



# New Zealand



## Facial Recognition Technology Privacy Impact Assessment

April 2026



## 1. Project description

### 1.1 Background

Bunnings Limited (Bunnings) is the owner and operator of home improvement stores. Following a sustained increase in the recorded rates of violent, threatening, aggressive, and intimidating behaviour, incidents involving weapons, physical and verbal assault, racial and sexual harassment, high-value theft, and organised retail crime (serious harm), Bunnings proposes to use facial recognition technology (FRT) for the lawful purpose of:

- protecting the health, safety, and security of team members and customers; and
- reducing organised crime and high-value theft,

by proactively reducing the incidence of serious harm by repeat offenders in stores (Purpose).

Bunnings intends to use FRT in stores solely for the Purpose, subject to any necessary privacy safeguards, processes and protocols as outlined in this Privacy Impact Assessment (PIA) to ensure the use of FRT remains effective, safe and compliant with the Privacy Act 2020 (Privacy Act) and the Biometrics Processing Privacy Code 2025 (Code).

### 1.2 Purpose of this PIA

Foodstuffs North Island's trial of FRT has shown that FRT is effective in reducing serious harmful behaviours, like assault, violence, aggression and theft, in retail stores. An independent evaluator concluded that FRT reduced harmful behaviours in Foodstuffs North Island stores that took part in the FRT trial by an estimated 16%. The Office of the Privacy Commissioner (OPC) also found in its inquiry into Foodstuffs North Island's use of FRT (OPC Inquiry)<sup>1</sup> that "FRT made a substantial difference in reducing rates of serious recidivist crime in stores".<sup>2</sup>

Based on Foodstuffs North Island's trial results and the findings of the OPC Inquiry, Bunnings believes that the use of FRT will assist in reducing incidents of serious harm caused by repeat offenders in stores. Bunnings considers that its stores (and the environments that stores operate in) are comparable to the Foodstuffs North Island stores that trialled FRT in 2024. In particular, the operations of both businesses are largely overseen by frontline workers and members of the public are present in the form of customers and other visitors, all of whom can be exposed to serious harm.

While FRT has been shown to be effective in reducing harmful behaviour in a comparable retail setting, Bunnings acknowledges that there are privacy risks inherent in the use of FRT that will need to be identified and mitigated in Bunnings' specific use of FRT. Bunnings has undertaken this PIA to:

- a) Identify any privacy concerns and potential privacy risks arising from the use of FRT in stores for the Purpose; and
- b) Identify and provide effective strategies, processes and privacy safeguards to mitigate those risks and reduce them to an acceptable level.

## 2. Purpose of using FRT

### 2.1 The problem

Stores are experiencing a sustained, year-on-year, increase in serious harm. Between FY22 and FY25, serious harm in stores increased by 130%. Of the serious harm incidents that occurred in stores in FY25, 34% of all recorded incidents were committed by repeat offenders.

Data recorded by Bunnings on threatening events (as defined below) shows that:

- a) In FY22, 303 threatening events were recorded. In FY22, 26% of these were committed by repeat offenders;
- b) In FY23, the number of threatening events increased to 544 (of which 11 were threats of harm or death and 22 were physical assaults) – a 79.5% increase on the previous year. In FY23, 24% of these were committed by repeat offenders;
- c) In FY24, 634 threatening events (including 9 threats of harm or death and 29 physical assaults) were recorded – a 16.5% increase on the previous year. In FY24, 29% of these were committed by repeat offenders; and
- d) In FY25, the number of threatening events increased again to 697 (of which 8 were threats of harm or death and 32 were physical assaults). In FY25, 34% of these were committed by repeat offenders.

<sup>1</sup> See the OPC's "Inquiry into Foodstuffs North Island trial use of facial recognition technology" and the resulting report found at <https://www.privacy.org.nz/assets/DOCUMENTS/20250603-FRT-Inquiry-Report-A1082856.pdf>

<sup>2</sup> See OPC Inquiry report at [136].

“Threatening events” include aggressive behaviour, physical assault, events involving a weapon, intoxication, erratic behaviour, discriminatory behaviour, and sexual harassment that have taken place in stores and their surrounding premises (e.g., car parks). Any threatening event that has an element of theft or fraud is classified as additional unlawful behaviour in the record of the event by Bunnings.

As is the case in most (if not all) retail settings, theft is often a lead indicator for serious harm in stores. During FY25, 53.4% of theft loss at stores was attributed to repeat offenders.

Bunnings is left with few practical options to proactively mitigate the risk of serious harm by repeat offenders. To effectively address the serious harm caused by repeat offenders, Bunnings requires a solution that proactively and accurately identifies those offenders.

## 2.2 Methods attempted to address the problem

Bunnings has tried to address serious harm in stores by relying on a range of security measures. This includes relying on team members to review manual security alerts and identify repeat offenders. However, this approach is often imprecise and ineffective as it relies on team members remembering the images of individuals that are the subject of the security alerts.

Bunnings has also used, and continues to use, other methods, including using CCTV systems in stores, using automatic licence plate recognition technology in store car parks, and issuing trespass notices to reduce the serious harm caused by repeat offenders. However, Bunnings considers that these methods are not as effective as they are generally reactive and by the time action can be taken, serious harm has already occurred.

## 2.3 Alternative options for addressing the problem

Bunnings has also considered several alternative methods to proactively identify and respond to repeat offenders to reduce the reoccurrence of serious harm. Alternative methods include protecting stock with anti-theft devices and more team members. Again, these methods have not assisted in proactively identifying repeat offenders.

Overall, Bunnings considers that the methods currently used, and the alternative options considered, are not as effective as FRT in proactively identifying repeat offenders and reducing serious harm in stores.

## 2.4 The solution

Bunnings aims to ensure a safe environment for its team members at work and its customers while shopping. Given the rising rates of serious harm in stores, Bunnings will use FRT in stores solely for the Purpose.

While Bunnings has identified FRT as an option to reduce serious harm, it will continue to use other methods and processes (including those discussed above) to address serious harm in stores.

Details on how the FRT system will operate as set out below.

### **Imagus by Vix Vizion**

Bunnings will use the Vix Vizion, Imagus Facial Recognition Solution (FRT system). Vix Vizion is an Australian company that provides facial recognition and video analytics solutions.

Bunnings carried out due diligence on Vix Vizion, which included a structured assessment of Vix Vizion’s technology, security controls and privacy practices.

### **Accuracy**

The National Institute of Standards and Technology (NIST), an agency of the US Department of Commerce, has evaluated the accuracy and bias of the FRT system<sup>3</sup>. NIST found that the FRT system is highly accurate in processing “wild” images.<sup>4</sup> “Wild” images are those where the subject does not pose for the image e.g., images that are taken from CCTV footage.

The FRT system is a newer version of the FRT solution trialled by Foodstuffs North Island in New Zealand. The OPC Inquiry found the FRT solution trialled by Foodstuffs North Island to be professionally tested as suitable for operating “in the wild”.<sup>5</sup>

Bunnings will use several measures to mitigate the risk of inaccuracy or bias, including ensuring: *(cont.)*

<sup>3</sup> 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.

<sup>4</sup> <https://www.vixvizion.com/nist-report> [June 24, 2022]

<sup>5</sup> OPC Inquiry report at [183].

- a) all relevant team members receive training prior to implementation of the FRT system and on an ongoing basis following the implementation. This includes training on the concerns relating to privacy, inaccuracy and bias (including unconscious bias and discrimination), and the privacy safeguards, protocols and processes adopted by Bunnings;
- b) when the FRT system identifies a match between the facial image of an individual who has entered a store and the image of an offender enrolled in Bunnings' FRT watchlist (FRT watchlist), an alert is generated within the FRT system (FRT alert). All FRT Alerts will be verified as a match by three authorised and trained team members before any action is taken;
- c) the FRT system in each store will be calibrated to an accuracy level of 93%, meaning only matches with an accuracy rating of at least 93% will trigger an alert in the FRT system;
- d) the criteria for enrolment on the FRT watchlist will be strictly limited as set out in section 4.2; and
- e) this PIA and the operation of the FRT system will be reviewed and updated on a regular basis, including to ensure that:
  - (i) any issues relating to inaccuracy or bias that are identified in the course of using the FRT system are appropriately addressed; and
  - (ii) the technical and operational settings of the FRT system remain appropriate;
  - (iii) the FRT system is effective at reducing incidents of serious harm; and
  - (iv) the use of the FRT system remains necessary for achieving the Purpose.

### 3. Summary of Bunnings' assessment of proportionality

Given:

- a) the sustained increase in serious harm by repeat offenders in stores;
- b) the impact that serious harm caused by repeat offenders has on team members, customers and other people who enter stores;
- c) FRT will be used solely for the Purpose;
- d) The effectiveness of FRT in reducing the harmful behaviour of repeat offenders in comparable retail settings (as shown in Foodstuffs North Island's trial);
- e) the alternative methods currently used or considered by Bunnings are not as effective as FRT in reducing the rates of serious harm by repeat offenders;
- f) Bunnings can technologically segregate the FRT watchlist to the specific geographic region of the store (or stores) where the enrolled offenders have committed serious harm (as discussed in more detail below); and
- g) the clear public benefit to team members of a safer workplace, and to individuals who enter a store of a safer environment, and the clear private benefit to Bunnings of reduced stock loss resulting from theft by repeat offenders,

Bunnings considers that the benefits (both public and private) of using FRT for the Purpose outweigh any residual privacy risk that remains once the privacy safeguards, processes and protocols outlined in this PIA are implemented.

In addition, Bunnings has considered the impacts on Māori by engaging with an independent Māori digital sovereignty and tikanga expert. Based on this engagement, Bunnings has strengthened its compliance measures by committing to New Zealand-based data storage, clarified its operational processes and training to account for cultural risks, and enhanced procedures for managing any misidentification in a respectful and culturally appropriate way.

In considering and designing its proposed implementation of FRT, Bunnings conducted a stakeholder consultation process, which included commissioning independent customer and team research. The research indicates that customers support FRT when it is used transparently, for a specific safety purpose, and with strong safeguards. Support is strongest when people understand how the technology works, what it does not do, and how their information is protected.

Customers support FRT for serious harm and high-risk incidents - including weapons (74%), physical violence (73%), repeat theft (71%), intimidation (71%), and organised retail crime (70%). Support drops significantly for lower-level issues such as loitering or low-value shoplifting (50%).

Based on the above, Bunnings considers the use of the FRT system to be a necessary and proportionate solution for the Purpose, provided that the compliance measures (including from a Māori data sovereignty and tikanga perspective) outlined in this PIA are implemented.

## 4. Use of the FRT system

### 4.1 How will Bunnings inform the public about its use of FRT?

To ensure transparency and accessibility, Bunnings will inform people who visit a store about the use of FRT in several ways, including in-store, digital, and external channels.

To inform customers that a store is using FRT, each store will display large signage at entry points and smaller signs will be placed throughout the store. These signs will be in English and te Reo Māori. These signs will explain: (i) that FRT is in use in the store; (ii) the purpose for which FRT is used; and (iii) how individuals can obtain further information.

Bunnings will update its Privacy Policy to be clear:

- that Bunnings collects the biometric information and personal information described in section 4.3 through FRT; and
- how this information is used, stored, disclosed and how it can be accessed and/or corrected by an individual.

Stores will have printed information about FRT at the customer service front desk and with people greeters about FRT (including printed copies of Bunnings' Privacy Policy).

In addition:

- Customer information (print and digital) will be made available in-store and online.
- An infographic explaining how human oversight works in alerts and interventions will also be available online as a literacy accessibility option.
- Bunnings will make clear public announcements using its own channels and media about how and when FRT is implemented in stores, the purpose of FRT and how individuals can obtain more information.
- There will be a dedicated FRT webpage on the Bunnings website that will set out why and how Bunnings is using FRT in stores for the Purpose.
- Team members will be trained on responding to FRT-related queries.

### 4.2 How will Bunnings collect and use biometric information and personal information using the FRT system?

The FRT system will collect and assess FRT-dedicated camera footage of the facial images of all individuals who enter a store.

The FRT system will convert the facial images into binary code on the store's local server. The binary code is not humanly readable, is encrypted, and cannot be interpreted by another system or reverse engineered. The binary code is unique and only used for matching purposes – the binary code is referred to as a "biometric template".

The biometric template is compared with the templates of the facial images of offenders enrolled in the FRT watchlist. The FRT system will be calibrated to an accuracy level of 93%, meaning only matches with an accuracy rating of at least 93% will trigger an FRT alert.

If the FRT system does not identify the collected image as a match to an image enrolled in the FRT watchlist, then the collected image and related biometric template will be automatically and permanently deleted within 10 seconds of entering the FRT system.

The FRT system will not be integrated with any other systems or security platforms. This means that the biometric information and personal information in the FRT system will not be shared with or accessed by any other systems.

#### **FRT watchlist enrolment**

a) **Criteria** for enrolment on the FRT watchlist is an offender that:

- i) has either:
  - engaged in serious harm in a store (other than high value theft as described in (b) below) towards team members, customers or other people in the store; or
  - engaged in serious harm that is high value theft, being theft (or attempted theft) of goods with a combined value of \$2000 in one or more theft incidents (or attempts); or
  - re-entered a store in breach of a trespass notice, where that trespass notice was issued for serious harm (as described in (a) or (b) above) in a store; and
- ii) is not a minor or vulnerable person.<sup>6</sup>

<sup>6</sup> For the purpose of this PIA, Bunnings considers a vulnerable person to be a person who, because of their age, health, disability, mental distress, or other circumstances, may be at greater risk of harm or unfair treatment, and who authorised, trained team members reasonably determine should not be included on an FRT watchlist.

## b) Enrolment region

Enrolment onto the FRT watchlist will be based on the specific geographic region where the serious harm occurred – if an offender committed serious harm in a store in the North Island, they will be enrolled in the FRT watchlist against all stores located in the North Island and if an offender committed serious harm in a store in the South Island, they will be enrolled in the FRT watchlist against all stores located in the South Island.

## c) Enrolment retention periods

Different retention periods will be applied to the enrolment of an offender in the FRT watchlist depending on the nature of the offending. The enrolment retention periods are set out in section 4.5.

## d) Enrolment process

All enrolments on and changes to the FRT watchlist are made by authorised, trained team members following approval by a member of Bunnings' loss prevention leadership team. All team members involved in the enrolment process will be specially trained not to enrol images of minors or vulnerable persons

## e) Review of enrolments

Enrolments on the FRT watchlist will be regularly reviewed to determine whether an offender should be removed (e.g., for image quality issues, excessive false positives, inaccuracy, bias or incorrect process etc.). Should any evidence of incorrect process or inaccuracy or bias be identified in an enrolment, that enrolment (including the image and biometric template) will be immediately deleted from the FRT watchlist and the relevant team members briefed and re-trained on the issues identified

### 4.3 Types of biometric information and personal information involved

The FRT system, including the FRT watchlist, will collect and/or hold the following types of information:

#### a) Biometric information

- i) the facial information of all individuals that enter stores, as captured by dedicated FRT cameras;
- ii) biometric templates of the facial images referred to in (i) above; and
- iii) a description of the serious harm committed by an offender at the time of an incident (this is captured so that team members can take appropriate action should they need to approach or monitor an offender enrolled in the FRT watchlist in the future).

#### b) Personal information

- i) the name of the offender enrolled in the FRT watchlist (if known);
- ii) if applicable, the trespass notice ID; and
- iii) a security system reference number.

### 4.4 What happens if there is a FRT system match?

If the FRT system identifies a match between a collected facial image and the image of an offender enrolled in the FRT watchlist:

- a) the FRT system will generate an FRT alert within the FRT system;
- b) an email notification will be sent to authorised, trained team members;
- c) two authorised, trained team members will review the FRT alert and manually compare the image of the offender against the FRT alert image of the individual that has entered the store. If those two team members verify the match, they will notify a trained store leader in the relevant store;
- d) if the store leader also verifies the match, the store leader will coordinate, appropriate action based on safety and security protocols set by Bunnings;
- e) once the FRT alert is actioned / resolved, the alert will be updated to confirm the FRT system match and a description of the incident will be manually added to the FRT watchlist by one authorised, trained team member and verified by another;
- f) if the images in the FRT alert are not confirmed as reasonably identical by either of the two authorised, trained team members or the store leader, then one of the relevant authorised, trained team members will update the FRT alert to note that the FRT system match was not confirmed; and
- g) the FRT alert, which includes the collected image and related biometric template, will be automatically deleted from the FRT system 72 hours after the image enters the FRT system. Bunnings retains information relating to FRT system alerts (but not the collected image or the biometric template) for record keeping, review and auditing purposes.

## 4.5 Storage and retention of biometric information and personal information

All biometric information and personal information collected and/or held in the FRT system will be securely stored on servers located in New Zealand.

Where no match is identified by the FRT system, the facial images and biometric templates of individuals entering a store are automatically and immediately (within 10 seconds of when it enter the FRT system) deleted.

Where a match is identified by the FRT system, then the FRT alert data will be automatically deleted from the FRT system 72 hours after the collected facial image enters the FRT system (regardless of whether the match is confirmed or not by authorised, trained team members).

Where a serious harm incident occurs, authorised, trained team members will manually enrol facial images of the offender collected by the store's CCTV system into the FRT watchlist as discussed above.

Biometric information and personal information of an offender will be stored in the FRT watchlist for different retention periods depending on the nature of the offending. The relevant retention periods are:

- a) High-value theft - up to 6 months;
- b) Violence or harassment - up to 12 months;
- c) Weapons-related incidents - up to 24 months;
- d) Organised retail crime (multiple incidents by the same person) - up to 12 months; and
- e) For any other act(s) of serious harm that does not fit into (a) to (d) above, a time period as reasonably determined by authorised, trained team members, which will be no more than 24 months

On expiry of these time periods, the enrolment (including the biometric information and personal information of the relevant offender) is automatically and permanently deleted from the FRT system.

## 4.6 Security of biometric information and personal information

All biometric information and personal information collected and/or held in the FRT system will be subject to strong data security and access controls, including strict user access permissions, multi-factor authentication, encryption, secure logging and monitoring, and regular security testing.

All authorised, trained team members will receive applicable training, and will be made aware of, and contractually commit to, applicable data security and confidentiality requirements.

Nominated advisors and service providers will not have general access to the biometric information held in the FRT systems unless otherwise directly provided by Bunnings (and only where the contracts with those advisors and service providers include appropriate confidentiality, privacy and data security undertakings).

- check what information is being collected to ensure compliance with FRT operational protocols; and
- review FRT logs to monitor access to the FRT system and biometric information to ensure the use is consistent with FRT operational protocols.

## 4.7 Disclosure of biometric information and personal information

Biometric templates cannot be viewed or removed from the FRT system.

Biometric information and personal information held in the FRT system (but, for the avoidance of doubt, not biometric templates) may be disclosed, in accordance with Bunnings' Privacy Policy, as follows:

- to relevant authorised team members with a legitimate need-to-know for the Purpose or as otherwise required by applicable law;
- to an offender enrolled in the FRT watchlist, where Bunnings receives an access request from that offender (and the identity of the offender in question has been verified);
- where Bunnings receives a request from Police for information about an offender enrolled in the FRT watchlist, the request will be managed by Bunnings' Privacy and Legal team. Police will not be provided biometric information and personal information held in the FRT system unless Bunnings is required by law to disclose that information;
- to the system supplier (Vix Vizion) and Bunnings' third-party service providers (including other members of the Bunnings group) solely to provide support and maintenance in relation to the FRT system. In each case, the information shared will be limited to what is strictly necessary and will be subject to appropriate confidentiality and security obligations.

Biometric information and personal information will not be used by any person to train the algorithms or models underlying the FRT system or any other system.

## 4.8 Access to and correction of biometric information and personal information

The signs, tools and channels described in section 4.1 will refer individuals to Bunnings' Privacy Policy for more information on an individual's right to request access to/correction of their biometric information (and personal information) held by the FRT system.

Individuals (including offenders enrolled in the FRT watchlist) can query if they are enrolled on the FRT watchlist by submitting a request to Bunnings to access and/or correct their biometric information and personal information held in the FRT system (if any).

Subject to the Privacy Act, access will only be granted once the identity of the requestor is verified. Information will be provided in a manner that is deemed appropriate and in accordance with Bunnings' obligations under the Privacy Act and the Code.

Bunnings team members will refer personal information access and correction requests to Bunnings' Privacy Officer.

## 4.9 Misidentification process

Bunnings will implement a process to address any misidentifications. This process will include practices and procedures aligned with tikanga (in particular, tapu, mana, mauri, hau, and utu) so that any misidentification is managed respectfully and in a culturally appropriate way. All relevant Bunnings team members will be trained on the misidentification process as part of the FRT training.

## 4.10 Process for appealing / disputing enrolment on the FRT Watchlist

Bunnings will implement a process to deal with requests to remove an offender from the FRT watchlist. Bunnings' Privacy Officer and all relevant authorised team members will receive FRT training on the appeal / disputes process.

As part of the design of its proposed FRT implementation, Bunnings undertook a stakeholder consultation process that included internal team engagement and commissioning independent customer research to understand customer and team member views, concerns, and expectations in relation to the use of FRT.

## 5. Consultation process

The results show strong public backing for FRT in retail environments, with net approval ranging from 79–83 per cent and rising to 85–87 per cent once customers understand how the technology works and how their data is protected. Support was highest when FRT was used transparently for specific safety reasons, such as handling weapons, violence, repeat theft, intimidation, and organised retail crime, whereas customers were less supportive of less serious issues like loitering or minor shoplifting.

The research also found that most customers are willing to accept FRT when it clearly reduces harm. 93 per cent support use that achieves more than a 10 per cent reduction in incidents, and 64 per cent are open to it even for smaller improvements. Only 7 per cent oppose it on principle.

Team members viewed FRT as a valuable safety tool, where its use is supported by clear guidance on their individual responsibilities, structured training on how FRT works, and access to adequate support.

The research outcomes are consistent with those of Foodstuffs North Island.

Bunnings engaged a Māori data expert for advice on the potential implications for Māori people. This engagement reinforced the importance of tikanga-aligned practice, cultural respect, and strong data governance, particularly given the significance of tā moko (traditional facial tattoos) and whakapapa (traditional Māori genealogy).

Bunnings will 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.

## 6. Further review

Bunnings intends that this PIA will be reviewed and updated annually unless there are changes to 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.

