

Bunnings Privacy team

C/- privacy@bunnings.com.au

04 August 2023

By email

RE: Use of facial recognition software

Dear Bunnings Privacy Team,

Thank you for your email dated 21 July 2023. We have some questions:

1. If Bunnings has indeed suspended its use of facial recognition technology pending the outcome of the Office of the Australian Information Commissioner (“**OAIC**”) investigation, why has signage been erected at the new Preston store to warn that facial recognition technology may be in use prior to a decision being made by the OAIC? Is Bunnings attempting to preempt the OAIC’s decision? Surely there is a risk that an adverse decision from the OAIC would require this signage to be replaced?
2. Would it not have been more prudent to wait until after the OAIC’s decision has been made before erecting potentially non-compliant signage, or is Bunnings confident that the OAIC will find that Bunnings’ use of facial recognition is lawful and that this signage provides both adequate notice to customers and procure their express consent for biometric data capture to occur. If so, on what basis has Bunnings formed this view?
3. You claim that facial recognition technology has been deployed “*for the purpose of preventing repeat abuse and threatening behaviour towards our team and customers and repeat theft [in the] retail sector*”. If this is an accurate representation of the facts, can you please tell us what data you have collected to support and inform your decision to deploy facial recognition technology?
 - a. Does the data set discriminate between acts of theft, violence, and abusive behaviour?

- b. Does this data set contain an inherent bias/time specific bias relating to inappropriate or threatening customer behaviour to Bunnings staff made during the mandatory enforcement of the Covid mask mandate and other State government initiated pandemic management requirements? Was there a spike in the data at this time?
 - c. How is the experience of the 'retail sector' relevant in forming part of your rationale to deploy facial recognition technology in your stores? What assurances do you have as to the accuracy of this external data upon which you have relied?
4. Given the widespread community concerns regarding the use of facial recognition technology, and the fact that Bunnings intends to use such technology to scan every person (including minor children) entering a Bunnings store, did Bunnings undertake a comprehensive Privacy Impact Assessment ("**PIA**") as strongly recommended by the OAIC?
 - a. If not, why not?
 - b. If yes, will Bunnings publish this PIA in the spirit of transparency, accountability and maintaining the public's trust?
 - c. Did Bunnings undertake any public consultation about its plans to use facial recognition technology with both customers and civil society groups such as the Australian Privacy foundation, Digital Rights Watch, and State and Territory Civil Liberties organisations? If not, why not?
5. Can Bunnings explain to EFA how the deployment of its facial recognition technology capability complies with the following Australian Privacy Principles ("**APPs**"):
 - a. APP 3.2, with respect to whether the deployment of facial recognition technology was reasonably necessary for its business activities: how and on what basis, given the facts and circumstances of this deployment, Bunnings concluded it is a proportionate and fair response to the perceived risks and how they outweigh the rights of individuals not to be surveilled by extremely invasive technology. Why do you treat — pre-emptively and uniformly — **all** customers as suspects?
 - b. APP 3.3, with respect to the collection of biometric information — defined as 'sensitive information' in the *Privacy Act 1988 (Cth)* ("**Privacy Act**"): how did Bunnings capture the express written or verbal consent from individuals entering a Bunnings store and how is the evidence of express consent stored?
 - c. APP 5, with respect to taking reasonable steps to give individuals a notice setting out the matters described to be included by APP 5.2 (a)-(j): Where is this fulsome notice made available to customers? If you

determined that the obligation required no reasonable steps to be taken to provide an APP 5 notice, please tell us how you reached this conclusion.

- d. APP 11, with respect to the collection of biometric information: what specific actions and techniques does Bunnings take to protect this extremely sensitive information from misuse, interference and loss, unauthorised access, modification or disclosure, and for how long does Bunnings retain this biometric information?
6. In addition, we note in section 1 of the Bunnings Privacy Policy that “*images from biometric software*” are classified as personal information and not sensitive information as defined by Section 6 of the Act. Why is the Bunnings Privacy Policy silent on its approach to the collection, use, and disclosure of sensitive information, given the high likelihood that Bunnings captures a broad range of sensitive information data types as part of its daily business operations – including biometric data which Bunnings notwithstanding has represented it has temporarily suspended ?

We look forward to your response. A copy of this letter will be sent to the OAIC for the purposes of transparency.

Yours sincerely,

Justin Warren
Chair – Electronic Frontiers Australia