligning their use of FRT with legal obligations and community standards. The following practices reflect lessons from the region and global privacy norms:

- Start with a Privacy Impact Assessment (PIA) to document risks, safeguards, and necessity.
- Limit use to high-risk areas and avoid broad or indiscriminate deployment.
- Provide clear signage with QR-code access to layered privacy policies.
- Use audit trails and role-based access controls to enforce oversight.
- Consider piloting with regulatory or community consultation.

Verkada's Privacy-by-Design Platform

Verkada's platform includes built-in tools that help support responsible, privacy-conscious use of FRT without sacrificing security. For example:

- FRT is off by default and must be enabled on a per camera basis.
- Person of Interest Only Face Search focuses the system on specific, known threats.
- Real-time and archive-based face blur helps balance monitoring with discretion.
- Customizable QR-code signage templates link to detailed privacy disclosures.
- Comprehensive audit logs show who accessed what and when.

These features help organizations meet the expectations of modern privacy regulators while improving safety and operational agility.

Learn More or Trial the Platform

Verkada offers 30 day pilots with full access to the Command platform and implementation support. Experience how our cloud-first platform and privacy-sensitive FRT tools can help you operate more securely and support compliance without sacrificing security.