30 September 2025

Retail NZ submission: Proactive technology solutions to reduce retail crime

Accompanying Letter on Biometric Processing and Information Sharing

Retail NZ welcomes the opportunity to provide detailed input to the Ministerial Advisory Group (MAG) consultation on technology solutions for retail crime prevention. While our formal responses to the submission portal questions reflect the core positions of our members, this accompanying letter is necessary to provide the essential nuance required for effective policy development, particularly concerning the deployment of Facial Recognition Technology (FRT) and the governance of information-sharing networks. Where we have not provided a response in the survey, it is because the question format does not allow us to represent the wide-ranging views of our members.

As the peak body representing the views and interests of New Zealand's retail sector, we are cognisant of the challenges of balancing the safety of the 230,000 retail employees, as well as customers in the face of significant and pervasive retail crime, and the important protections to privacy set out in the Privacy Act 2020 and the Biometric Processing Privacy Code 2025 which comes into force on 3 November 2025.

While Retail NZ does not itself participate in informal information sharing or FRT, our members do, and our response takes into account their perspective.

1. Context-Dependent Regulation: Guidelines Over Rigid Legislation

Retail NZ supports a regulatory environment based on flexible, principles-based guidelines, such as those established in the *Biometric Processing Privacy Code 2025*, rather than prescriptive legislative rules.

The retail environment is highly diverse: a small suburban dairy faces different threats and possesses different resources than a large supermarket chain or a specialised jewellery store. We are concerned that rigid, fixed rules would be unable to accommodate this range of circumstances and may become quickly obsolete with the advancement of technology.

We believe the existing framework, particularly the *Biometric Processing Privacy Code 2025*, provides the necessary structure, allowing the Office of the Privacy Commissioner (OPC) to work collaboratively with the sector. This approach enables the development of detailed, fit-for-purpose guidance that can be adapted by individual businesses, ensuring that privacy safeguards are always proportionate and relevant to their specific operational context.

RETAIL NZ
Level 9, 175 Victoria Street, Wellington 6011

NZ // 0800 472 472 info@retail.kiwi
AU // 1800 128 086 www.retail.kiwi

2. Informal Information-Sharing Networks

We acknowledge that many retailers currently use informal, low-tech information-sharing mechanisms (such as WhatsApp groups and Facebook groups) to enhance staff safety and protect property. These networks provide a cost-effective communication line, particularly for small businesses. Whether the informal networks stay as they are, receive direct support from government with stronger governance requirements, or are replaced or supplemented by council or industry-led partnerships as in the UK, steps must be taken to ensure these networks are legitimate, safe and legally compliant. Governance features that mirror the principles applied to FRT should be adopted. These safeguards include:

- Clear inclusion criteria requiring verifiable evidence (not mere suspicion)
- Human verification of images and information
- The establishment of audit trails
- A formal retraction/correction process across all participants
- Time-limited sharing/retention protocols
- Member vetting and training to guard against bias and discrimination.

Retailers should have access to guidance and training to help them strike the balance between protecting privacy and preventing crime. We believe that specific legislative change to the Privacy Act to provide new protections is unnecessary. Instead, comprehensive, clear guidelines and training are the best approach to ensure retailers remain fully accountable for appropriate data sharing while having the confidence to actively and legally participate in these crime-prevention networks.

Existing groups such as Eyes-On Wellington, supported by Wellington City Council and the Wellington Police District, invite local retailers to share real time intelligence within a secure platform. These groups also offer training to help staff recognise and deal with potential threats. These groups demonstrate the viability for low tech and community-based crime prevention solutions. Retail NZ would support further investigation as to the efficacy of these groups at preventing crime.

Joining a local business support group helps to enhance community connections and effectively puts more eyes on stores. In the Retail NZ Crime Survey 2023 a large retailer stated, "It's also critical that we continue to build strong relationships with both local and national Police, community groups and other retailers — and we're prioritising doing this." This shows that retailers see clear value in community networks for creating a sense of safety.

3. Thresholds for Facial Recognition Technology (FRT) Use

We are aware of two large national retailers actively using FRT. Other businesses are considering implementing FRT, although the majority of our members, in particular smaller and medium-sized retailers, tell us they would be unlikely to employ FRT, primarily due to cost of implementation and maintenance, although some have concerns about the backlash from the public until FRT is more widely established.

FRT is an inherently intrusive technology, therefore retailers should determine if its use is a proportionate approach for their business. In general, its use should be reserved for addressing serious harmful behaviour which may include violent or repeat offending.

Threshold is Defined by Impact, Not Dollar Value

The use of FRT should not be determined by a fixed minimum dollar value. Instead, the decision must be made by each retailer, based on a careful assessment of the proportionality of the measure relative to the impact of the crime on their specific business.

1. **High-Risk Contexts:** In environments like a jewellery shop, a theft incident necessarily involves violence (e.g., smashing a cabinet), making the act itself the primary justification for FRT use, regardless of the value of the item stolen.
2. **Cumulative Impact:** For small businesses, repetitive low-level theft, such as repeated low value shoplifting, may pose a serious financial threat to the business's sustainability. In such instances, if less intrusive alternatives prove ineffective, the cumulative private benefit to the business may substantially outweigh the privacy risk, thereby justifying FRT deployment under Rule 1(4) of the *Biometric Processing Privacy Code 2025*.

4. Suitability of FRT for Small Stores

FRT is unlikely to be the best tool for small businesses due to its inherent complexity and significant resource demands, meaning it is not a "set and forget" type of technology. The implementation of FRT is resource-intensive, likely to require substantial investment not only in the technology itself but also, more significantly, in the training and ongoing oversight and management of staff, processes and procedures. Data from the UK shows less than 10% of businesses that employ Facewatch FRT are small businesses. For some businesses, the potential crime reduction benefits of implementing FRT does not justify the significant costs of the technology.

Without proper training and expertise in-house, there is a risk that the technology may be misused or that compliance with the *Biometric Processing Privacy Code 2025* cannot be maintained. For small businesses, particularly those with fewer staff, FRT may be ineffective because offenders might already be deep inside the store by the time an alert is triggered, verified and acted upon. In smaller stores, staff may recognise repeat offenders more quickly than the FRT alert can be triggered.

Furthermore, implementing FRT carries high privacy risks related to overcollection, surveillance, misidentification and bias, which require adherence to robust security safeguards, confirming that the technology demands continuous human oversight and management to ensure its effectiveness and compliance.

5. Watchlist Sharing and Centralisation

The sharing or centralisation of watchlists, whether through FRT or low-tech means, presents a significant increase in privacy risk. A number of our members would be interested in shared watchlists in certain situations.

Shared Watchlist Justification

We acknowledge that pooled watchlists (e.g., within a local business district) may be justified to address organised crime or store-hopping by serious recidivist offenders. If a shared system is proposed:

1. **High Threshold:** It must be restricted to the current high thresholds of serious/violent offending or high-harm recidivism.

2. **Oversight:** Any proposed centralised system must be designed with close regulatory monitoring and oversight from the OPC and an independent industry body, alongside partnership with local agencies and retailers.
3. **Suppliers:** Any proposed system must be provided by a credible and reliable supplier that can demonstrate robust data management and security protocols. It is essential that the system utilises a verified New Zealand database to ensure accuracy and reduce the risk of bias and misidentification.

6. Conclusion and Commitment

Retail NZ believes that technology, including FRT, is a powerful tool to combat the unacceptable levels of crime and violence experienced by our sector. The successful Foodstuffs North Island trial demonstrated that FRT can be effective in reducing serious harmful behaviour when implemented with robust, human-centric privacy safeguards.

We support the development of clear guidelines and best practice protocols, working in partnership with the MAG and the OPC, to ensure that any adoption of FRT or information-sharing is context-dependent, effective and compliant with privacy obligations. This ensures the appropriate balance is maintained between crime prevention, staff safety and the privacy rights of New Zealanders.

Ngā mihi nui,

Carolyn Young

Chief Executive