NEC

Facial Recognition in Retail

An Overview of its Applications in New Zealand

Why Retailers Choose FRT

Facial recognition technology (FRT) is rapidly transforming the retail landscape, offering business owners an innovative solution to rising concerns around **safety, security, and efficiency**.

Foodstuffs North Island's six-month trial across 25 stores—New World and PAK'nSAVE— **successfully reduced serious incidents by 42%** and retail crime by 8%. Most importantly, it prevented an estimated 100 assaults and verbal abuse cases, proving FRT's power in protecting staff and customers.

Over 100 assaults prevented

For retail businesses, the benefits are clear**: safer staff, and a better customer experience**. But there's a balancing act to consider—privacy. Customers and employees expect their data to be handled carefully, and retailers must comply with privacy laws while protecting their bottom line.

NEC

As you look at adopting Facial Recognition Technology (FRT), it's essential to weigh the pros and cons:

- **Safety First**: FRT can prevent aggressive behaviour and safeguard your team.
- **Customer Trust**: Address privacy concerns proactively, ensuring transparent data usage.
- **Compliance**: Stay on top of privacy regulations and staff training.

With the right approach, FRT can protect your business, increase efficiency, and create **a safer environment** for both staff and customers.

Let's take a closer look at the what, why, and how of facial recognition in retail, so you can make an informed, strategic decision.

FRT is becoming an important tool in today's retail environment. It supports safer spaces by helping businesses identify potential risks early and reduce violent incidents, while also enhancing operational efficiency. With this capability comes the responsibility to carefully manage privacy, comply with regulations, and ensure staff are appropriately trained.

NEC

Staff assaults increased **131%**

92% of retailers impacted by crime

148,599 crimes reported in 2023 (NZ)

FRT gives you the **peace of mind** to focus on running your business while safeguarding your **staff and customers.**

Increasing Violence Against Retail Staff

Retail businesses are facing increasing levels of violence against staff.

In New Zealand, retailers continue to report rising incidents of verbal and physical abuse. Woolworths New Zealand has publicly reported a 131% increase in physical assaults on team members in recent reporting periods, leading to a $45 million investment in enhanced safety measures.

This challenge extends beyond New Zealand. Across North America, Europe, and other major markets, retailers are reporting rising levels of aggression and violence toward frontline teams.

Global industry associations continue to identify workplace violence in retail as a growing safety concern, underscoring the need for proactive risk mitigation strategies.

NEC

Facial Recognition as a Solution

As a retailer, this growing trend puts your staff and customers at risk. Facial recognition technology (FRT), particularly live facial recognition (LFR) deployed for watchlist identification, is emerging as a key solution, helping retailers protect their teams, deter criminal activity, and manage safety concerns more effectively.

92% of NZ retailers experienced crime last year

$2.6B lost annually in NZ retail crime

131% increase in staff assaults at Woolworths NZ*

Source: *Woolworths to Spend $45 Million on Safety Initiatives After 131% Rise in Physical Assaults*, RNZ, 2023. https://www.rnz.co.nz/news/business/502872/woolworths-to-spend-45-million-on-safety-initiatives-after-131-percent-rise-in-physical-assaults

NEC

How Facial Recognition works

- Facial recognition searches for faces on a watchlist, such as trespassed individuals.
- NEC's system does not store faces of regular customers.
- Best-in-class vendors rely on advanced algorithms evaluated by NIST benchmarking tests.

Face Capture

High-resolution cameras capture images of customers as they enter the store.

Face Matching

Images are compared against a watchlist of trespassed or banned individuals.

Watchlist Identification

Store personnel are alerted in real time when a match is found, including the reason for being on the watchlist.

Immediate Response

Staff can verify the individual's identity and take appropriate action **before an incident occurs** (e.g., asking them to leave).

NEC

What is an Algorithm?

And why does it matter?

- A biometric algorithm uses a person's physical or behavioral characteristics to identify them
- Algorithms are trained with diverse biometric data to deliver speed and accuracy. Here is the capture and match process:

- Algorithms create a unique "faceprint" by analysing facial features (e.g., eyes, mouth).
- "Faceprints" are compared against stored databases to identify matches (e.g., trespassed individuals).
- The quality of the algorithm directly affects how accurately the system can identify faces, especially with different lighting or angles.

Algorithm quality ensures accuracy across diverse conditions.

Challenges with Facial Recognition

Some Common Challenges:

- Communicating how it is being used
- What information is captured
- Managing privacy risks

While adopting facial recognition technology can present challenges, including customer perception and media scrutiny, transparency around its use is critical — especially as violent incidents against retail staff have risen significantly in recent years, with some major supermarket chains reporting increases of up to 50% in physical assaults.

Lack of Understanding: Many are unaware of how biometrics works, raising privacy and security concerns.

Misconceptions: Customers may see biometrics as invasive or solely for surveillance.

Reducing Staff Assaults: Clear messaging on **why** facial recognition is being introduced

Privacy Impact and Compliance in New Zealand

The Importance of Compliance

Facial recognition deployments must align with relevant laws and regulations, such as New Zealand's Privacy Act 2020. Compliance ensures both legal adherence and the building of customer trust.

Key Considerations for Compliance

(According to privacy.org.nz)

Lawful Purpose: Clearly define the legitimate business purpose for facial recognition (e.g., security, staff safety). Principle 1 of the Privacy Act.

Notification: Notify customers about FRT usage through visible signage and policy documentation. Transparency aligns with Principle 3 of the Privacy Act.

Minimising Intrusion: Ensure FRT is not used in an overly intrusive or unfair way. Consider using real-time processing to avoid unnecessary data retention (Principle 4).

Data Security: Implement robust encryption and secure storage for biometric data to protect against breaches. Compliance with Principle 5 is critical.

Access and Correction: Allow individuals to access their data and correct inaccuracies. This upholds their rights under Principles 6 and 7.

Accuracy and Retention: Keep data accurate and up-to-date and delete it when no longer required (Principles 8 and 9).

Disclosure: Clearly communicate the purpose of sharing data, adhering to Principle 11.

NEC

Start with a Privacy Impact Assessment (PIA)

1. Define the Purpose

- Clearly outline the goals of the initiative requiring a PIA.
- Identify the types of personal data involved.

2. Identify Risks and Impacts

- Analyse potential privacy risks and their impact on individuals through a PIA.
- Consider factors like data collection, storage, and use.

3. Evaluate Compliance

- Assess the initiative's compliance with New Zealand's Privacy Act as part of the PIA.
- Identify any gaps or areas needing improvement.

4. Develop Mitigation Strategies

- Use PIA findings to create safeguards addressing identified risks.
- Adjust project design to strengthen data protection.

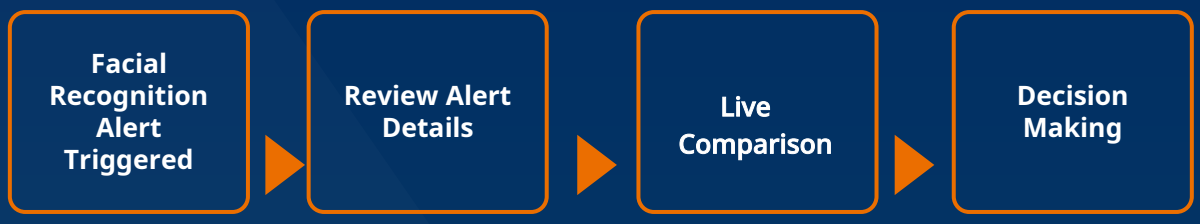
5. Document and Communicate

- Record the PIA process, findings, and mitigation strategies.
- Share results with stakeholders for transparency.

NEC

FRT Alert Handling: Human Oversight & Continuous Learning

Facial recognition real time alerts are a tool — not a replacement for human judgement. Retail safety teams remain in control of every decision, supported by clear procedures, ongoing training, and systematic monitoring and feedback. This ensures alerts are handled responsibly, consistently, and with continual improvement in mind.



The facial recognition system detects a potential match and sends an alert in real time.

Staff check the alert's location, timestamp, and FRT image comparison.

Staff compare the captured image with the individual in-store for confirmation.

Based on verification, staff decide on the next steps.

System Alert Review: Confirm the real time alert by checking details and comparing images.

Secondary Verification: Escalate to a manager if needed for further confirmation.

Non-Confrontational Approach: Approach individuals calmly and professionally, following protocols.

Documentation: Record all steps, decisions, and outcomes for accountability.

Ongoing Training: Ensure regular staff training on procedures, customer sensitivity, and risk mitigation.

NEC

Staff Training and Procedures

Your facial recognition process should be well-defined and publicly available to mitigate negative perceptions or reputational risks. This should include things like human intervention and secondary verification.

Critical Role of Training: Facial recognition is a supportive tool, not a sole decision-maker. Processes should include human oversight and verification.

Transparency:
Clearly define and publicise your facial recognition process to ensure proper program management and mitigate reputational risks.

Key Training Elements:

- Adding individuals to watchlists: Define criteria, approval processes and notification processes.
- Staff actions for identified individuals.
- Detailed incident documentation.
- Regular refresher training.
- Deployment reviews to ensure optimal camera positioning.

NEC

Bias and Fairness

Earlier facial recognition systems faced challenges with demographic bias. Today, independent testing plays a critical role in measuring performance and fairness. NEC's algorithms consistently rank among the top performers in independent evaluations conducted by the U.S. National Institute of Standards and Technology (NIST), demonstrating high accuracy across large, diverse datasets. Importantly, every alert is reviewed by trained staff, supported by ongoing training and continuous monitoring to ensure responsible use.

Historical Racial Bias: Early facial recognition systems had higher error rates for darker skin tones.

Lack of Diverse Datasets: Non-diverse training data led to poor accuracy for underrepresented groups.

Advancements in Algorithms: NIST (National Institute of Science and Technology)-tested algorithms now ensure high accuracy across all ethnicities, reducing bias.

NEC

Myths vs Facts

Myth #1: Biometric solutions are inherently racially biased.

Fact #1: Biometric solutions are be designed for fairness. Leading algorithms show no bias per NIST testing.

Myth #2: Biometrics are a tool of discrimination and surveillance.

Fact #2: Biometrics enhance security and accessibility while respecting privacy. NEC's system does not store faces of regular shoppers.

Myth #3: Facial Recognition is one step closer to a Police State.

Fact #3: Facial recognition is regulated by New Zealand's privacy laws and only used for trespassed individuals. CCTV is already widely adopted in retail stores.

Myth #4: Biometric data is inherently insecure and vulnerable to misuse.

Fact #4: Secure storage with encryption, access controls, and data-handling protocols ensures data protection.

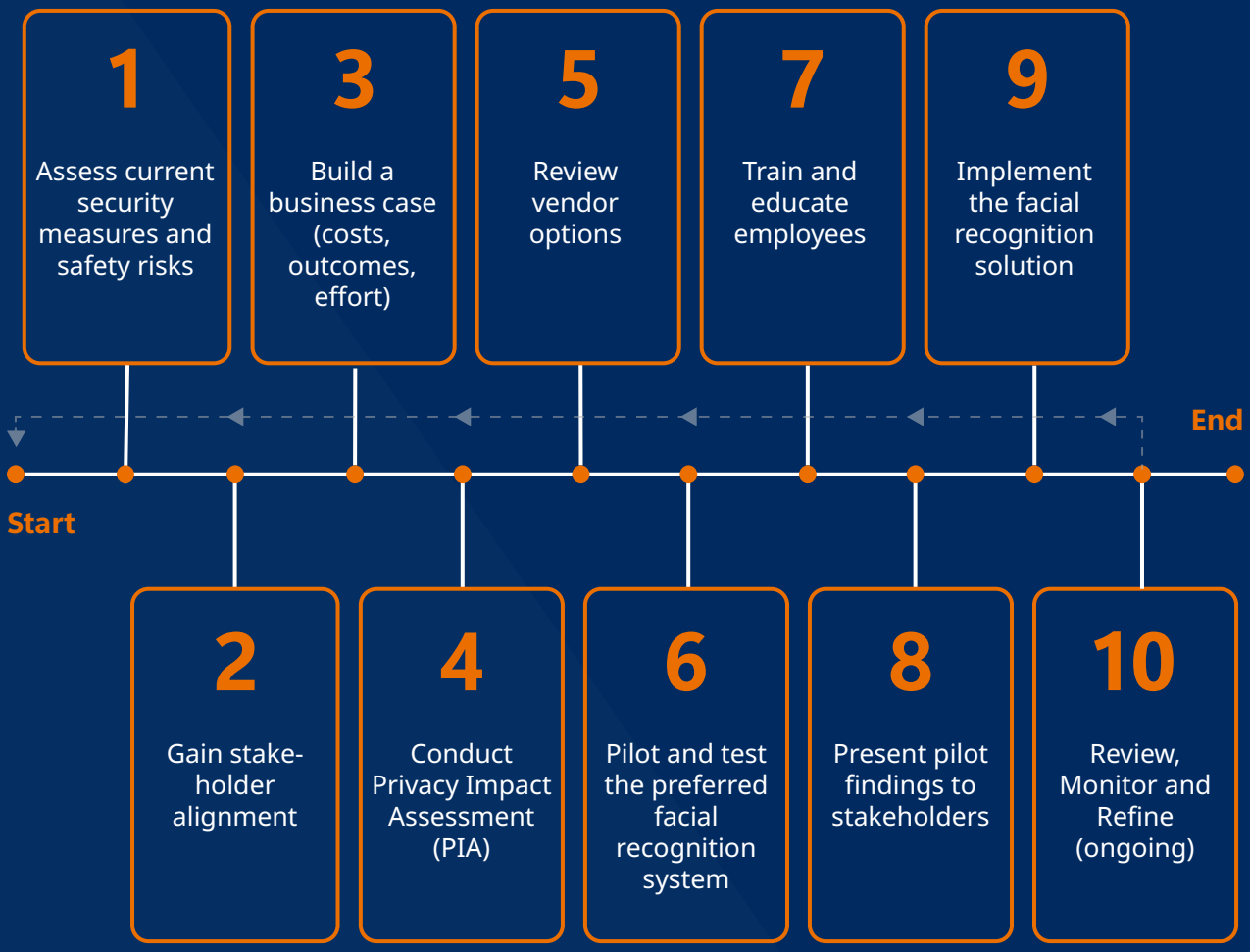
Myth #5: Biometric solutions are a replacement for human judgment.

Fact #5: Biometrics assist decision-making but rely on human oversight to ensure responsible and ethical use.

Independently tested by NIST (U.S.) and NPL (UK) with leading benchmark performance.

NEC

Facial Recognition Buyer Journey



Implementing facial recognition technology in a retail environment has the potential to be transformative. However, it requires careful consideration of operational, technical, and ethical factors.

Given the sensitive nature of facial recognition, understanding the key steps is essential to ensure a successful deployment.

NEC

Key Considerations for Implementing FRT

Business Objectives

Clearly define the safety challenge facial recognition is intended to address. How does it support staff

Stakeholder Alignment

Are internal teams aligned on objectives, risks, and governance requirements? What processes are in place to support collaboration, documentation, and accountability?

Technical Readiness

Is your IT infrastructure prepared for secure integration? Are camera systems, storage, and network capacity sufficient to support reliable performance?

Training & Change Management

Is there a structured training programme to ensure alerts are assessed consistently and responsibly? How will you manage employee or customer concerns and support adoption?

Monitoring, Review & Continuous Improvement

Are there formal processes to review system performance, assess outcomes, and refine procedures? Is a feedback loop in place to support ongoing improvement?

Data, Privacy & Compliance

Are privacy considerations clearly addressed? Has a Privacy Impact Assessment (PIA) been completed, and are governance controls documented?

Defining Success

What does success look like in strengthening staff safety? Which metrics will be monitored, reviewed, and refined over time?

NEC

Facial Recognition Risks and Mitigations

Risk	Description	Mitigation
Privacy Violations	Unlawful or unethical capture or misuse of personal data.	Conduct a Privacy Impact Assessment (PIA) to evaluate data collection, storage, and access controls. Ensure transparent practices.
Data Security Risks	Unauthorised access to stored data of trespassed individuals may lead to data theft or misuse.	Implement robust encryption, secure storage, and strict access controls. Follow information security best practices.
Racial Bias	Facial recognition algorithms may exhibit higher error rates for certain demographic groups in poor lighting conditions.	Use NIST-approved algorithms trained with diverse datasets. Ensure proper camera placement and lighting for improved accuracy.
Transparency Issues	Lack of clear communication about how and why facial recognition is used may lead to customer distrust.	Provide visible signage, press releases, and public policies explaining the system's purpose and processes.
Over-Reliance on System	Dependence on technology may replace human judgment, increasing the risk of misidentification and reputational harm.	Incorporate secondary verification with human oversight. Train staff to use facial recognition responsibly.
Reputation Damage	Public concerns over privacy can lead to reputational harm and resistance.	Engage in community consultations, share ethical commitments, and emphasise safety benefits. Be transparent with customers.
Legal Compliance	Risk of non-compliance with privacy and data protection laws.	Regularly review and update system usage according to privacy laws, such as the New Zealand Privacy Act.

NEC

Conclusion

Facial recognition technology (FRT) supports retailers in responding to increasing violence against staff. With responsible implementation, human verification, and continuous oversight, it helps create safer retail environments.

- Implementing this technology must comply with **New Zealand law** and align with your **security objectives**.
- This white paper provides **practical steps** to get started, focusing on:
  - **Clarifying the problems** you're solving.
  - Aligning **stakeholders**.
  - Educating on the **benefits and risks** of facial recognition.

For more information:

- Email us to request our comprehensive guide or a friendly, no-obligation discussion about your specific business needs at **hello@nec.co.nz.**
- Visit our website **www.nec.co.nz**.

NEC