



Facial Recognition Technology Privacy Impact Assessment Report

August 2026

1. Project description

1.1 Project Summary

Foodstuffs North Island Limited (**FSNI**) is the franchisor of over 300 supermarket stores¹ in the North Island of Aotearoa New Zealand (**Stores**). Following a significant increase across all Stores in the recorded rates of assault (physical and verbal) and other forms of aggressive, violent and threatening behaviour, theft, burglary and robbery (**Harmful Behaviour**), FSNI and certain Stores (**FRT Stores**) trialled the use of facial recognition technology (**FRT**) for the sole purpose of preventing and reducing repeated Harmful Behaviour by previous offenders (**Purpose**). FRT allows FRT Stores to proactively identify and manage previous offenders, allowing stores to intervene before they commit further Harmful Behaviour.

The findings from the independently designed and evaluated trial indicate that the use of FRT in the FRT Stores was effective in reducing serious Harmful Behaviour – assaults, incidents of verbal abuse and incidents of disorderly conduct – by repeat offenders. The independent evaluator has confirmed that FRT continues to be effective with an estimated 369 serious incidents (including assault and other forms of aggressive, violent and threatening behaviour) avoided since the start of the trial to the beginning of July 2026.

FSNI's values (as summarised below) underpin its approach to the use of FRT as set out in this PIA:

- (a) **Think Customer:** FSNI and FRT Stores are focused on making sure all customers have a safe shopping experience.
- (b) **In It Together:** FSNI and FRT Stores want to make sure all team members are safe when doing their job – the team looks after and backs each other.
- (c) **Courageous:** FSNI and FRT Stores are focused on being bold and innovative – we want to create the safest retail environment for team members and customers.
- (d) **Above the Line:** FSNI and FRT Stores take 100% ownership, accountability and responsibility for the use of FRT in a compliant way and are committed to ensuring that processes and privacy safeguards are continuously improved through learning.

The Office of the Privacy Commissioner (**OPC**) initiated an inquiry into the use of FRT by FRT Stores (**OPC Inquiry**)² and released its report in June 2025. The OPC Inquiry concluded that the trial was compliant with the Privacy Act 2020 and FRT made “a substantial difference in reducing rates of serious recidivist crime” in FRT Stores.³

¹ This includes New World, PAK'nSAVE, Four Square and Gilmours.

² See [Inquiry into Foodstuffs North Island trial use of facial recognition technology](#).

³ See OPC Inquiry Report discussion from [136] – [144].

As FRT has been shown to be effective in achieving the Purpose, the FRT Stores intend to continue to use FRT for the Purpose subject to the recommendations set out in this PIA to ensure the use of FRT remains effective, safe and compliant with the Privacy Act 2020 (**Privacy Act**) and the Biometric Processing Privacy Code 2025 (**Code**).

1.2 Purpose of this PIA

FSNI has undertaken this PIA on behalf of the FRT Stores.

While FRT has been shown to be effective, FSNI and FRT Stores understand there are risks associated with FRT from a privacy perspective. The purpose of this PIA is to:

- (a) identify any privacy concerns and potential privacy risks arising from the use of the FRT System (as defined in section 2.3) by FRT Stores; and
- (b) identify and provide effective strategies and recommendations to assist FRT Stores in mitigating those risks.

1.3 Review and consultation process

As part of its assessment of FRT prior to, during and following the trial, FSNI reviewed various information sources and consulted with several internal and external stakeholders, including the OPC and two separate external Māori data consultants, in relation to the use of FRT in FRT Stores.

FSNI has also assessed the use of FRT by FRT Stores against the Māori Data Governance Model published by Te Kāhui Raraunga Charitable Trust.

As at the date of this PIA, FSNI continues to engage with Māori (including iwi representatives from across the North Island and FSNI and FRT Store employees who identify as Māori) – this engagement will inform FRT Stores' ongoing use of FRT.

2. Purpose of using FRT

Between 1 January 2023 and 31 December 2025, 47.1% of all recorded retail crime incidents were committed by repeat offenders across the Stores and 58% of all recorded retail crime incidents were committed by repeat offenders across the FRT Stores.

During the 1 January 2025 to 31 December 2025 period, there were 7,257 harmful events⁴ in Stores, up 5.9% on the same time period in the previous year.

In retail settings, theft is often a lead indicator for other harmful behaviour. Stores continue to report an increase in violence and assaults associated with theft by offenders. During the 1 January 2025 to 31 December 2025 period, there were 18,217

⁴ "Harmful events" include assault (physical and verbal), breach of trespass / banning notices, other forms of aggressive, violent and threatening behaviour, burglary and robbery.

harmful event and theft incidents in all Stores, up 3.4% on the same period in the previous year.

Stores in lower socio-economic areas have indicated that they are feeling increasingly helpless as offenders' attitudes toward managers and staff are becoming more brazen. These incidents deter owners from continuing operation because of the risk to the personal safety of staff, customers and owner operators, and the resulting loss of profit. This is also consistent with the experience of other retail stores in New Zealand and Australia.

The Police have indicated to Stores that, due to resource constraints and retail crime having lower priority, Police do not attend to theft-related matters that have a value of less than \$1,000. This leaves Stores with little immediate recourse against offenders other than issuing verbal and formal trespass notices where practical and, when necessary, submitting claims with supporting evidence to the Police. Police cannot successfully prosecute repeat offenders unless Stores provide sufficient supporting evidence. To assist Stores to efficiently compile the appropriate evidence from CCTV footage, Stores require a solution that accurately identifies repeat offenders.

2.1 Methods attempted to address the problem

FRT Stores have tried to prevent the recurrence of Harmful Behaviour by relying on a range of measures. This includes relying on security personnel to identify previous offenders by their unaided memory alone. This is not an effective or accurate method of identification for several reasons. In addition to the fallibility of memory, a repeat offender may, for example, easily re-enter a FRT Store when the relevant security personnel who previously dealt with that individual are not on shift or have otherwise left the FRT Store's employment. Individuals may also change their appearance, making it more difficult for security personnel to identify them by mere memory.

FRT Stores have also tried a number of other methods, including increasing security and training, improving store layout, and deploying fog cannons in smaller FRT Stores. However, none of these methods allow FRT Stores to proactively identify and manage previous offenders, before they commit further Harmful Behaviour.

2.2 Alternative options for addressing the problem

FSNI and FRT Stores have considered several alternative methods to proactively identify previous offenders and respond to repeated harm they cause in an attempt to prevent and reduce the recurrence of Harmful Behaviour. These alternative methods include weapon detection technology and smart CCTV cameras to identify and track suspicious behaviour. Again, these methods do not assist in proactively identifying repeat offenders.

Overall, FSNI and FRT Stores consider that the methods attempted and the alternative options considered are not effective in assisting FRT Stores to proactively identify previous offenders and prevent and reduce the incidence of repeated Harmful Behaviour by those offenders.

2.3 The solution

FSNI (on behalf of FRT Stores) identified and trialled FRT as an option to assist FRT Stores to reduce the incidence of repeated Harmful Behaviour by previous offenders by allowing FRT Stores to proactively monitor for and identify previous offenders.

FRT proved to be effective in reducing the repeat of harmful behaviour by previous offenders in the FRT Stores during the trial. The independent evaluator found that FRT Stores experienced an estimated 16% reduction in serious harm and approximately 115 serious harm events (including assault) were prevented during the trial period.⁵

Based on data collected and evaluated by the independent evaluator from the start of the trial to the beginning of July 2026, the independent evaluator estimates that around 369 serious incidents (including assault and other forms of aggressive, violent and threatening behaviour) have been avoided as a result of the use of the FRT System. The independent evaluator also estimates that during this period FRT has reduced serious Harmful Behaviours (including assault and other forms of aggressive, violent and threatening behaviour) by 13%, shoplifting by 23% and breaches of trespass by 31%.

FSNI and FRT Stores acknowledge that addressing Harmful Behaviour requires a multi-layered approach that involves different methods, strategies, processes and tools. While FSNI and FRT Stores have identified FRT as one of those tools – in particular, to assist in preventing and reducing repeated Harmful Behaviour by proactively monitoring for and identifying previous offenders – FSNI and FRT Stores will continue to utilise other methods, strategies, processes, alongside FRT, to address Harmful Behaviour.

Imagus by Vix Vizion

FRT Stores will continue to use the Vix Vizion, *Imagus* Facial Recognition Solution (**FRT System**). Vix Vizion is an Australian company that provides facial recognition and video analytics solutions.

The OPC Inquiry found the FRT system trialled by FSNI and FRT Stores to be professionally tested as suitable for operating “in the wild”.⁶

Accuracy

The National Institute of Standards and Technology (**NIST**), an agency of the US Department of Commerce, has evaluated the accuracy and demographic bias of the

⁵ See also the OPC’s finding that FRT was an effective way of reducing serious harm (OPC Inquiry report at [136] – [144]).

⁶ OPC Inquiry report at [183].

FRT System.⁷ NIST found that the FRT System is highly accurate in processing “wild” images – i.e., those where the subject does not pose for the image.⁸

FRT Stores will use several measures to mitigate the risk of inaccuracy and bias, including:

- (a) all authorised FRT Store personnel are trained on the use of the FRT System and the verification process for FRT Alerts, including on the concerns relating to privacy, inaccuracy and bias (unconscious and conscious);
- (b) the FRT System in each FRT Store is calibrated to an accuracy level of 93%,⁹ meaning only matches with an accuracy rating of at least 93% will trigger an FRT System match;
- (c) two authorised and specially trained FRT Store personnel must verify the FRT System match before any action is taken; and
- (d) this PIA and the operation of the FRT System will be updated and reviewed on a regular basis, including to ensure that:
 - (i) any issues relating to inaccuracy and bias that are identified in the course of using the FRT System are appropriately addressed;
 - (ii) the technical and operational settings of the FRT System remain appropriate;
 - (iii) the FRT System is effective at reducing incidents of Harmful Behaviour; and
 - (iv) the use of the FRT System remains necessary for achieving the Purpose.

3. Summary of assessment of proportionality

Given:

- (a) the extent of Harmful Behaviour by repeat offenders in FRT Stores;
- (b) the impact that Harmful Behaviour caused by repeat offenders has on FRT Store staff, customers and other people who enter those stores;
- (c) FRT will be used solely for the Purpose;

⁷ NIST established a Face Recognition Testing Program in 2000 to provide independent evaluations of both prototype and commercially available facial recognition algorithms. NIST has extensive experience in measuring and reporting on the accuracy and reliability of FRT and has also provided state-of-the-art technology benchmarks and guidance to the FRT industry.

⁸ See <https://www.vixvizion.com/nist-report>.

⁹ The independent evaluator and OPC (see OPC Inquiry report at [191] and [227(a)]) recommended the algorithmic accuracy setting should be increased from 90%. While the OPC recommended a 92.5% accuracy setting, FSNI and FRT Stores have increased the setting to 93%.

- (d) the effectiveness of FRT in preventing incidents of repeated Harmful Behaviour by previous offenders (as demonstrated by the trial in FRT Stores and the data collected on an ongoing basis following the trial);
- (e) that the alternative methods currently used or considered by FSNI and FRT Stores are not as effective as FRT in preventing or reducing the rates of Harmful Behaviour by repeat offenders;
- (f) the FRT System watchlist for each FRT Store will only apply to that specific FRT Store (and won't be shared with other FRT Stores);
- (g) FRT Stores' legal and moral obligation to provide a safe workplace for their staff and a safe environment for members of the public who enter the FRT Stores;
- (h) the clear public benefit to FRT Store staff and the public of a safer workplace and FRT Store environment, and the clear private benefit to FRT Stores to ensure compliance with the legal and moral obligation to provide a safe workplace and Store environment and of reduced stock loss resulting from theft by previous offenders,

and:

- (i) provided the inherent privacy risk (including from a Māori data sovereignty, tikanga and Te Ao Māori perspective) identified in this PIA is mitigated and reduced to an acceptable level by adopting and implementing the privacy recommendations set out in this PIA,

FSNI and FRT Stores consider the use of the FRT System to be a necessary and proportionate solution for preventing and reducing the incidence of repeated Harmful Behaviour by previous offenders.

4. Use of the FRT System

4.1 How do FRT Stores inform the public about their use of FRT?

To inform customers that a FRT Store is using FRT, each FRT Store displays large-format signage at all entry points before the individuals enter the range of the FRT System cameras. Smaller signs (A4) are placed throughout the FRT Store. Signs are displayed in English and Te Reo Māori. The signs explain:

- that FRT is in use in the FRT Store;
- the purpose for which FRT is used; and
- how individuals can obtain more information about the use of FRT in FRT Stores (see below).

All signage refers to the relevant FRT Store's banner privacy policy and the FSNI FRT webpage, both of which contain specific information about the use of FRT by FRT Stores, including a list of the FRT Stores. FRT Store staff are trained to: (a) direct customers, on request, to where they can find more information about the use of FRT and FRT Stores have easily accessible physical copies of their FRT Store banner privacy policy; and (b) verbally inform customers, who they reasonably believe are visually impaired, that FRT is in operation.

4.2 How do FRT Stores collect and use Personal Information and Biometric Information using the FRT System?

FRT System collection

Each FRT Store's FRT System collects and reviews facial images of all individuals that enter that store and assigns a unique, de-identified facial signature to each facial image for matching purposes. This facial signature is referred to as a 'biometric template'. The collection of images is done via dedicated FRT cameras or through the FRT Store's CCTV cameras that send footage through separate feeds to the CCTV system and FRT System (there is no integration between the systems).

Where the FRT System does not identify the image as a match with a Person of Interest (as defined below) that is enrolled in the watchlist within the FRT System (**FRT Watchlist**), the image and related biometric template is automatically and permanently deleted within 60 seconds of the image entering the FRT System.

Where a Harmful Behaviour incident occurs in a FRT Store, authorised FRT Store personnel manually enrol facial images of Persons of Interest collected by the FRT Store's CCTV system into the FRT Watchlist as set out below.

Matching of facial images

Each biometric template created by the FRT System when an individual enters the FRT Store is matched against biometric templates of Persons of Interest in that FRT Store's FRT Watchlist. Each FRT Store's FRT System is calibrated so a match is only triggered if the collected image matches the image of a Person of Interest in the FRT Watchlist with an accuracy level of 93% or more. Non-matched images and related biometric templates are automatically and permanently deleted within 60 seconds of the image entering the FRT System.

FRT Watchlist Enrolment

Where a Harmful Behaviour incident occurs in a FRT Store, authorised FRT Store personnel manually enrol facial images of individuals into the FRT Watchlist from that FRT Store's CCTV footage, if they reasonably believe, based on supporting evidence, that the individual is a **Person of Interest (POI)**, being an:

- (a) **Offender** – an individual that has:
 - (i) engaged in Harmful Behaviour by:
 - (A) assaulting (physically or verbally), or behaving in a violent, aggressive, threatening or abusive manner towards, staff and/or other customers;
 - (B) damaging FRT Store product(s) and/or property;
 - (C) stealing or attempting to steal high-value items from the FRT Store; or

- (ii) re-entered the FRT Store in breach of their trespass notice where that trespass notice was issued because the individual engaged in Harmful Behaviour; or
- (b) **Accomplice** – an individual who has actively assisted an Offender in the commission of Harmful Behaviour, e.g., helps the Offender to flee the FRT Store by driving a get-away car, or hinders FRT Store personnel from responding to the Harmful Behaviour.

Before enrolling a POI in the FRT Watchlist, two authorised FRT Store personnel must take reasonable steps to:

- (c) confirm that the individual is a POI (that is, they meet the criteria for enrolment); and
- (d) ensure that the FRT Watchlist enrolment information is accurate, relevant and not misleading (e.g., ensuring the image to be uploaded to the FRT Watchlist is a good quality image).

Authorised FRT Store personnel are not permitted to enrol any minors (i.e., someone under the age of 18 years old) or vulnerable persons (i.e., a person with a disability) into the FRT Watchlist.

Any POI who was on a FRT Store's FRT Watchlist as at the date of this PIA will remain enrolled on that Watchlist until the relevant enrolment period for that POI ends in accordance with this PIA.

4.3 What types of Personal Information and Biometric Information does the FRT System collect?

The FRT System, including the FRT Watchlist, collects the following types of:

- (a) Personal information (together, **Personal Information**):

Functionality	Description
POI Name	The name of the POI (if volunteered or otherwise collected).
Behaviour*	Description of Offender's Harmful Behaviour at the time of incident, e.g., aggressive, abusive, violent, or in the case of an Accomplice, details of how they assisted the Offender. *This information is used so that staff can take appropriate action, should they need to approach or monitor that individual in the future.

Trespass notice reference ID	If applicable, the trespass notice ID. If the FRT Watchlist entry is for an Accomplice, the trespass notice ID of the Offender is also included.
Security system reference number	Security system reference number.
Verifier name	The name of authorised FRT Store personnel that have verified the enrolment and/or FRT System match.

(b) Biometric information (together, **Biometric Information**):

Functionality	Description
Image	Images of the person captured by the FRT Store's FRT System cameras.
Biometric template*	An encrypted digital biometric signature generated from the image. *This is the only additional personal information that FRT Stores will collect that existing systems used by FRT Stores do not.

4.4 What happens if there is a FRT System match?

If the facial image collected and reviewed by the FRT System matches an image in the FRT Watchlist:

- (a) authorised FRT Store personnel receive an alert from the FRT System (**FRT Alert**);
- (b) two authorised FRT Store personnel must verify the accuracy of the FRT System match;
- (c) if the match is not confirmed as reasonably identical by two authorised FRT Store personnel, then no action is taken;
- (d) if the match is confirmed as reasonably identical by two authorised FRT Store personnel, the authorised personnel respond to the FRT Alert;
- (e) once the FRT Alert is resolved, the FRT Alert is updated to confirm the match and a description of the incident is manually added to the FRT Watchlist by one of the authorised FRT Store personnel and verified by another authorised staff member;
- (f) the information within the FRT System that is the subject of the FRT Alert (including the facial image and related biometric template) is automatically and

permanently deleted from the FRT System at midnight on the day the image first enters the FRT System;

- (g) prior to the deletion of the information from the FRT System described in paragraph (e) above, the FRT System sends an automated email to FSNI with the FRT Alert information (but not the collected image or the biometric template) for record keeping, review and auditing purposes. This information is automatically and permanently deleted three years from the date of the FRT Alert.

All authorised FRT Store personnel that have access to the FRT System and FRT Alerts are trained to verify the accuracy of matches (e.g. carefully checking CCTV footage to check the accuracy of the match and verify an individual's identity), and on the process to be followed in the event of a misidentification.

4.5 Storage and Retention of Personal Information and Biometric Information

All Personal Information and Biometric Information stored in the FRT Watchlist and/or held in the FRT System is stored in Aotearoa New Zealand.

Where the FRT System does not detect a match between the collected image and the image of a POI that is enrolled in the FRT Watchlist, the collected image and related biometric template are automatically and permanently deleted within 60 seconds of the image entering the FRT System.

Where the FRT System detects a match and alerts authorised FRT Store personnel, the information within the FRT System that is the subject of that FRT Alert (including the facial image and related biometric template) is automatically and permanently deleted from the FRT System at midnight on the day the image first enters the FRT System.

Personal Information and Biometric Information of a Person of Interest stored in the FRT Watchlist is stored for a duration of:

- (a) 3 months for an Accomplice; or
- (b) up to (but not exceeding) 2 years for an Offender.

4.6 Security of Personal Information and Biometric Information

All Personal Information and Biometric Information collected and/or held in the FRT System is securely stored on servers in Aotearoa New Zealand, and is subject to robust technical data security controls and strict access controls.

All authorised FRT Store personnel receive training on the use of and security processes for the FRT System and all access is logged and regularly reviewed. Authorised FRT Store personnel do not receive access to the FRT System until training is completed.

FSNI (and its nominated advisors and service providers that are bound by obligations of confidentiality) may process the Personal Information and Biometric Information from the FRT System. This is done solely on behalf of the relevant FRT Store. FSNI

(and its nominated advisors and service providers) do not access or use Personal Information or Biometric Information from the FRT System for their own purposes.

FRT Stores may also engage contracted security guards, via third-party service providers, to assist with any actions taken in store in response to an FRT Alert that is confirmed as a match by two authorised FRT Store personnel. The engagement of such security guards is subject to the terms of the third-party service provider's services agreement with the FRT Store.

4.7 Disclosure of Personal Information and Biometric Information

Biometric templates cannot be accessed or extracted from the FRT System.

The FRT Stores do not share any information from their FRT System with any other Stores (including other FRT Stores) or upload any information from FRT System into any third party programs or applications.

Personal Information and Biometric Information held in the FRT System (but for the avoidance of doubt, not biometric templates) may be disclosed, in accordance with a FRT Store's banner privacy policy, as follows:

- (a) to authorised FRT Store personnel with a legitimate need-to-know, consistent with the purpose of collection or as otherwise required by applicable law;
- (b) to an individual, where a FRT Store receives a request from that individual whose Personal Information and Biometric Information is recorded in the FRT Watchlist (and the identity of the individual in question has been verified);
- (c) to law enforcement agencies, but only where compelled to do so by law;
- (d) FSNi and the FRT Store's service providers solely for the purpose of assisting the FRT Store with operating its FRT System. FSNi and FRT Stores take steps to ensure that these parties only use the information to perform their contractual functions for us (and not for any other purposes) and handle the information on our behalf in accordance with applicable privacy laws and confidentiality undertakings; and
- (e) to Vix Vizion, the FRT System provider, but only for support and maintenance services and subject to appropriate data security and confidentiality undertakings. Personal information and Biometric Information is not used by the FRT System provider or any other person to train the algorithms or models underlying the FRT System (or any other system).

4.8 Access to and correction of Personal Information and Biometric Information

Individuals (including a POI) may submit an access and/or correction request to the relevant FRT Store to review and correct any Personal Information and Biometric Information about them held in the relevant FRT Store's FRT System (including querying whether they are enrolled in the relevant FRT Store's FRT Watchlist).

Subject to the Privacy Act, access is granted once the identity of the requestor is verified. Information is provided in a manner that is deemed appropriate in light of the circumstances and a FRT Store's obligations under the Privacy Act and the Code.

4.9 Removal from FRT Watchlist

A Person of Interest may query their enrolment in the FRT Watchlist by submitting a removal request to privacy@foodstuffs.co.nz. The email request should set out: (i) the FRT Store the incident took place in; (ii) the date and time of the incident; (iii) what happened; and (iv) the reasons why their Personal Information and Biometric Information should be removed from the FRT System.

If a FRT Store receives such a removal request, authorised FRT Store personnel have the discretion, in limited circumstances, to remove a POI from the FRT Watchlist.

All FRT Stores must maintain a record of why a POI was removed from the FRT Watchlist, or why the request was denied. FSNI regularly monitors and audits a FRT Store's compliance with the FRT removal process.

All authorised FRT Store personnel receive training on the grounds underpinning the discretion to remove a POI from the FRT Watchlist and can request guidance from FSNI if they are unsure.

In addition to direct removal requests, enrolments in the FRT Watchlist are reviewed on a quarterly basis to determine whether a POI should be removed (e.g., for image quality issues, excessive false positives, bias or incorrect process etc.). Should any evidence of incorrect process, inaccuracy or bias be identified in an enrolment, that enrolment (including the image and biometric template) is immediately deleted from the FRT Watchlist and the relevant FRT Store personnel briefed and re-trained on the issues identified.

4.10 Misidentification process

FRT Stores have implemented a process for dealing with any misidentifications that take place. This includes practices and processes that are aligned with tikanga (in particular, tapu, mana, mauri, hau and utu) to ensure any misidentification is managed in a respectful and culturally appropriate way. Misidentified individuals are also given the option of having the matter resolved through a tikanga-Māori led approach.

All relevant authorised FRT Store personnel receive training on the misidentification process.

4.11 Further Review

FSNI and FRT Stores record performance data from the FRT System and will regularly review that data to assess whether: (A) the technical and operational settings of the FRT System remain appropriate; (B) the FRT System is effective at reducing incidents of Serious Harm; and (C) the use of the FRT System remains necessary for achieving the Purpose.

FSNI and FRT Stores intend that this PIA will be reviewed and updated on an annual basis unless there are changes in the use of the FRT System. Where there are changes in the use of the FRT System, this PIA will be reviewed and updated in light of those changes.