Commissioner initiated investigation into 7-Eleven Stores Pty Ltd (Privacy) (Corrigendum dated 12 October 2021) [2021] AICmr 50 (29 September 2021)

Decision and reasons for decision of
Australian Information Commissioner and Privacy Commissioner, Angelene Falk

Respondent	7-Eleven Stores Pty Ltd
Decision date	29 September 2021 (Corrigendum 12 October 2021)
Case reference number	CII20/00004
Catchwords	Privacy — *Privacy Act 1988* (Cth) — Australian Privacy Principles — APP 3.3 – APP 5 – whether facial images are personal information — whether consent obtained for collection of sensitive information — whether collection of sensitive information was reasonably necessary for entity's functions and activities — whether reasonable steps were taken to notify of APP 5 matters – breaches substantiated – requirement to destroy faceprints collected through the customer feedback mechanism

Determination

1. I find that from 15 June 2020 to 24 August 2021, 7-Eleven Stores Pty Ltd (the **respondent**) interfered with the privacy of individuals whose facial images and faceprints it collected through its customer feedback mechanism, within the meaning of the *Privacy Act 1988* (Cth) (**Privacy Act**), by:
   a. collecting those individuals' sensitive information without consent, and where that information was not reasonably necessary for the respondent's functions and activities, in breach of Australian Privacy Principle (**APP**) 3.3
   b. failing to take reasonable steps to notify individuals about the fact and circumstances of collection and the purposes of collection of that information, in breach of APP 5.

Declarations

2. I make the following declarations under the Privacy Act:
   a. I declare under s 52(1A)(a) that:
      i. in the period 15 June 2020 to 24 August 2021, the respondent interfered with the privacy of individuals whose facial images and faceprints it collected through the customer feedback mechanism referred to in paragraph 4, and
      ii. the respondent must not repeat or continue this conduct.
   b. I declare under s 52(1A)(b) that within **90 days** of the date of this determination, the respondent must:
      i. destroy, or cause to be destroyed, all faceprints that it has collected through the customer feedback mechanism, in breach of APPs 3.3 and 5, and
      ii. provide written confirmation to my office when it has complied with paragraph 2(b(i) above.

Findings and Reasons

Background

3. The respondent is a private company which has over 700 stores across Victoria, New South Wales, ACT, Queensland and Western Australia.[1] The stores are 'convenience stores' which sell grocery items. Some stores are attached to petrol stations and sell fuel.
4. In the period 15 June 2020 to 24 August 2021 (the **Relevant Period**), the respondent deployed facial recognition technology in its stores as part of a customer feedback mechanism (the **Facial Recognition Tool**).[2] The Facial Recognition Tool was deployed in 700 stores nationwide.[3]
5. The Facial Recognition Tool was supplied by a third party supplier (the **Service Provider**).
6. Key features of the Facial Recognition Tool were:
   - A tablet device located inside the respondent's stores enabled a customer to complete a voluntary survey about the customer's in-store experience.
   - Each tablet had a built-in camera that took facial images of a customer as they completed the survey.
   - The customer's facial image was captured at two points in time – when the individual first engaged with the tablet, and then after they completed the survey. [4]
   - Facial images were stored on the tablet for around 20 seconds before being uploaded via a secure connection to a secure server hosted in Australia within the Microsoft Azure infrastructure (the **Server**).[5]

[1] https://www.7eleven.com.au/get-to-know-us/about-us.html
[2] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 2, 3.
[3] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 1.
[4] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 1-2.
[5] R3.1 – Letter from the respondent to the OAIC dated 28 May 2021 p 2.

- Once this upload occurred, the facial image was deleted from the tablet.[6]
- The Service Provider used an application programming interface to process the facial images on behalf of the respondent (the **Detect API**). The Detect API converted each facial image to an encrypted algorithmic representation of the face (**faceprint**) and assessed and recorded inferred information about the customer's approximate age and gender.
- The faceprint was then sent to another API (the **Similarity API**), along with all other faceprints generated by responses entered on the same tablet for the last 20 hours. The Similarity API looked for faceprints that were similar. If there was a high probability match, then the corresponding matched survey results were flagged.[7]
- The facial images were retained on the server for 7 days. In the respondent's submission, this was so that the Service Provider could identify and correct any issues, and reprocess survey responses if necessary.
- There was no defined retention period for faceprints, but, in the respondent's submission, after 24 hours any attempt to identify a match using the Similarity API would result in an error.[8]
- Like the faceprints, customers' survey answers were stored in a dedicated encrypted database.[9] All survey responses were timestamped and associated with the relevant store where the relevant tablet was located.[10]

7. As at March 2021, approximately 1.6 million survey responses had been completed.[11]
8. The respondent's purpose for capturing facial images and generating faceprints was to detect if the same person was leaving multiple responses to the survey within a 20 hour period on the same tablet. If they were, their responses may not have been genuine, and were excluded from the survey results. It also enabled the respondent to have a broad understanding of the demographic profile of customers who completed the survey.[12]
9. The respondent could access individual survey responses at any time on the Service Provider's portal. The Service Provider also generated and provided the respondent with regular reports showing recent survey results, and a quarterly insight report. These reports did not contain any images or faceprints and did not contain any personal information (except in rare cases where a customer voluntarily provided this in the free text section of their survey response).[13]

Investigation by the OAIC

10. On 13 July 2020, the Office of the Australian Information Commissioner (**OAIC**) made preliminary inquiries to the respondent under s 42(2) of the Privacy Act. On 3 August 2020, the respondent replied to the preliminary inquiries.

---

[6] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 3
[7] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 8.
[8] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 8.
[9] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 6
[10] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 6.
[11] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 6
[12] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 4, R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 2.
[13] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 9.

11. On 21 February 2021, the OAIC notified the respondent that I intended to commence an investigation under s 40(2) in relation to the use of the facial recognition technology, and that I would consider whether the respondent had met the requirements of APPs 3.3, 3.5 and 5.

12. I have made findings in relation to APPs 3.3 and 5. I have not made a finding in relation to APP 3.5.

13. The respondent collected several types of information through the Facial Recognition Tool, including information about age and gender. However, my findings focus on the acts and practices of the respondent in relation to facial images and faceprints, because, as I discuss below in paragraphs 80 to 84, I consider these to be sensitive biometric information about individuals.

14. As stated in paragraph 4 above, my investigation considered the acts or practices of the respondent from 15 June 2020 to 24 August 2021.

15. On 24 August 2021 the OAIC provided the Acting Deputy Commissioner's preliminary view in this investigation to the respondent for comment, setting out his preliminary findings, reasons, and draft declarations.

16. On 2 September 2021, the respondent advised that after receiving the preliminary view, it promptly asked its Service Provider to disable image capturing on the tablet devices in its stores. The respondent stated that the Service Provider has since confirmed that it has complied with that request. I discuss this submission further at paragraphs 128 to 135 below.[14]

The Law

17. All references to provisions in this determination are to those contained in the Privacy Act except where indicated.

18. The APPs, which are set out in Schedule 1 to the Privacy Act, regulate the collection, use, disclosure and security of personal information held by Australian government agencies and certain private sector organisations (**APP entities**). Section 15 prohibits an APP entity from doing an act, or engaging in a practice, that breaches an APP.

19. Subsection 52(1A) provides that, after investigating an act or practice of a person or entity under s 40(2), the Commissioner may make a declaration that includes one or more of the following:

- a declaration that the act or practice is an interference with the privacy of one or more individuals, and the entity must not repeat or continue the act or practice[15]
- a declaration that the entity must take specified steps within a specified period to ensure that the act or practice is not repeated or continued[16]
- a declaration that the entity must perform any reasonable act or course of conduct to redress any loss or damage suffered by one or more individuals[17]

[14] R4 – Email from the respondent to the OAIC dated 2 September 2021.
[15] Privacy Act, s 52(1A)(a)
[16] Privacy Act, s 52(1A)(b)
[17] Privacy Act, s 52(1A)(c)

- a declaration that one or more individuals are entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice[18]
- a declaration that it would be inappropriate for any further action to be taken in the matter.[19]

20. The relevant law is set out at **Attachment A.**

Material considered

21. In making this determination, I have had regard to:

- information and submissions provided by the respondent
- information obtained from online sources by officers of the OAIC
- the Australian Privacy Principles Guidelines, February 2014 (**APP Guidelines**),[20] the OAIC's guidance on What is Personal Information,[21] the OAIC's Privacy Regulatory Action Policy[22] and the OAIC's Guide to Privacy Regulatory Action, July 2020.[23]

22. The APP Guidelines outline the mandatory requirements of the APPs, how I will interpret the APPs, and matters that I may take into account when exercising my functions and powers under the Privacy Act. The APP Guidelines are not legally binding and do not constitute legal advice about how an entity should comply with the APPs in particular circumstances.

Respondent as an APP entity

23. The Privacy Act regulates the acts and practices of 'APP entities'. An 'APP entity' is either an organisation or an agency (s 6). An 'organisation' includes a body corporate that is not a 'small business operator' (s 6C).

24. The respondent is a body corporate registered in Australia, and there is no evidence before me to indicate that it is a small business operator for the purposes of the Privacy Act.[24] I therefore find that the respondent is an organisation and an APP entity.

Findings on Breach

Personal information

Law

25. For the provisions of the Act to apply, the information in question must be 'personal information' as defined in the Privacy Act. Personal information is defined in s 6(1) as

---

[18] Privacy Act, s 52(1A)(d)
[19] Privacy Act, s 52(1)(d)
[20] As at July 2019.
[21] https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/#introduction
[22] https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/
[23] https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/
[24] https://www.7eleven.com.au/get-to-know-us/about-us.html

'information or an opinion about an identified individual, or an individual who is reasonably identifiable: (a) whether the information or opinion is true or not; and (b) whether the information or opinion is recorded in a material form or not'.

26. Information or an opinion is 'about' an individual where the individual is the subject matter of the information or opinion. The Full Federal Court considered the definition of 'personal information' that applied in the Privacy Act as at 1 July 2013, and relevantly stated:

> The words "about an individual" direct attention to the need for the individual to be a subject matter of the information or opinion. This requirement might not be difficult to satisfy. Information and opinions can have multiple subject matters. Further, on the assumption that the information refers to the totality of the information requested, then even if a single piece of information is not "about an individual" it might be about the individual when combined with other information.'[25]

27. Whether information or an opinion is 'about' an individual is ultimately a question of fact and will depend on the context and the circumstances of each particular case.[26]

28. Whether a person is 'reasonably identifiable' is an objective test that has practical regard to the context in which the issue arises. Generally speaking, an individual is 'identified' when, within a group of persons, the individual is 'distinguished' from all other members of a group.

29. Certain information may be unique to a particular individual, and therefore may (in and of itself) establish a link to that person. However, for an individual to be 'identifiable', they do not necessarily need to be identified from the specific information being handled. An individual can be 'identifiable' where the information is able to be linked with other information that could ultimately identify the individual.[27] An individual can be reasonably identifiable, by any person (or machine) other than the subject themselves.

Consideration

30. The respondent submitted that:

- Facial images and faceprints were not personal information because they are not used to identify, monitor or track any individual.
- The Service Provider's system operated independently from the respondent's other systems,[28] and none of the information collected by the Facial Recognition Tool was associated or matched with any personal information or customer data.[29]
- A limited number of the Service Provider's employees could access the images while they were held on the Server, for the purposes of identifying errors and other issues with the system. However, the images were heavily blurred so that the faces were not

[25] *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 at [43] and [64] per Kenny and Edelman JJ at [63].

[26] See *Telstra Corporation Limited and Privacy Commissioner* [2015] AATA 991 (18 December 2015) at [112], and *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 at [43] and [64] per Kenny and Edelman JJ.

[27] https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/

[28] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 5.

[29] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 1, 2.

identifiable. The 'raw' images (where faces were identifiable) could only be accessed by a very small number of the Service Provider's software engineers. [30]

- The faceprint was unique for every photo (so uploading the same photo twice would result in two different faceprints). The faceprint was a random string of characters, and could not be used to detect duplicate faces outside the Similarity API.[31]

Were facial images personal information?

31. The images captured by the tablets were digital images of an individual's face.

32. As facial images showed individuals' faces, I consider that those images were 'about' an individual.

33. While acknowledging that only a small number of the Service Provider's software engineers could view the 'raw' unblurred facial images, I am satisfied that an individual was reasonably identifiable from their facial image, for the following reasons:

    - A facial image alone will generally be sufficient to establish a link back to a particular individual, as these types of images display identifying features unique to that individual.
    - The respondent processed facial images for the purpose of biometric identification (see paragraph 82).

34. On that basis, I find that the facial images that were captured by the tablets were personal information within the meaning of s 6(1).

Are faceprints personal information?

35. Faceprints were created by automatically converting facial images into an encrypted algorithmic representation of a customer's face.

36. As these were digital representations of a particular individual's facial features, I am satisfied that they were 'about' an individual.

37. For an individual to be 'identifiable', they do not necessarily need to be identified from the specific information being handled. An individual can be 'identifiable' where it is possible to identify the individual from available information, including, but not limited to, the information in issue.[32]

38. As outlined in paragraph 6, customers' facial images were analysed to generate faceprints.[33] These faceprints were compared to other faceprints to identify faceprints that were sufficiently similar. The Facial Recognition Tool also directly linked individuals' faceprints with survey responses, by using each faceprint as an 'identifier' to detect if the same individual was leaving multiple survey responses.[34] These processes enabled an individual depicted in a faceprint to be distinguished from other individuals whose faceprints were held on the Server. Accordingly, I am satisfied that individuals depicted in faceprints were reasonably identifiable.

---

[30] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 7.
[31] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 8.
[32] OAIC, *Publication of MBS/ PBS data: Commissioner initiated investigation report,* 23 March 2018, p 4, available at https://www.oaic.gov.au/privacy/privacy-decisions/investigation-reports/mbspbs-data-publication/.
[33] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 4.
[34] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 4, R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 2.

39. I find that the faceprints were 'personal information' within the meaning of s 6(1).

Findings

APP 3.3 – Collection of sensitive information

Law

Collection of solicited personal information

40. APP 3 outlines when an APP entity may collect solicited personal information.

41. APP 3.3 prohibits an APP entity from collecting sensitive information about an individual unless:

- The individual consents to the collection of the information, and (as relevant to organisations) the information is reasonably necessary for one or more of the entity's functions or activities.
- One of the exceptions in APP 3.4 applies in relation to the information.

42. An APP entity 'collects' personal information 'only if the entity collects the personal information for inclusion in a record or generally available publication'.[35] The definition of 'record' in s 6(1) includes a document or an electronic or other device.

43. An APP entity 'solicits' personal information 'if the entity requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included'.[36] The request may be made to an individual.[37] A 'request' is an active step taken by an entity to collect personal information, and may not involve direct communication between the entity and the individual.[38]

44. The concept of 'collection' applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means, including from individuals, other entities, and biometric technology, such as voice or facial recognition.[39] It includes collection by 'creation' which may occur when information is created with reference to, or generated from, other information the entity holds.[40]

Sensitive information and biometrics

45. The definition of 'sensitive information' under the Privacy Act extends to two particular kinds of biometric information:

- 'biometric information that is to be used for the purpose of automated biometric verification or biometric identification' and

[35] Privacy Act s 6(1).
[36] Privacy Act s 6(1).
[37] The definition of 'organisation' includes an individual. See Privacy Act s 6C.
[38] https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-3-app-3-collection-of-solicited-personal-information/#ftn1
[39] https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/#collects
[40] https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles/#part-2-australian-privacy-principles-and-data-analytics

- 'biometric templates'.[41]

46. 'Biometric information' and 'biometric templates' are not defined in the Privacy Act.

47. 'Biometrics' encompasses 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).[42] These characteristics cannot normally be changed and are persistent and unique to the individual.

48. '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.

49. 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.[43] 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.

Consent

50. The four key elements of consent are:

- The individual is adequately informed before giving consent.
- The individual gives consent voluntarily.
- The consent is current and specific.
- The individual has the capacity to understand and communicate their consent.

51. Consent can be express or implied.[44]

52. Express consent is given explicitly, either orally or in writing. An APP entity should generally seek express consent from an individual before handling the individual's sensitive information, given the greater privacy impact this could have.

53. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity. Consent may not be implied if an individual's intent is ambiguous or there is reasonable doubt about the individual's intention.[45]

Reasonably necessary for the entity's functions and activities

54. An APP entity must only collect personal information which is reasonably necessary for one or more of the entity's functions or activities.

---

[41] See definition of 'sensitive information, Privacy Act, s 6(1).

[42] Office of the Victorian Information Commissioner, *Biometrics and Privacy*, available at https://ovic.vic.gov.au/resource/biometrics-and-privacy/ (accessed 16 February 2021). See also, ISO/ IEC 2382-37 *Information Technology – Vocabulary, Part 37: Biometrics.*

[43] International Organization for Standardisation, *Standard ISO/IEC 2382-37: 2017(en), Standard 3.3.22* < https://www.iso.org/obp/ui/#iso:std:iso-iec:2382:-37:ed-2:v1:en> (at 12 March 2021).

[44] Privacy Act s 6(1).

[45] APP Guidelines [B.34] – [B.58].

55. The terms, 'function' and 'activity', are not defined in the Privacy Act. They are to be construed pursuant to their ordinary meaning, by reference to the language of the statute as a whole, and the context, general purpose and policy of the provision.

56. The word 'function' is relevantly defined to mean 'a kind of action or activity which is proper to a person, thing or institution'; or 'the purpose for which something is designed or exists'; or a 'role'.[46] 'Activity' is defined as 'a specific deed, action, function, or sphere of action'.[47]

57. An organisation's functions or activities include:

- current functions or activities of the organisation
- proposed functions or activities the organisation has decided to carry out and for which it has established plans
- activities the organisation carries out in support of its other functions and activities, such as human resource, corporate administration, property management and public relations activities.[48]

58. 'Necessary' is not defined in the Privacy Act. The High Court of Australia has noted that 'there is, in Australia, a long history of judicial and legislative use of the term 'necessary', not as meaning essential or indispensable, but as meaning reasonably appropriate and adapted'.[49] However, in the context of the Privacy Act, it would not be sufficient if the collection, use or disclosure is merely helpful, desirable or convenient.[50]

59. In evaluating whether a collection of personal information is reasonably necessary for a particular function or activity, consideration should be given to whether any interference with personal privacy is proportionate to a legitimate aim sought. In *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285, Bell J applied similar collection principles in force at the time under the *Information Privacy Act 2000 (Vic)* and noted:

> Reasonable proportionality comes into the interpretation and application of the provisions of cl 1 of the Information Privacy Principles because the specified standards are evaluative in nature: it is necessary to determine in a given case what is 'necessary' in IPP 1.1, 'lawful and fair' and not 'unreasonably intrusive' in IPP 1.2, 'practicable' and 'reasonable' in IPP 1.3, 'reasonable and practicable' in IPP 1.4 and what are 'reasonable steps to ensure' in IPP 1.5.To a greater or lesser extent, matters of fact and degree are involved, which requires consideration of what is at stake for the individual (including the nature of the personal information in question) and balancing, in a reasonably proportionate way, the nature and importance of any legitimate purpose and the extent of the interference.

60. Factors relevant to determining whether a collection of personal information is reasonably necessary for a function or activity include:

- the primary purpose of collection
- how the personal information will be used in undertaking a function or activity of the APP entity, and

---

[46] *dictionary.com*; accessed 28 June 2021 at https://www.dictionary.com/browse/function.
[47] *dictionary.com*; accessed 28 June 2021 at https://www.dictionary.com/browse/activity.
[48] APP Guidelines [3.13].
[49] Mulholland v Australian Electoral Commissioner [2004] HCA 41 [39] (Gleeson CJ).
[50] APP Guidelines [B.113].

- whether the entity could undertake the function or activity without collecting that personal information, or by collecting a lesser amount of personal information.[51]

61. It is the responsibility of an APP entity to be able to justify that a particular collection is reasonably necessary.

Consideration

Did the respondent solicit facial images and faceprints?

62. The respondent requested or invited customers to complete the survey and made tablets available in its stores for customers to complete their responses. The process of providing a survey response included the active step of capturing the individual's facial image and using this information to generate a faceprint.

63. On that basis, I am satisfied that the respondent 'solicited' facial images and faceprints within the meaning of s 6(1).

Did the respondent collect facial images?

64. As discussed in paragraph 6, facial images were captured by a camera on the tablet, where they were kept for around 20 seconds. Then they were uploaded to a secure Server and retained for 7 days.[52]

65. The tablets and Server were 'records' within the meaning of s 6(1), as these were each an 'electronic or other device'. On this basis, I am satisfied that facial images were 'collected' within the meaning of s 6(1) (even though the facial images were only stored on the tablet for a short time).

66. The question is then whether the *respondent* collected the facial images in the Relevant Period.

67. The respondent asserted that facial images were collected by tablets supplied by the Service Provider as an end-to-end solution.[53] The respondent also submitted:

- It had no access to the facial images held by the Service Provider.[54]
- It had no ability to independently access, change or retrieve the information processed by the Service Provider for the respondent, and there was no established mechanism or process for the respondent to seek access to any such information from the Service Provider.[55]
- The images and faceprints were stored on a server hosted within Microsoft Azure infrastructure. The server was controlled by the Service Provider, which could add, remove or reconfigure the services provided from that Server without needing to engage with Microsoft or any other third party.[56]

68. I have considered the contractual arrangements between the respondent and the Service Provider. The Service Provider provided hardware, software and certain other services (including the Facial Recognition Tool) under a written agreement between the

[51] APP Guidelines [3.17]-[3.19].
[52] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 3
[53] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 2.
[54] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 2.
[55] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 3
[56] R3.1 – Letter from the respondent to the OAIC dated 28 May 2021 p 2.

respondent and the Service Provider (the **Agreement**), a copy of which was provided to the OAIC in the investigation.

69. Under the Agreement: [redacted]

70. [redacted] I am not satisfied that the respondent is released from its obligations under the Privacy Act to handle personal information in accordance with the APPs.

71. I am satisfied that the respondent 'collected' the facial images and faceprints within the meaning of s 6(1) on the basis that:

- The tablets were set up in the respondent's stores at the request of the respondent and for the respondent's purposes.
- The tablets were used to capture the respondents' customers' facial images, while they were completing surveys about their in-store experiences. The purpose of collection was to improve the genuineness of the customer feedback provided to the respondent and assist the respondent with demographic profiling.[57]
- The respondent had a contractual right to use the tablets for its internal business purposes.
- The respondent had contractual control over its data held on the Server [redacted].

72. For the sake of completeness, I have not considered whether the Service Provider collected the facial images. Even if it did, this does not mean that the respondent could not also collect the same facial images. Two entities may collect the same personal information[58] (just as two entities may 'hold' the same information under the Privacy Act).

Did the respondent collect faceprints?

73. The respondent asserted that the Service Provider used the Detect API to generate a faceprint for each facial image. The Server automatically converted facial images to faceprints.

74. The respondent's submissions were inconsistent as to how long the faceprints are stored for. The respondent initially asserted that faceprints were stored temporarily on the Server for 7 days, and then permanently deleted automatically.[59] However, in later submissions the respondent stated that '[t]here is no defined retention period' for faceprints.[60] From this I understand that faceprints are retained indefinitely on the Server.

75. I have found in paragraph 65 above that the Server was a 'record' within the meaning of s 6(1).

76. 'Collection' includes collection by 'creation'. This may occur when information is created with reference to, or generated from, other information the entity holds. Faceprints were generated from other information the respondent held (namely facial images). On that basis, I am satisfied that the faceprints were collected for inclusion in a record, and were therefore 'collected' within the meaning of s 6(1).

---

[57] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 2.

[58] *Australian Information Commissioner v Facebook Inc (No 2)* [2020] FCA 1307 at [184]; *Commissioner Initiated Investigation into Uber Technologies, Inc. & Uber B.V. (Privacy)* [2021] AICmr 34 (30 June 2021) at [71].

[59] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 6

[60] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 8.

77. The question is then whether the *respondent* collected the faceprints in the Relevant Period.

78. The respondent submitted that faceprints were generated by, and stored on, a server controlled by the Service Provider.[61] The respondent stated that it had no access to the faceprints held by the Service Provider.[62] Only the Service Provider could access faceprints for the limited purpose of quality control, system maintenance and adjustments to the image processing algorithm.[63]

79. I again refer to the Agreement between the respondent and the Service Provider, as outlined in paragraphs 68 to 70 above. While I accept that the respondent may not have had access to the faceprints, I am satisfied that the respondent 'collected' faceprints within the meaning of s 6(1) on the basis that:

- The faceprints were generated in accordance with the terms of the Agreement, at the respondent's request and for the respondent's purposes.
- The faceprints were generated from the respondents' customers' facial images, while they were completing surveys about their in-store experiences. The purpose of collecting these faceprints was to improve the genuineness of the customer feedback provided to the respondent and assist the respondent with demographic profiling.[64]
- The respondent had contractual control over its data held on the Server [redacted].
- The respondent had a contractual right to use the Server that processed the faceprints, for its internal business purposes.

Were facial images and faceprints sensitive information?

80. As stated in paragraph 45 above, the definition of 'sensitive information' in the Privacy Act extends to 'biometric information that is to be used for the purpose of automated biometric verification or biometric identification' and 'biometric templates'.[65]

81. I consider that the facial images and faceprints collected by the respondent were 'biometric information'. As discussed in paragraph 47, biometric characteristics pertaining to an individual's face are persistent, cannot normally be changed, and are unique to that individual. The facial images show physiological features and characteristics of an individual's face that meet these criteria. Similarly, faceprints, as 'an algorithmic representation of the face',[66] also recorded persistent and largely unique information about an individual's face.

82. I am also satisfied that these facial images and faceprints were used in an automated biometric identification system. For the reasons set out in paragraphs 33 to 38, I have formed the view that individuals depicted in facial images and faceprints were reasonably identifiable, because the Facial Recognition Tool enabled an individual depicted in a faceprint to be distinguished from other individuals whose faceprints were held on the Server. This process was automated[67] and based on comparing biometric characteristics (see above).

---

[61] R3.1 – Letter from the respondent to the OAIC dated 28 May 2021 p 2.
[62] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 2.
[63] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 3.
[64] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 2.
[65] Section 6(1) of the Privacy Act
[66] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 3.
[67] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 2.

83. In addition, faceprints are 'an algorithmic representation of a face',[68] derived from biometric samples (facial images) and enrolled in a biometric identification system (the Server on which the automated matching process described above occurs). On that basis, I am satisfied that faceprints are 'biometric templates'.

84. I consider that both the facial images and faceprints are sensitive information within the meaning of s 6(1).

85. As the respondent collected sensitive information during the Relevant Period, APP 3.3 required:

- the respondent to obtain consent to the collection, and
- that the collection was reasonably necessary for one or more of the respondent's functions or activities (unless an exception applies).

Did individuals consent to the collection of their sensitive information?

86. There is no evidence that individuals expressly consented to the collection of their facial images or faceprints.

87. While entities generally should not rely on implied consent when collecting sensitive information,[69] I consider below whether individuals impliedly consented to the collection of their facial images and faceprints by the respondent.

88. The respondent submitted that the Facial Recognition Tool was 'entirely optional and voluntary',[70] and that if a customer did not consent to the use of this technology, the customer could elect to not enter the store or not use the tablet.[71]

89. The respondent also submitted that in an effort to be transparent with customers about the use of this technology, it displayed a notice at the entrance to its stores to alert customers that upon entering the store they may be subject to facial recognition technology.[72] A copy of the three different notices displayed by the respondent is at **Attachment B** (the **Store Notices**).

90. The Store Notices each showed an image of what appears to be a video or CCTV camera. The notice labelled 'FuelSite-Code7110125' also included the following text:

> Site is under constant video surveillance.
>
> By entering the store you consent to facial recognition cameras capturing and storing your image.

91. The respondent's Privacy Policy, which was available on its website,[73] stated:

> **What personal information we collect and hold**
>
> We only collect personal information that is reasonably necessary for our business functions and activities and to provide you with our products and services.

[68] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 3.
[69] APP Guidelines [B.41].
[70] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 1.
[71] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 4.
[72] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 4, 8.
[73] https://www.7eleven.com.au/privacy-policy.html

> If you are a customer and you decide not to provide certain personal information to Us, We may not be able to provide you with the product or service you are after.
>
> By acquiring or using a 7-Eleven product or service or providing your personal information directly to us, you consent to 7-Eleven collecting, storing, using, maintaining and disclosing your personal information for the purposes set out in this Privacy Policy.
>
> …
>
> 7-Eleven may also collect photographic or biometric information from users of our 7-Eleven App and visitors to our stores, again, where you have provided your consent. 7-Eleven collects and holds such information for the purposes of identity verification.
>
> **How we collect personal information**
>
> Generally, We collect most personal information directly from you, for example where you:
>
> …
>
> - use a feedback kiosk from our stores; …

92. I consider that consent cannot be implied in the above circumstances.

93. Consent may not be implied if an individual's consent is ambiguous or there is reasonable doubt about the individual's intention.[74] While I accept that use of the tablet was voluntary, I am not satisfied that the act of using the tablet unambiguously indicated an individual's agreement to collect their facial image and faceprint, in circumstances where:
    - There was no information provided on or in the vicinity of the tablet, or during the process of completing the survey, about the respondent's collection of facial images and faceprints.[75]
    - The Store Notices were unclear, and, given the prevalence of these kind of notices in stores and public places, may have created an impression that the respondent captured customers' images using a facial recognition CCTV camera as part of surveillance of the store.
    - The respondent's Privacy Policy did not link the collection of photographic or biometric information to the use of in-store 'feedback kiosks'.

94. Any consent provided in the circumstances described above would not have met the criteria listed in paragraph 50:
    - Customers were not adequately informed about what they were being asked to consent to. The Store Notices and Privacy Policy did not state what information was being collected and how it would be handled by the respondent. Without being given this information, customers were not in a position to understand the implications of providing or withholding consent.

[74] APP Guidelines [B.39].
[75] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 29-37.

- The Store Notices and Privacy Policy were neither current nor specific, as they did not request consent contemporaneously before or during the survey process, or refer to that process.
- The Privacy Policy bundled together multiple collections, uses and disclosures of personal information, preceded by a general statement that '[b]y acquiring or using a 7-Eleven product or service or providing your personal information directly to us, you consent to 7-Eleven collecting, storing, using, maintaining and disclosing your personal information for the purposes set out in this Privacy Policy'.[76] Bundling requests for consent in this way undermines the voluntariness of any consent provided, as it does not give individuals the opportunity to choose which collections they agree to and which they do not.[77]

95. Even if the Privacy Policy had included comprehensive information about the information collected by the respondent through the facial recognition system and how it is handled, an APP entity cannot infer consent simply because it has published a policy about its personal information handling practices.[78] 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.[79] 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.

96. If an entity intends to collect sensitive information from its customers, a request for consent should:
    - clearly identify the kind of information to be collected, the recipient entities, and the purpose of the collection
    - be sought expressly and separately from a privacy policy at a current point in time
    - be fully informed and freely given (see paragraph 50).

97. For the above reasons, I consider that individuals did not consent to the collection of their sensitive information by the respondent.

98. For the sake of completeness, I note that the respondent provided the OAIC with two versions of the Service Provider's privacy policy, which described the collection of facial images and faceprints. As stated in paragraph 95, a privacy policy published on an entity's website is not generally a basis for inferring consent. Even if an entity could infer consent from a privacy policy, consent could not be inferred from the Service Provider's privacy policy. The Store Notices and the respondent's Privacy Policy did not state the name of the Service Provider, so individuals would not have been aware that a third party was providing services to the respondent, and would have had no reason to look for the Service Provider's privacy policy.

99. None of the exceptions in APP 3.4 are relevant to this matter.

---

[76] https://www.7eleven.com.au/privacy-policy.html
[77] APP Guidelines [B.45]-[B.46].
[78] *Flight Centre Travel Group (Privacy)* [2020] AICmr 57 (25 November 2020) [53].
[79] https://www.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/AICmr/2020/57.html

Was the collection of facial images and faceprints reasonably necessary for the respondent's functions or activities?

100. The respondent is a retailer of petrol and convenience items, including food and drinks.[80]

101. The respondent submitted that:

- It deployed facial detection technology to its stores as part of a 'customer feedback capture mechanism' which enabled customers to complete a survey about their in-store experience.[81]
- The purpose of collecting customers' facial images and faceprints was to detect and flag potentially non-genuine survey responses, such as if the same person left multiple responses within a 20 hour period. The respondent provided the example of a store team member posing as a customer and rating their own performance positively multiple times. The respondent did not provide any other possible motivations for individuals to leave non-genuine responses.
- The information collected also gave the respondent a broad understanding of the demographic profile of its customers who completed the survey (specifically their approximate age and assumed gender).[82]

102. I accept that implementing systems to understand and improve customers' in-store experience is a legitimate function or activity in support of the respondent's main function of selling petrol and convenience items in its stores.

103. However, I consider that, the respondent has not justified that collecting its customers' sensitive biometric information (including facial images and faceprints) was 'reasonably necessary' for understanding and improving customers' in-store experience. I have had regard to the following factors:

- I am not satisfied that it was reasonably necessary to collect 'sensitive' biometric information (see paragraph 84 above) for this function or activity. I note the risk of adversity to individuals should this kind of information be misused or compromised, as it cannot be reissued or cancelled like other forms of compromised identification information. The risks associated with collection of such information are not proportional to the function or activity of understanding and improving customers' in-store experience.
- The respondent did not conduct a privacy impact assessment (**PIA**) in relation to the in-store feedback mechanism 'project'.[83] A PIA would have helped to analyse the possible impacts on individuals' privacy resulting from collection and handling of biometrics, and to identify options for avoiding, minimising or mitigating adverse privacy impacts (including by identifying potential alternatives for achieving the goals of the project without collecting such information). It would also have assisted in assessing the proportionality of collecting biometrics for the purpose of understanding customers' in-store experience.
- There appear to be other ways in which the respondent could have identified potentially non-genuine responses and collected demographic information, which

[80] Respondent's website, available at https://www.7eleven.com.au/ (accessed on 11 June 2021).
[81] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 2.
[82] R1.1 – Letter from the respondent to the OAIC dated 3 August 2020 p 4.
[83] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 2.

would have had a lesser privacy impact on individuals. For example, the respondent could have included additional survey questions asking the customer whether they had already responded to the survey in the same store in the last 20 hours, and to nominate an age range and gender. The respondent could also have taken other steps, in running its business, to discourage dishonest behaviour by employees and effectively measure staff performance.

104. The respondent did not receive information from the Service Provider about the total number of survey responses that were flagged as non-genuine. Rather, these were simply excluded from the reports generated by the Service Provider.[84] In the absence of actual information about the prevalence of non-genuine survey responses, it would appear difficult to assess whether collection of facial images and faceprints is reasonably necessary. That said, even if the respondent could demonstrate that there were non-genuine survey responses, this would not have established that the collection of sensitive biometric information was reasonably necessary, for the reasons set out in paragraph 103.

105. In the above circumstances, I am not satisfied that the large-scale collection of customers' sensitive biometric information through the respondent's customer feedback mechanism, was reasonably appropriate or adapted to the activity of understanding and improving customers' in-store experience.[85] At most, it may have been helpful or convenient to collect this kind of information for this purpose. Any benefit to the respondent was disproportionate to, and failed to justify, the potential harms associated with the collection and handling of sensitive biometric information.

106. Accordingly, the collection of customers' facial images and faceprints during the Relevant Period through the customer feedback mechanism, was not reasonably necessary for the respondent's functions and activities.

Finding of breach – APP 3.3

107. I find that during the Relevant Period the respondent interfered with the privacy of individuals whose facial images and faceprints it collected through its customer feedback mechanism, by collecting those individuals' sensitive information without consent, and in circumstances where that information was not reasonably necessary for the respondent's functions and activities, in breach of APP 3.3.

APP 5 – notification of the collection of personal information

Law

108. APP 5.1 requires an APP entity that collects personal information about an individual to take such steps (if any) as are reasonable in the circumstances to notify the individual of such matters referred to in APP 5.2 (**APP 5 matters**), or to otherwise ensure that the individual is aware of any such matters.

109. Transparency obligations such as those in APP 5 are intended to ensure that individuals have knowledge of, and choice and control over, how information about them is handled by APP entities. Conversely, a lack of transparency can affect individuals'

[84] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 6.

[85] The respondent started conducting surveys using the tablets on 15 June 2020. From 15 June 2020 to 25 March 2021, approximately 1.6 million survey responses have been completed. R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 6.

ability to exercise their rights under the Privacy Act, such as the right to request access to and correction of their personal information, or to make a complaint.

110. In this case, the relevant APP 5 matters are:

- if the individual may not be aware that the APP entity has collected their personal information, the fact that the entity so collects, or has collected, the information and the circumstances of that collection,[86] including the method of collection[87]
- the purposes for which the APP entity collects personal information,[88] including the primary purpose of collection (that is, the specific function or activity for which particular personal information is collected).[89]

111. Reasonable steps that an entity should take will depend upon the circumstances, including the sensitivity of the personal information; the possible adverse consequences for the individual; any special needs of the individual; and practicability, including the time and cost of taking measures. In particular, more rigorous steps may be required when collecting sensitive information.[90]

112. The timing of the obligation to notify individuals under APP 5.1 is at or before the time that the APP entity collects the personal information. If this is not practicable, it must notify as soon as practicable after collection.

Consideration

What steps did the respondent take to notify individuals of APP 5 matters?

113. As discussed in paragraph 89 above, the respondent submitted that it displayed a notice at the entrance to its stores to alert customers to the fact that upon entering the store they may be subject to facial recognition technology. Copies of the Store Notices are at **Attachment B**. The respondent submitted that apart from the Store Notices, there were no other privacy notices displayed on or about the tablet or during the survey process.[91]

114. The respondent's Privacy Policy on its website also referred to the APP 5 matters.[92] The respondent's Privacy Policy on its website notified individuals of the relevant APP 5 matters as follows:

> …
>
> 7-Eleven may also collect photographic or biometric information from users of our 7-Eleven App and visitors to our stores, again, where you have provided your consent. 7-Eleven collects and holds such information for the purposes of identity verification.
>
> …

[86] APP 5.2(b)(ii)
[87] APP Guidelines [5.11].
[88] APP 5.2(d)
[89] APP Guidelines [5.15].
[90] APP Guidelines [5.4].
[91] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 5.
[92] https://www.7eleven.com.au/privacy-policy.html

Generally, We collect most personal information directly from you, for example, where you:

- order and purchase goods or services through our website and/or apps;
- register for participation in a competition, promotion or survey;
- request customer service or contact us;
- apply for employment;
- make a franchise or other specific enquiry necessitating a response;
- participate in a digital interactive activity;
- use a feedback kiosk from our stores; or
- register for and use a product or service, such as the 7-Eleven Fuel Card, or a relevant 7-Eleven App.

…

Unless otherwise disclosed during the collection process, personal information which We collect from you is used only for the purposes consistent with the reasons it was provided, for a related purpose, or where otherwise permitted by law.

Examples of how We may use your personal information include:

- to provide products and services to you and provide you with information about them;
- to process your payments or refunds;
- to administer, manage, and improve our products and services, including to perform identity related checks;
- to understand the use of our products, services and digital channels and to make improvements to them;
- to respond to particular requests from you;
- to assist in investigating your complaints and enquiries;
- in general to promote and market to you our various businesses, services, products and special offers and those of our trading partners.

…

We may disclose your personal information to:

- our payment processing provider for the purposes of processing your payment or refund;
- your authorised representative, when you ask us to do so;
- our franchisees;

- law enforcement agencies and other government and regulatory bodies as required or authorised by law.

We will not otherwise disclose this personal information except when authorised to do so by law.

Were the steps taken by the respondent to notify individuals of the APP 5 matters reasonable in the circumstances?

115. The Store Notices and the respondent's Privacy Policy did not address all the APP 5 matters.

116. Firstly, the Store Notices in Privacy Policy did not inform individuals about the fact and circumstances of collection of facial images and faceprints, as is required by APP 5.2(b). Although one of the three Store Notices and the Privacy Policy referred to the collection of images, these resources did not inform individuals about the collection of faceprints, or the method by which the respondent collected facial images and faceprints.

117. To meet the above requirement, I would expect the respondent to have provided a collection notice that specifically stated that:

- The respondent collects facial images of individuals who complete the feedback survey on tablets in front of cashiers in the respondent's stores.[93] (I would expect a similar level of detail in descriptions of any other locations of tablets.)
- The respondent analyses the facial images using facial recognition technology to generate and collect faceprints of those individuals.

118. Secondly, the Store Notices and Privacy Policy did not adequately inform individuals about the purpose for which the above information was collected:

- The Store Notices provided no information about the respondent's purpose of collection (though, as discussed at paragraph 93, I consider that they may have created an erroneous impression that the respondent captured customers' images using facial recognition CCTV for the purpose of store surveillance).
- The Privacy Policy stated that the respondent collects 'photographic or biometric information … for the purposes of identity verification'. I am not satisfied that this statement would have enabled individuals to understand the specific function or activity for which the respondent collected the personal information. The respondent did not collect facial images and faceprints to verify individuals' identities. The respondent collected this information to detect if the same person was leaving multiple responses to the survey within a 20 hour period on the same tablet.

119. To meet the above requirement, I would expect the respondent to have provided a collection notice with a more detailed description of the purposes of collection. For example, the collection notice could have stated that the respondent collects facial images and faceprints for biometric matching, in order to identify if an individual is leaving multiple survey responses within a period of time, and to assist the respondent with demographic profiling.

120. While I have considered the respondent's Privacy Policy above, I also note that even if the Privacy Policy did provide adequate information about APP 5 matters, simply publishing a privacy policy on a website does not amount to compliance with APP 5.

[93] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 28.

121. As discussed in paragraph 95, 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. It is not generally a way of providing notice under APP 5. It is not reasonable to assume that customers will have searched for the respondent's Privacy Policy online and read through it before entering the store and completing the survey.

122. Instead, having regard to the sensitivity of the information, the respondent should have included a collection notice on, or in the vicinity of, the tablet screen. The collection notice should have notified customers about APP 5 matters before the start of the survey, and crucially, before the first facial image of the customer was captured. This was a practical and cost-effective step that the respondent could reasonably have taken in the circumstances, to draw customers' attention to the collection of their sensitive biometric information and the purpose of that collection. However, the respondent did not take such a step.[94]

123. For the above reasons, I consider that the respondent did not take reasonable steps to notify individuals of APP 5 matters.

124. For the sake of completeness, I note that the respondent provided the OAIC with the Service Provider's privacy policies, which, since an update published on 20 May 2021, describe the collection of facial images and faceprints and provide a more detailed description of the purpose of collection. For the reasons set out in paragraph 98, I do not consider that this satisfies the respondent's obligations under APP 5.

Finding of breach – APP 5

125. I find that, during the Relevant Period the respondent interfered with the privacy of individuals whose facial images and faceprints it collected, by failing to take reasonable steps to notify individuals about the fact and circumstances of collection and the purposes of collection of that information, in breach of APP 5.

Remedies

126. There are a range of regulatory options that I may take following an investigation commenced on my own initiative. In determining what form of regulatory action to take, I have considered the factors outlined in the OAIC's Privacy Regulatory Action Policy[95] and the OAIC's Guide to Privacy Regulatory Action.[96]

127. I consider that the following factors weigh in favour of making a determination that finds that the respondent has engaged in conduct constituting an interference with the privacy of an individual and must not repeat or continue such conduct:

a. The objects in s 2A of the Act include promoting the protection of the privacy of individuals, and promoting responsible and transparent handling of personal information by entities.[97]

b. The conduct is serious:

[94] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 5.
[95] Privacy Regulatory Action Policy [38].
[96] Guide to Privacy Regulatory Action [4.9].
[97] Privacy regulatory Action Policy at [38].

i. Although the exact number of affected Australians is unknown, that number is likely to be very large, given that, as at March 2021, approximately 1.6 million survey responses had been completed.

ii. The matter involves the sensitive biometric information of all the affected Australian individuals.[98]

c. The burden on the respondent likely to arise from the regulatory action is justified by the risk posed to the protection of personal information.[99]

d. There is specific and general educational, deterrent or precedential value in making a determination in this matter. [100]

e. There is a disagreement between the OAIC and the respondent about whether an interference with privacy has occurred, and this determination allows this question to be resolved.[101]

f. There is a public interest in making declarations setting out my reasons for finding that an interference with privacy has occurred and the appropriate response by the respondent.

Specified steps

128. Under s 52(1A)(b) I may declare that the respondent must take specified steps within a specified period to ensure that an act or practice investigated under s 40(2) is not repeated or continued.

129. I appreciate the respondent's cooperation with this investigation, and the candour of its submissions in response to the OAIC's inquiries.

130. I also acknowledge that after receiving the preliminary view, the respondent asked the Service Provider to disable image capturing on the tablet devices in its stores, and am advised that the Service Provider has done so.[102]

131. On this basis, I am satisfied that the respondent is no longer collecting individuals' facial images and faceprints through its customer feedback mechanism. Accordingly I do not need to make a declaration to cease the conduct.

132. I have taken account of the respondent's submissions that facial images are stored for 20 seconds on tablets before being transferred to the Server and that facial images are stored on the Server for only 7 days. As more than 7 days have passed since the respondent ceased collecting these images, I am satisfied that the respondent no longer holds any facial images collected by the Facial Recognition Tool. Accordingly, I do not need to make a declaration that those images are deleted.

133. While acknowledging these proactive steps, I remain concerned that faceprints collected by the Facial Recognition Tool in breach of APPs 3.3 and 5, have not been deleted. I am not satisfied that de-identification is a viable step in the circumstances, noting that the purpose of the Facial Recognition Tool is to enable automated biometric identification of individuals.

---

[98] Privacy regulatory Action Policy at [38].
[99] Privacy regulatory Action Policy at [38].
[100] Privacy regulatory Action Policy at [38].
[101] Guide to Privacy Regulatory Action at [4.9].
[102] R4 – Email from respondent to the OAIC dated 2 September 2021.

134. I acknowledge the respondent's submission that '[a]fter 24 hours, the faceprint effectively expires' and any attempt to identify a match using the Similarity API would result in an error.[103] However, given the respondent did not make any submissions in relation to the draft declaration requiring it to destroy faceprints, there is insufficient evidence before me to be satisfied that the faceprints have been irretrievably destroyed, or if this is not possible, put beyond use. Personal information is put beyond use where an entity:

- is not able, and will not attempt, to use or disclose the personal information
- cannot give any other entity access to the personal information
- surrounds the personal information with appropriate technical, physical and organisational security (including, at a minimum, access controls including logs and audit trails)
- commits to take reasonable steps to irretrievably destroy the personal information if, or when, this becomes possible. [104]

135. Accordingly, I make a declaration requiring the respondent to destroy, or cause to be destroyed, all faceprints it has collected through the customer feedback mechanism, in breach of APPs 3.3 and 5, to ensure this act or practice is not continued. I am also requiring the respondent to provide written confirmation to the OAIC when it has complied with this declaration. I am satisfied that this is a reasonable and appropriate remedy in the circumstances.

Angelene Falk
Australian Information Commissioner and Privacy Commissioner

29 September 2021

Review rights

A party may apply under s 96 of the *Privacy Act 1988* (Cth) to have a decision under s 52(1) or (1A) to make a determination reviewed by the Administrative Appeals Tribunal (AAT). The AAT provides independent merits review of administrative decisions and has power to set aside, vary, or affirm a privacy determination. An application to the AAT must be made within 28 days after the day on which the person is given the privacy determination (s 29(2) of the Administrative Appeals Tribunal Act 1975). An application fee may be payable when lodging an application for review to the AAT. Further information is available on the AAT's website (www.aat.gov.au) or by telephoning 1300 366 700.

A party may also apply under s 5 of the *Administrative Decisions (Judicial Review) Act 1977* to have the determination reviewed by the Federal Circuit Court or the Federal Court of Australia. The Court may refer the matter back to the OAIC for further consideration if it finds the Information Commissioner's decision was wrong in law or the Information Commissioner's powers were not exercised properly. An application to the Court must be lodged within 28 days of the date of the determination. An application fee may be payable when lodging an application to the Court. Further information is

[103] R2.1 – Letter from the respondent to the OAIC dated 25 March 2021 p 8.
[104] APP guidelines, chapter 11, [11.38] – [11.39], available at: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-11-app-11-security-of-personal-information/

available on the Court's website (www.federalcourt.gov.au/) or by contacting your nearest District Registry.

Corrigendum

1) At paragraphs 45 and 80, delete 'biometric information collected for use in automated biometric verification and identification systems' and replace with 'biometric information that is to be used for the purpose of automated biometric verification or biometric identification'
2) At paragraph 46, delete ', 'biometric systems''
3) At paragraph 82, delete quotation marks around 'automated biometric identification system'.

Attachment A

Relevant Law – *Privacy Act 1988* (Cth)

Determination powers

52 Determination of the Commissioner

(1) After investigating a complaint, the Commissioner may:

(a) make a determination dismissing the complaint; or

(b) find the complaint substantiated and make a determination that includes one or more of the following:

(i) a declaration:

(A) where the principal executive of an agency is the respondent—that the agency has engaged in conduct constituting an interference with the privacy of an individual and must not repeat or continue such conduct; or

(B) in any other case—that the respondent has engaged in conduct constituting an interference with the privacy of an individual and must not repeat or continue such conduct;

(ia) a declaration that the respondent must take specified steps within a specified period to ensure that such conduct is not repeated or continued;

(ii) a declaration that the respondent must perform any reasonable act or course of conduct to redress any loss or damage suffered by the complainant;

(iii) a declaration that the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint;

(iv) a declaration that it would be inappropriate for any further action to be taken in the matter.

APP entity

6 Interpretation
In this Act, unless the contrary intention appears:
…
APP entity means an agency or organisation.

Interference with privacy

13 Interferences with privacy
APP entities
(1) An act or practice of an APP entity is an interference with the privacy of an individual if:
(a) the act or practice breaches an Australian Privacy Principle in relation to personal information about the individual; or

(b) the act or practice breaches a registered APP code that binds the entity in relation to personal information about the individual.

…

APP compliance

15 APP entities must comply with Australian Privacy Principles

An APP entity must not do an act, or engage in a practice, that breaches an Australian Privacy Principle.

Personal information

6 Interpretation

In this Act, unless the contrary intention appears:

…personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

3 Australian Privacy Principle 3—collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency—the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation—the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the APP entity; or

(c) the APP entity is an organisation and a permitted health situation exists in relation to the collection of the information by the entity; or

(d) the APP entity is an enforcement body and the entity reasonably believes that:

(i) if the entity is the Immigration Department—the collection of the information is reasonably necessary for, or directly related to, one or more enforcement related activities conducted by, or on behalf of, the entity; or

(ii) otherwise—the collection of the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(e) the APP entity is a non-profit organisation and both of the following apply:

(i) the information relates to the activities of the organisation;

(ii) the information relates solely to the members of the organisation, or to individuals who have regular contact with the organisation in connection with its activities.

Note: For ***permitted general situation***, see section 16A. For ***permitted health situation***, see section 16B.

Means of collection

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Solicited personal information

3.7 This principle applies to the collection of personal information that is solicited by an APP entity.

5 Australian Privacy Principle 5—notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or

(b) to otherwise ensure that the individual is aware of any such matters.

5.2 The matters for the purposes of subclause 5.1 are as follows:

(a) the identity and contact details of the APP entity;

(b) if:

(i) the APP entity collects the personal information from someone other than the individual; or

(ii) the individual may not be aware that the APP entity has collected the personal information;

the fact that the entity so collects, or has collected, the information and the circumstances of that collection;

(c) if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);

(d) the purposes for which the APP entity collects the personal information;

(e) the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;

(f) any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;

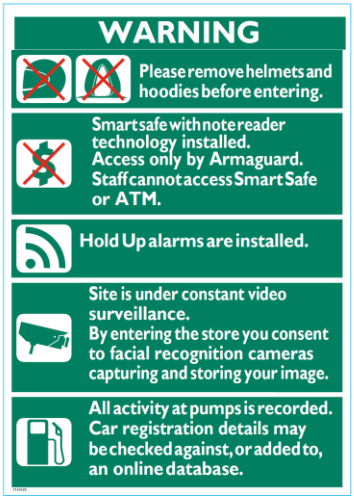
(g) that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;

(h) that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;

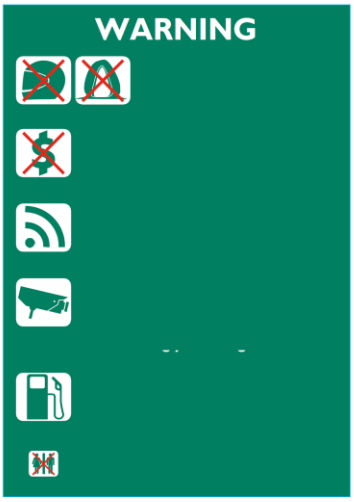
(i) whether the APP entity is likely to disclose the personal information to overseas recipients;

(j) if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

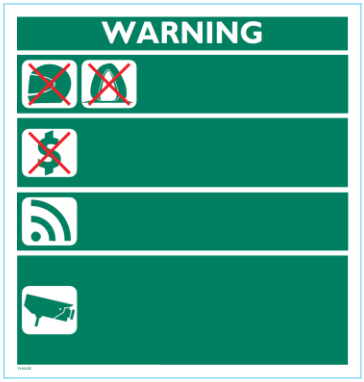
Attachment B



Fuel Site - Code 7110125



Fuel Site (no restroom) - Code 7110712



Non Fuel Site - Code 7110126