CHOICE

24 June 2022

Office of the Australian Information Commissioner
Via email: enquiries@oaic.gov.au

Dear Commissioner,

Kmart, Bunnings and The Good Guys' use of facial recognition technology in store

I write in regard to Kmart, Bunnings and The Good Guys' practices related to the notification of collection, collection and use of sensitive information obtained through facial recognition technologies in their retail stores.

CHOICE asks you to launch a Commissioner-initiated investigation under s.40(2) of the *Privacy Act 1988* ('**the Act**') for breaches of the Act by Kmart, Bunnings and The Good Guys ('**the retailers**').

Specifically, we request an investigation into the retailers' compliance with Australian Privacy Principles ('**APPs**') 1, 3 and 5, with respect to the requirements that these organisations:

- APP 1.3 – have a clearly expressed and up-to-date APP Privacy Policy about how the entity manages personal information;
- APP 3.3(a)(ii) – only collect 'sensitive information' where it is reasonably necessary;
- APP 3.3(a) – only collect 'sensitive information' with consent;
- APP 3.5 – only collect personal information by lawful and fair means; and
- APP 5.1 – take reasonable steps to notify an individual of the APP 5 matters or to ensure the individual is aware of those matters.

CHOICE is concerned that the retailers' practices related to their use of facial recognition technology pose significant risks to individuals. The social and economic risks include invasion of privacy, misidentification, discrimination, profiling and exclusion, as well as vulnerability to cybercrime through data breaches and identity theft.

Key issues

CHOICE has concerns with the retailers' practices for two main reasons:

1. **Lack of notice and consent in the collection of sensitive information.** The retailers' use of online privacy policies and small signage in store as the key mechanisms to provide notice and obtain consent from individuals about the collection of their sensitive information is insufficient and non-compliant.

2. **The stated business purpose is disproportionate to the privacy harms posed to individuals.** The retailers' large scale collection and use of their customers' sensitive information significantly invades the privacy of its customers. It is a disproportionate response to the risk of theft and anti-social behaviour in stores.

CHOICE's investigation

In April 2022, CHOICE commenced an investigation into the use of facial recognition technology in major Australian retail stores. CHOICE requested information from 25 leading Australian retailers on their use of facial recognition technology (**Appendix A**) and analysed their privacy policies, available online (**Appendix B**).

Based on the responses and analysis, CHOICE identified that Kmart, Bunnings and The Good Guys are collecting and using their customers' sensitive information via the use of facial recognition technology. More specifically, the retailers are collecting sensitive biometric data known as a 'faceprint' through their facial recognition technology systems.

CHOICE staff visited the retail stores to identify notices that indicated to customers both the use of facial recognition technology and the collection and use of sensitive information. Evidence of these notices can be found at **Appendix C**.

On 15 June 2022, CHOICE published its findings in an article entitled "Kmart, Bunnings and The Good Guys using facial recognition technology in stores".[1] The article received widespread media coverage indicating that the Australian community was not aware of the retailers' practices in relation to the use of facial recognition technology in store. Kmart, Bunnings and The Good Guys issued public statements in response (**Appendix D**).

[1]Blakkarly, J 2022, 'Kmart, Bunnings and The Good Guys using facial recognition technology in store', *CHOICE*, 15 June, www.choice.com.au/facialrecognition

Public sentiment and community expectations

CHOICE conducted a nationally representative survey between March and April 2022, asking more than 1000 Australians about their awareness of facial recognition technology.[2] The survey found:

- 76% of respondents didn't know retailers were using facial recognition.
- 83% of respondents think retail stores should be required to inform customers about the use of facial recognition before they enter the store.
- 78% expressed concern about the secure storage of faceprint data.
- 65% are concerned about stores using the technology to create profiles of customers that could cause them harm.

The findings indicate that a majority of Australians are either unaware or not supportive of the use of facial recognition technology in retail settings.

Scope of conduct in relation to the Privacy Act

The information at issue is 'personal information'

CHOICE asserts that facial images, and faceprints generated from them, are 'about' individuals, who are 'reasonably identifiable', under the definition of 'personal information' in the Act.[3]

Even if the retailers do not attempt to use the facial recognition technology to make an identification of any particular customer, in the sense of finding out their name, CHOICE maintains that the facial images and faceprints at issue constitute 'personal information' for the purposes of the Act.

The retailers' conduct is very similar to that examined in your Determination against 7-Eleven.[4]

The objective of facial recognition technology is to identify individuals, at least in the sense of being able to distinguish one person from another, with a high degree of confidence. CHOICE notes that your Determination against 7-Eleven states that even though individuals could not necessarily "be identified from the specific information being handled", the information was still 'reasonably identifiable' in law, because the faceprints were used as an 'identifier' which "enabled an individual depicted in a faceprint to be distinguished from other individuals whose faceprints were held on the Server".[5]

---

[2] CHOICE Consumer Pulse March 2022 is based on a survey of 1034 Australian households. Quotas were applied for representations in each age group, as well as genders and location, to ensure coverage in each state and territory across metropolitan and regional areas. Fieldwork was done between 22 March and 7 April 2022.

[3] *Privacy Act 1988* (Cth) pt II div 1. s6, available at https://www.legislation.gov.au/Details/C2022C00135

[4] *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd* [2021] AICmr 50, available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/50.html

[5] *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd* [2021] AICmr 50, at [38], available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/50.html

The information at issue is 'sensitive information'

Section 6 of the Act defines 'sensitive information' as including: "biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or … biometric templates".

CHOICE notes that in your Determination against Clearview AI, the Office of the Australian Information Commissioner ('**OAIC**') found that:

> "'Biometric information' and 'biometric templates' are not defined in the Privacy Act.
>
> 'Biometrics' encompass a variety of different technologies that use probabilistic matching to recognise a person based on their biometric characteristics. Biometric characteristics can be physiological features (for example, a person's fingerprint, iris, face or hand geometry), or behavioural attributes (such as a person's gait, signature, or keystroke pattern). These characteristics cannot normally be changed and are persistent and unique to the individual.
>
> A 'biometric template' is a digital or mathematical representation of an individual's biometric information that is created and stored when that information is 'enrolled' into a biometric system. Machine learning algorithms then use the biometric template to match it with other biometric information, for verification, or to search and match against other templates within a database, for identification.
>
> 'Biometric systems' scan, measure, analyse and recognise a particular and unique biometric (such as facial features), physical, biological and behavioural traits and characteristics to identify a person".[6]

CHOICE also notes that you determined that both the raw image and the vector generated from it are 'biometrics' and thus 'sensitive personal information':

> "I am satisfied that, consistent with the definition of 'biometrics' … Scraped and Probe Images show physiological features of an individual's face. The vectors generated from these images record information about measurements of an individual's facial characteristics. For each kind of information, the recorded characteristics pertaining to an individual are persistent, cannot normally be changed and are unique to that individual. For these reasons, Scraped and Probe Images collected by the respondent, and the vectors generated from these images, are 'biometric information'".[7]

[6] *Commissioner initiated investigation into Clearview AI, Inc*. [2021] AICmr 54, at [121]-[124]; available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/54.html
[7] *Commissioner initiated investigation into Clearview AI, Inc.* [2021] AICmr 54, at [137]; available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/54.html

Similar reasoning was applied in the 7-Eleven case.[8]

The conduct at issue involves a 'collection'

CHOICE notes that in the Clearview AI case, you found that the vectors generated from images were 'collected'. The decision found that 'collects' includes collection by 'creation' which may occur when information is created with reference to, or generated from, other information the entity holds".[9] CHOICE believes that the faceprints generated from the facial recognition systems used by the retailers will likewise constitute a 'collection by creation', which must therefore comply with APP 3.

After CHOICE's investigation, Bunnings publicly claimed that it does not 'collect' personal information because the information is 'not retained'.[10] However, CHOICE notes that the Bunnings Privacy Policy (**Appendix B**) actually states that they do 'collect' this information:

> *"The types of personal information that we may collect about you includes:*
> - *images from facial recognition software"*

CHOICE asserts that even a transient collection, such as images stored only briefly, will constitute a 'collection' for the purposes of APPs 3-5.[11]

Potential breaches of the Act - APP 1

Clearly expressed and up-to-date APP Privacy Policy

The retailers' privacy policies (**Appendix B**) do not clearly express how the entities manage personal, including sensitive, information obtained through use of facial recognition technologies.

CHOICE made multiple requests for information to the retailers regarding how sensitive information is collected, held, used and destroyed, as we could not identify how these processes were managed in the retailers' privacy policies. Bunnings was the only retailer who responded to our requests for information during the investigation.

CHOICE is concerned that the retailers were not forthcoming on how they manage sensitive information obtained through facial recognition technologies. The difficulties that CHOICE, Australia's largest consumer organisation, faced in obtaining such information indicates a reluctance by the retailers to be clear, transparent and upfront about their privacy practices.

---

[8] *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd* [2021] AICmr 50, at [49], available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/50.html
[9] *Commissioner initiated investigation into Clearview AI, Inc.* [2021] AICmr 54, at [74], available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/54.html
[10] See a history of correspondence at https://www.efa.org.au/2022/06/16/australian-retailers-using-face-surveillance/
[11] *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd* [2021] AICmr 50 at [65], available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/50.html

The inadequately expressed privacy policies in combination with the retailers' unwillingness to provide information on how they manage sensitive information acts as a barrier to individuals seeking to understand how their sensitive information is managed by the retailers.

Potential breaches of the Act - APP 3

Reasonably necessary collection of sensitive information

The collection of any type of personal information, no matter how benign, must be reasonably necessary. Under APP 3, collecting personal information because it will be "helpful, desirable or convenient" is not enough; an entity's collection of personal information must be "reasonably necessary" for one of the organisation's "functions or activities".[12]

CHOICE notes that this test involves consideration as to whether the impact on individuals' privacy is "proportionate to a legitimate aim sought".[13] In the case of 7-Eleven, while the OAIC noted that "implementing systems to understand and improve customers' in-store experience" was a legitimate aim of the business, the collection of biometric templates was not a proportionate way to achieve that aim.[14]

In other words, the risk posed to the individuals must be weighed against the business objectives, and serious consideration must be applied to determining whether those objectives could be achieved in a less privacy-invasive manner.

CHOICE asserts that the retailers' collection of sensitive information from its customers is not reasonably necessary for the stated purpose of 'loss prevention or store safety purposes' under APP 3.4(b)[15] (refer **Appendix B**).

We maintain that there are other less invasive technologies such as CCTV that would achieve the same business goals of loss prevention and store safety. The use of facial recognition technology by the retailers poses a disproportionate privacy risk to individuals entering the store due to the sensitive nature of information collected and used.

Risks associated with the collection and use of sensitive information through facial recognition technology include social and economic harms such as invasion of privacy, misidentification, discrimination, profiling and exclusion. In addition, data collected by the retailers could be vulnerable to cybercrime such as data breaches and identity theft. We contend that these harms

[12] *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd* [2021] AICmr 50, at [58], available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/50.html
[13] *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd* [2021] AICmr 50, at [59], available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/50.html
[14] *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd* [2021] AICmr 50, at [102], available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/50.html
[15] APP 3.4(b) - taking appropriate action in relation to suspected unlawful activity or serious misconduct.

could be minimised through use of other less invasive technologies, which do not involve the collection or use of sensitive information such as faceprints.

CHOICE therefore asserts that any benefit to the retailers is disproportionate to, and fails to justify, "the potential harms associated with the collection and handling of sensitive biometric information", as outlined in your Determination against 7-Eleven.[16]

Collection of sensitive information with consent

When collecting sensitive information, APP 3.3(a) requires that organisations obtain the consent of every individual, unless an exception applies.

None of the exceptions, such as those listed at s.16A of the Act, apply to the retailers' practices that are the subject of this complaint. The test for meeting the s.16A exception uses the phrase "necessary" rather than "reasonably necessary", suggesting a higher threshold for an exception to be applied. CHOICE maintains that general claims about "loss prevention or store safety purposes" do not reflect a situation that is serious, immediate and/or targeted such as to justify the use of facial recognition on all customers entering a store as "necessary".[17]

CHOICE asserts that the retailers have not sought their customers' express consent before handling their sensitive information.

Seeking express consent for the collection of sensitive information is critical "given the greater privacy impact this could have."[18] Express consent should be given explicitly, either orally or in writing, for example through a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement.[19] CHOICE contends that the retailers did not seek oral or written consent from customers before their sensitive information was handled.

Equally, CHOICE asserts that the retailers have not obtained a valid consent from every individual whose sensitive information is being collected.

In order to be valid, consent "must be freely given, specific, unambiguous, and informed".[20] In particular, CHOICE notes that you have stated that "consent is not freely given when the provision of service is conditional on consent to personal information handling that is not necessary for the provision of the service";[21] and that consent will only meet the 'voluntary' test

---

[16] *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd* [2021] AICmr 50, at [105], available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/50.html

[17] Item 2 in the Table to s.16A allows for collection of personal information if "(a) the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in; and (b) the entity reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter".

[18] Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines*, Version 1.3, July 2019, para B.41.

[19] Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines*, Version 1.3, July 2019, para B.36

[20] Office of the Australian Information Commissioner, "Privacy Act Review Issues Paper submission", 14 December 2020, part 5.18; available at https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/

[21] Office of the Australian Information Commissioner, "Privacy Act Review Issues Paper submission", 14 December 2020, part 5.42; available at https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/

"if an individual has a genuine opportunity to provide or withhold consent".[22] Factors relevant to deciding whether consent is voluntary include the alternatives open to the individual.[23]

CHOICE notes that in the 7-Eleven case, similar to the retailers at issue here, the retailer had notices outside its stores. 7-Eleven argued that "if a customer did not consent to the use of this technology, the customer could elect to not enter the store".[24]

However CHOICE notes that you found that customers had not consented. Your ruling found that "consent may not be implied if an individual's consent is ambiguous or there is reasonable doubt about the individual's intention".[25]

CHOICE believes that the same factors are at issue with these retailers. The retailers cannot infer consent simply because they provided customers with notice of a proposed collection, use or disclosure of personal information. Customers may not have seen the notices (see '**Notice obligations**' below), and even if seen and read, may not have understood the implications, and thus we question whether any agreement was 'informed'. CHOICE asserts that customers' silence cannot be taken as consent. As a result, there is reasonable doubt about each individual's intention.[26]

Further, the 'voluntary' element is missing, as customers have no alternative to conduct their shopping without being subject to facial recognition.

The capacity of some customers, such as children, to be able to provide an informed consent about the collection of their sensitive information must also be questioned.

Collection of personal information by lawful and fair means

APP 3.5 requires organisations to collect personal information only by lawful and fair means. CHOICE suggests that an 'unfair' means of collection could include the use of facial recognition on customers which they would not expect.

CHOICE notes that in your Determination against Clearview AI, you stated that: "a 'fair means' of collecting information is one that … is not unreasonably intrusive".[27]

CHOICE asserts that the retailers have not collected personal, including sensitive, information by fair means. We believe the use of facial recognition technology in store to collect sensitive

[22] Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines*, Version 1.3, July 2019, para B.43.
[23] Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines*, Version 1.3, July 2019, para B.44.
[24] *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd* [2021] AICmr 50 at [88], available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/50.html
[25] *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd* [2021] AICmr 50 at [93], available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/50.html
[26] Office of the Australian Information Commissioner, *Australian Privacy Principles guidelines*, Version 1.3, July 2019, para B.39.
[27] Commissioner initiated investigation into Clearview AI, Inc. [2021] AICmr 54, at [168], available at http://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2021/54.html

biometric data is unreasonably intrusive. Equally, the retailers have been collecting personal information covertly without the knowledge (let alone consent) of customers.

Potential breaches of the Act - APP 5

Notice obligations

CHOICE maintains that the retailers have not provided sufficient notice to their customers regarding the collection and use of sensitive information in their privacy policies and signage in store.

The retailers have included information on the use of facial recognition technology in their privacy policies to notify customers of its use. These privacy policies are available on the retailers' websites (refer **Appendix B**). CHOICE finds issue with this practice as the privacy policy available online is divorced from the experience of shopping in store. It is not common practice for customers to search online and read the retailers' privacy policies while in physical retail settings. As a result, the online privacy policy does not provide sufficient notice to individuals about the collection and use of sensitive information in store.

The retailers have also indicated the use of facial recognition technology in store through signage at the entrance of their stores (refer **Appendix C**). This signage is equally insufficient in notifying customers of the collection and use of sensitive information, as the signs do not expressly state that facial recognition technology is used to collect sensitive biometric information and for what purpose. For example, Kmart's notice to customers states: "*This store has 24 hour CCTV coverage, which includes facial recognition technology.*"

CHOICE notes that in the 7-Eleven case, similar to the retailers at issue here, the retailer had signs outside its stores. In your Determination, you found the signs insufficient to meet the requirements of APP 5.

CHOICE maintains that the signage used is insufficient to actually achieve 'notice' to customers. The widespread media coverage of CHOICE's investigation and the investigation's 'newsworthiness' indicated to CHOICE that members of the community were not aware of the retailers' practices.

Equally, CHOICE's nationally representative survey found that less than 1 in 10 people in the Australian community were aware of the use of facial recognition technology by the three retailers. The survey asked Australians which retailers they believed currently used facial recognition technology. For Bunnings only 8% of respondents believed that facial recognition technology was being used, with Kmart and The Good Guys at 7% and 6% respectively (refer **Table 1**).

Table 1: CHOICE Consumer Pulse March 2022: Public understanding of the use of facial recognition technology in retail settings.

Q. And which of the below, if any, do you believe currently use facial recognition technology?	
Retailer	**%**
Bunnings	8
Kmart	7
The Good Guys	6

We maintain that due to the sensitivity of the personal information being collected, the retailers should have taken more rigorous measures to ensure that individuals were made aware of the retailers' practices.

Desired outcomes

Australian retailers are increasingly adopting new and emerging technologies both in their physical and online stores. There are significant risks to an individuals' privacy, as well as risks to their social and economic wellbeing associated with such technologies.

CHOICE urges you as Commissioner to investigate this matter further and consider taking enforcement action against Kmart, Bunnings and The Good Guys for failure to meet their obligations under the Act.

For further information, please contact us on 02 9577 3376 or via apereira@choice.com.au.

Yours sincerely,

Amy Pereira
Senior Campaigns and Policy Adviser
CHOICE

Appendix A: Questions posed to 25 major Australian retailers

CHOICE questions - facial recognition in retail stores
5 messages

[redacted] Wed, Apr 27, 2022 at 11:14 AM
To: media@bunnings.com.au

Hi

CHOICE, Australia's largest consumer organisation, is conducting an investigation into the use of digital tracking technologies and facial recognition in retail stores. We would appreciate your assistance answering the following questions about your business(es):

Bunnings

Please respond by Friday 13 May 2022.

1. Do you use any kind of facial recognition technology in your retail stores? Or do you use any kind of object detection, face detection, facial identification, facial tracking, smart cameras or any other kind of visual tracking technology in your retail stores? **Please describe it in simple terms.**

If yes:

1. For what purposes do you use the technology?
2. What kinds of data are collected by the technology, including personal and/or sensitive data?
3. How is this data stored and for how long is it kept?
4. Please list, in detail, any third parties that you share the data with, including data partners, data brokers, marketing affiliates and other third parties.
5. How do you inform your customers about the use of this technology? Please provide examples of any communication materials.
6. Have any customers raised concerns regarding your use of this technology?

Thank you and feel free to contact me if you have any questions
kind regards

Appendix B: Retailers' privacy policies

Bunnings

Bunnings' privacy policy[28] includes two mentions of the use of facial recognition technology in store:

Collection of personal information

1. Personal information is information that identifies you or from which you may reasonably be identified. The types of personal information that we may collect about you includes:
    - images from facial recognition software

Use and disclosure of personal information

4. We use and disclose your personal information in connection with carrying on our business (including to provide products and services to you and relating to our involvement in loyalty schemes that we participate in) and in some circumstances for the businesses of the Wesfarmers group of companies.

5. We may use your personal information:
    - in the case of images from facial recognition software, for loss prevention or store safety purposes;

Kmart

Kmart's privacy policy[29] includes two mentions of the use of facial recognition technology in store:

Collection of personal information

1. The types of information that we collect about you could include:
    - images from facial recognition software;

Use and disclosure of personal information

3. We use and disclose your personal information in connection with carrying on our business, (including to provide products and services to you and relating to our involvement in loyalty schemes that we participate in) and in some circumstances for the businesses of the Wesfarmers group of companies.

4. We may use your personal information to:

[28] Bunnings Privacy Policy 2022, available at https://www.bunnings.com.au/policies/privacy-policy
[29] Kmart Privacy Policy 2022, available at https://www.kmart.com.au/privacy-policy/

- in the case of images from facial recognition software and body cameras, for loss prevention or store safety purposes;

The Good Guys

The Good Guys' privacy policy[30] includes two mentions of the use of facial recognition technology in store:

Why does The Good Guys collect, hold, use and disclose personal information?

The Good Guys collects, holds, uses and discloses personal information for a number of purposes connected with our business operations, which include:

- carrying out day to day surveillance of our stores for operational, security and customer experience purposes. Our cameras may use facial and feature recognition technology to capture an image of an individual's face, features and clothing and to track an individual through the store. Such images may be retained and used by us to identify an individual on future visits to our stores. Such surveillance is strictly for the purposes of security and theft prevention and managing/improving customer experience at our stores.

What personal information does The Good Guys collect?

The kinds of personal information we collect or which we may hold about you may include:

- video and audio surveillance and recording of you (including facial and feature images) when you visit one of our stores or pick up goods from a collection area.

[30] The Good Guys Privacy Policy 2022, available at https://www.thegoodguys.com.au/privacy-policy

Appendix C: Notification of collection of personal information

Image 1: Sign outside Kmart, Marrickville, NSW

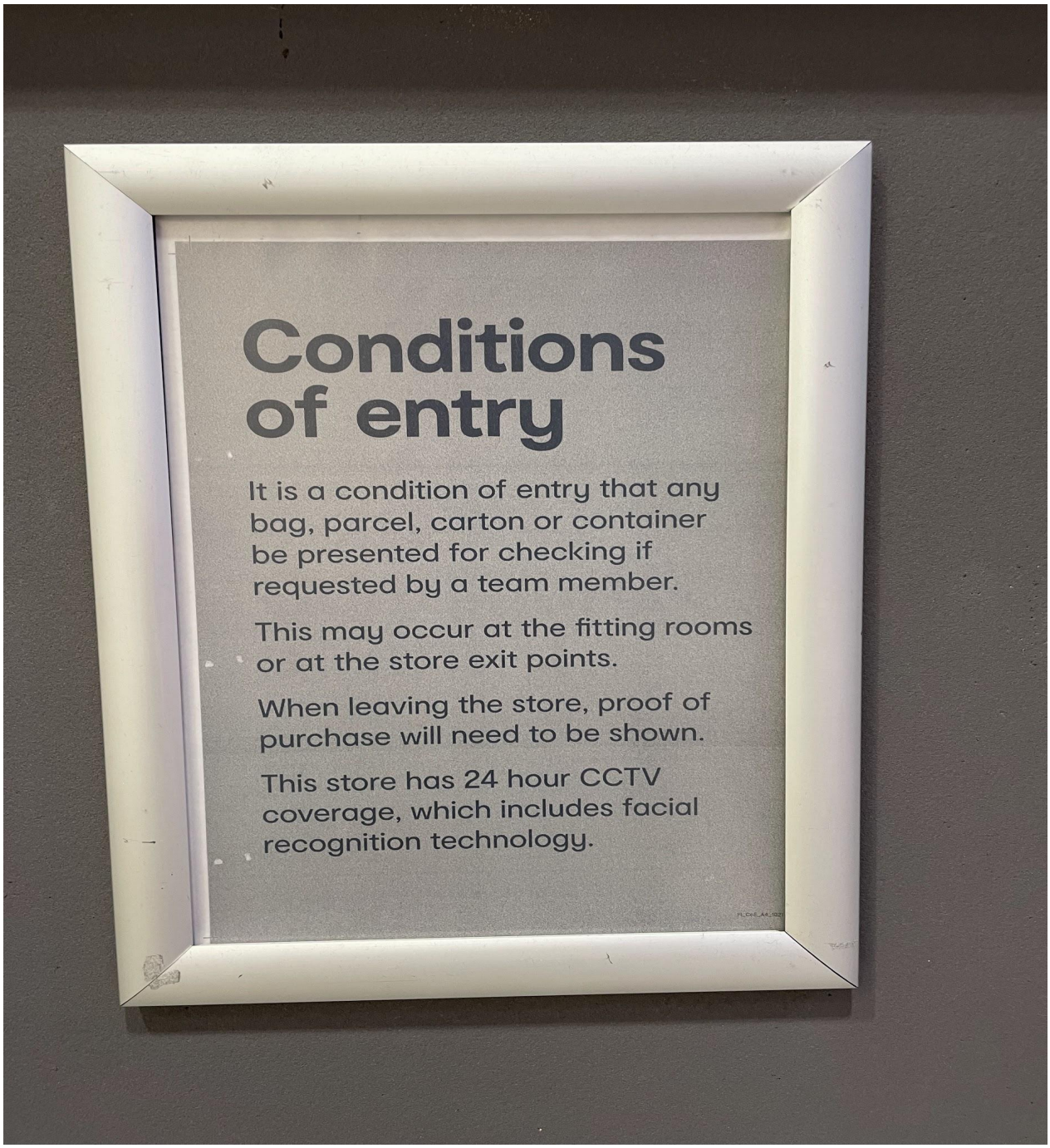

Image 2: Sign outside Bunnings, Alexandria, NSW

Appendix D: Public response from retailers

Statement from Kmart Spokesperson:

At Kmart we are trialling facial recognition in a small number of stores for the limited purposes of safety and loss prevention (such as reducing refund fraud).

We are committed to keeping personal information private and protected in compliance with privacy law.

We make our customers aware of facial recognition through our conditions of entry signage in participating stores and through our Kmart privacy policy.

Statement from Simon McDowell, Bunnings Chief Operating Officer:

We are disappointed by CHOICE's inaccurate characterisation of Bunnings' use of facial recognition technology in selected stores. This technology is used solely to keep team and customers safe and prevent unlawful activity in our stores, which is consistent with the Privacy Act.

In recent years, we've seen an increase in the number of challenging interactions our team have had to handle in our stores and this technology is an important tool in helping us to prevent repeat abuse and threatening behaviour towards our team and customers.

There are strict controls around the use of the technology which can only be accessed by specially trained team. This technology is not used for marketing, consumer behaviour tracking, and images of children are never enrolled.

We let customers know if the technology is in use through signage at our store entrances and also in our privacy policy, which is available via the homepage of our website.

Statement from The Good Guys:

The Good Guys is trialling in two stores the use of a new CCTV system that can use face and feature recognition technology. This technology is used solely for the purposes of loss prevention and the safety of our store team members and customers. We let our customers know the technology is in use in these two stores through our store entrance signage, and in our privacy policy that is available on our website.