Electronic Frontiers Australia Inc.
ABN: 35 050 159 188
W www.efa.org.au
E email@efa.org.au
@efa_oz

Office of the Australian Information Commissioner
GPO Box 5218
Sydney NSW 2001

22 June 2022

By online form

Dear Commissioner,

RE: Australian Retailers Using Facial Recognition

The undersigned groups wish to formally complain about the reported use of facial surveillance technologies by Australian retailers, as first reported by Choice on 14 June 2022[1].

We have approached the retailers and are not satisfied with their responses thus far. They do not appear to understand the technology they have deployed, nor the broader implications for society. They also appear to be fundamentally mistaken about the operation of privacy law.

We had hoped that the Commissioner's ruling in *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd* [2021] AICmr 50 (**the 7-Eleven matter**) would provide sufficient clarity to organisations considering the use of facial surveillance technology. Alas, it appears not.

We urge the Commissioner to quickly and definitively rule on this matter so that, as we believe, there can be no doubt that this kind of privacy intrusion is not permitted under the law, and that it has no place in Australian society. A delay in deciding this matter will allow the privacy harms to continue, affecting a great number of Australians.

We also urge the Commissioner to use its financial penalty powers so that there is a clear disincentive for organisations to consider ignoring privacy law in the way the retailers have done here.

Our complaint is further detailed below.

Yours sincerely,

Justin Warren	Lizzie O'Shea	David Vaile
Chair	Chair	Chair
Electronic Frontiers Australia	Digital Rights Watch	Australian Privacy Foundation

[1] 'Kmart, Bunnings and The Good Guys Using Facial Recognition Technology in Stores', *CHOICE* (14 June 2022) <https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/kmart-bunnings-and-the-good-guys-using-facial-recognition-technology-in-store>.

Co-signing Organisations

About EFA

Established in January 1994, EFA is a national, membership-based, not-for-profit organisation representing Internet users concerned with digital freedoms and rights.

https://www.efa.org.au/

About Digital Rights Watch

Digital Rights Watch is a national not-for-profit organisation defending human rights and freedoms online, so that the connection and creativity can flourish.

https://digitalrightswatch.org.au/

About the Australian Privacy Foundation

Established in July 1987, the Australian Privacy Foundation (APF) is the nation's foremost independent civil society body concerned with community data protection, privacy, and information security expectations. APF leads the struggle to defend the right of people to control their personal information, protect it from abuse and be free of unjustified intrusion.

https://privacy.org.au

Complaint - Australian Retailers Using Facial Recognition

Reporting by Choice[2] has revealed that major Australian retailers including Bunnings, Kmart and The Good Guys (the **Retailers**) are using facial recognition technology in some of their retail outlets.

Bunnings has advised Electronic Frontiers Australia (**EFA**) that the alleged purpose of the use of this technology is, in combination with CCTV surveillance, to "support the safety of our team and customers against repeat violent or threatening behaviour, and to prevent unlawful behaviour in ... stores"[3].

Representations from Bunnings to the EFA[4] suggest that Bunnings is scanning *all* customers in stores using this technology, and using facial recognition to compare customer 'faceprints' to a list of faceprints of banned customers to enable 'action' to be taken. It is unclear what actions may be taken.

We believe that the current use of facial recognition systems by the Retailers constitute a breach of the Australian Privacy Principles. Our reasoning is set out below.

Collection of 'sensitive information'

According to Choice's report, the Retailers are using facial recognition technology to create 'faceprints' from CCTV footage.

We note that the following are included in the definition of 'sensitive information' in s6 of the Privacy Act 1988:

---

[2] Ibid.

[3] Electronic Frontiers Australia, Inc, 'Australian Retailers Using Face Surveillance' (16 June 2022) <https://www.efa.org.au/2022/06/16/australian-retailers-using-face-surveillance/>.

[4] Ibid.

(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or

(e) biometric templates.

We note the Information Commissioner's finding in *Commissioner initiated investigation into 7- Eleven Stores Pty Ltd* [2021] AICmr 50 (**the *7-*Eleven matter**) that faceprints are 'personal information'—and that facial images and faceprints are 'sensitive information'—within the meaning of s 6(1) of the Privacy Act.[5]

Lack of valid consent

APP 3.3 provides that APP entities must not collect sensitive information unless:

- they have obtained consent to the collection and the collection is 'reasonably necessary for their functions or activities, or
- an exception listed in APP 3.4 applies.

The APP Guidelines provide that, for consent to be valid, it may be express or implied, but:

- the individual must be adequately informed before giving consent,
- the individual must give consent voluntarily,
- the consent must be current and specific, and
- the individual must have the capacity to understand and communicate their consent.[6]

We note that Bunnings stated to Choice:

> *"We let customers know about our use of CCTV and facial recognition technology through signage at our store entrances and also in our privacy policy, which is available on our website".*

---

[5] *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd* [2021] AICmr 50, 80.

[6] Office of the Australian Information Commissioner, 'Australian Privacy Principles Guidelines' B.35 <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines>.

Providing notice of collection is not the same as obtaining consent. In *Commissioner initiated investigation into Clearview AI, Inc (Privacy)* [2021] AICmr 54 (**the Clearview matter)**, Commissioner Falk stated:

> *A privacy policy is a transparency mechanism that, in accordance with APP 1.4, must include information about an entity's personal information handling practices including how an individual may complain and how any complaints will be dealt with. It is not generally a way of providing notice and obtaining consent. Any such consent would not be current and specific to the context in which that information is being collected, and bundles together different uses and disclosures of personal information.*[7]

We consider that the Retailers have failed to obtain valid consent. We contend that the above approach does not meet the requirement that consent be adequately informed, nor that consent must be current *and specific*, nor that the affected individuals would have the capacity to understand and communicate their consent.

In addition, the fact that the technology operates on *every* person entering a store means that minors, who *cannot* legally consent, are also having their biometric information collected and used by the retailers.

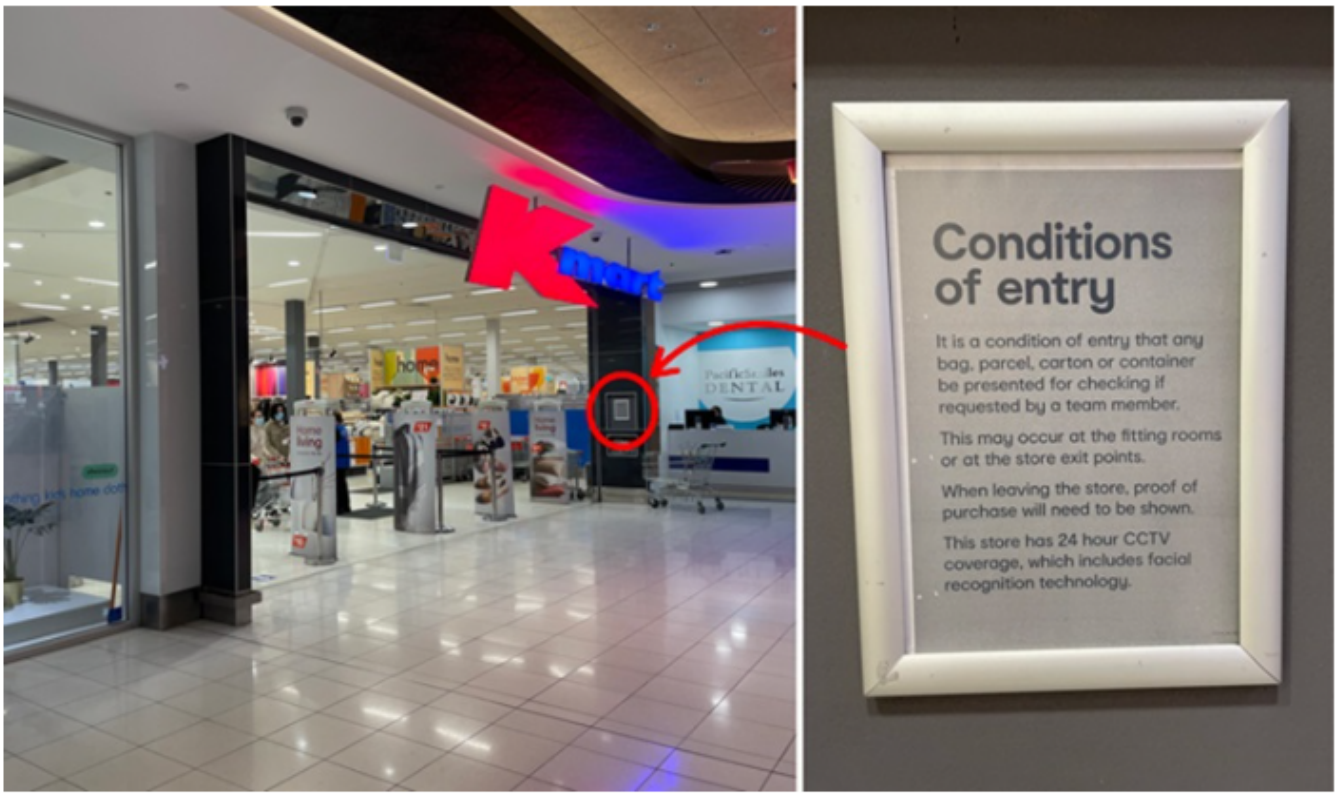
We further contend that the collection of biometric information is *covert collection*.

Notices insufficient

Firstly, we contend that it is highly unlikely that customers will notice or read signage at store entrances. Such signs are often not prominent or noticeable, and drafted in vague terms.

Choice's reporting included the following example:

[7] *Commissioner initiated investigation into Clearview AI, Inc (Privacy)* [2021] AICmr 54, 154.



Signage at the Kmart store in Marrickville, New South Wales.

This signage does not state the purpose of collection, or how the faceprints will be handled. We recognise that different signage may be used by Bunnings or the Good Guys. We note that in the *7-Eleven* matter, similar signage was not considered sufficient to enable informed consent, as:

- customers were not adequately informed about what they were being asked to consent to,
- the signage did not clearly state what information was being collected and how it would be handled by *7-Eleven*, and
- without being given this information, customers were not in a position to understand the implications of providing or withholding consent [at 94].

We note that such signage is unlikely to satisfy the notification requirements outlined in the APP guidelines for APP 5[8]:

[8] Office of the Australian Information Commissioner (n 6) 5.

- the APP entity's identity and contact details
- the fact and circumstances of collection
- whether the collection is required or authorised by law
- the purposes of collection
- the consequences if personal information is not collected
- the entity's usual disclosures of personal information of the kind collected by the entity
- information about the entity's APP Privacy Policy
- whether the entity is likely to disclose personal information to overseas recipients, and if practicable, the countries where they are located

As such, even if customers do notice and read the signage, we contend that signage similar to the Choice example would not be sufficient to support 'adequately informed' consent.

Lack of informed consent

We observe that the Bunnings and Kmart Privacy Policies do mention that images may be collected from CCTV and facial recognition software, for the purposes of "*loss prevention or store safety purposes*". The Good Guys policy includes similar language, stating that they 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... strictly for the purposes of security and theft prevention and managing/improving customer experience*".

However, in our opinion, it is not reasonable to expect customers to read a privacy policy published on a website before attending a brick and mortar store. In that respect, we note the Information Commissioner's findings in the 7-Eleven matter:

> "...an ***APP entity cannot infer consent simply because it has published a policy about its personal information handling practices***. *A privacy policy is a transparency mechanism that, in accordance with APP 1.4, must include information about an entity's personal information handling practices, including how an individual may complain and how any*

> *complaints will be dealt with.* ***It is not generally a way of providing notice and obtaining consent****. Any consent inferred from the existence of a privacy policy would not be current and specific to the circumstances in which the information is being collected."*[9]

As a side note, we observe that the Bunnings and Kmart Privacy Policies (which are substantially similar) are over 3,600 words long. The Good Guys policy is over 5,800 words long. A readability analysis suggests that the policies would require tertiary education to fully understand (the policies all score ~34 on the Flesch Kincaid Reading Ease test[10]). In practice, these policies are therefore not accessible to the 2/3 Australians[11] who do not have a university degree.

Collection is covert

Given the inadequate notification discussed above, we consider that the circumstances of the collection of biometric information is covert.

In the Clearview matter, Commissioner Falk found [at 172-173] that in the circumstances and "in the absence of specific and timely information about the respondent's collection practices" that Clearview AI, Inc had engaged in covert collection. We consider the activities of the Retailers, as far as we are able to determine given the limited information available about their activities, are very similar to the activities of Clearview, AI. Specifically:

- The Retailers do not adequately notify individuals that their image is captured and used to create a faceprint.
- The Retailers publicly available notices and privacy policies provide limited information about their information handling practices. For example, they do not explain:
    - that the Retailers generate biometric templates for matching purposes

---

[9] *Commissioner initiated investigation into 7-Eleven Stores Pty Ltd* (n 5) 95.

[10] *Wikipedia* (online at 18 June 2022) 'Flesch–Kincaid readability tests'.

[11] 'Education and Work, Australia, May 2021 | Australian Bureau of Statistics' (9 November 2021) <https://www.abs.gov.au/statistics/people/education/education-and-work-australia/latest-release>.

- how the Retailers algorithms analyse captured images to generate faceprints (biometric vectors)
- how faceprints derived from captured images are used to identify sufficiently similar faceprints
- which third parties may be shown Matched Images, and the countries those third parties are located in.

We consider the behaviour of the Retailers is sufficiently similar to that described by the Commissioner in the Clearview matter that Retailers are likely performing covert collection of biometric information.

The Commissioner noted that there are significant risks of harm to individuals from such collection:

> *The covert collection of biometric information in these circumstances carries significant risk of harm to individuals. This includes harms arising from misidentification of a person of interest by law enforcement (such as loss of rights and freedoms and reputational damage), as well as the risk of identity fraud that may flow from a data breach involving immutable biometric information.*[12]

The Commissioner also noted that privacy harms from indiscriminate surveillance are not merely individual, but collective, affecting everyone in society:

> *More broadly, the indiscriminate scraping of facial images may adversely impact all Australians who perceive themselves to be under the respondent's surveillance, by impacting their personal freedoms.*[13]

Reasonableness and Proportionality

We recognise that the Retailers have a legitimate need to manage customer and staff safety and mitigate theft. However, it is not self-evident that a system that conducts

[12] *Commissioner initiated investigation into Clearview AI, Inc. (Privacy)* (n 7) 174.
[13] Ibid 176.

facial recognition on all customers is a reasonable, necessary, or proportionate response to those risks, or that the resulting impact on customer and community privacy is justified.

Other implementations of facial recognition have been observed to result in false positives; organisations that overly rely on these technologies for enforcement decisions have thereby made incorrect decisions, and unnecessary and negatively impacted individuals. For example, the 2018 arrest of Robert Williams in Detroit, Michigan for an alleged theft on the basis of a false positive facial recognition identification[14].

As such, it is critical that the risks of this technology be well understood and mitigated. In this instance, there is no indication that the Retailers have done so; indeed, Bunnings' representations to EFA[15] suggest they do not fully understand that the technology that they have implemented requires surveillance of *all* customers.

Conclusion

Facial recognition is not a risk-free technology, nor is it magic. While it is becoming more accessible to organisations, the increasing ubiquity of this technology does not obviate the requirement to comply with the Privacy Act and the APPs.

There are numerous concerns over this use of the technology that have not been addressed by the Retailers in their public communications.

- It is unclear whether the Retailers undertook any proactive risk assessment process, such as the preparation of a Privacy Impact Assessment, or otherwise made any attempt to limit the impacts on individual customers. Arguably, the failure to do so could constitute a failure to take reasonable steps to keep personal information secure, per APP 11.1.

---

[14] Adi Robertson, 'Detroit Man Sues Police for Wrongfully Arresting Him Based on Facial Recognition', *The Verge* (13 April 2021) <https://www.theverge.com/2021/4/13/22382398/robert-williams-detroit-police-department-aclu-lawsuit-facial-recognition-wrongful-arrest>.

[15] Electronic Frontiers Australia, Inc (n 3).

- It is unclear whether the Retailers have assessed their respective facial recognition systems for possible bias, or how Retailers will handle false positives.
- It is unclear how long the Retailers will retain the faceprints they create, if they are stored locally or shared between stores, or if they are part of a broader database system (for instance, with Westfarmers; the parent company of Bunnings and Kmart).
- It is unclear whether the faceprints and the facial recognition technology will be used for any other purpose, such as tracking or targeted marketing, or whether biometric information will be on-sold. While some Retailers have claimed that they will not use the collected biometric information for these purposes, their demonstrated ignorance of how the technology actually functions means we must give little weight to such claims.

In the light of the ongoing review of the Privacy Act[16], this matter underlines the need for additional and specific regulation to govern the use of facial recognition technology, in particular to prevent disproportionately intrusive levels of biometric surveillance. The Retailers have claimed that their use of this technology complies with the Privacy Act, while we believe (as do many privacy professionals with whom we have discussed the matter) that it manifestly does not. Any lingering ambiguity risks permitting others to commit future privacy harms while claiming that their activities are legitimate under cover of that ambiguity.

We note that the recalcitrance of the Retailers in response to widespread public outcry on this matter indicates that individual rights of action are also likely to be needed so that the outsized power of major retailers can be effectively countered with a similar level of individual and collective power. We note that while the Commissioner considers this matter, the facial surveillance systems remain in place and continue to harm Australians' individual and collective privacy. Justice delayed is justice denied.

---

[16] 'Review of the Privacy Act 1988', *Attorney-General's Department* (5 November 2020) <https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988>.