Commissioner Initiated Investigation into the Australian Federal Police (Privacy) [2021] AICmr 74 (26 November 2021)

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

Respondent	Australian Federal Police
Decision date	26 November 2021
Case reference number	CII20/00010
Catchwords	Privacy — *Privacy Act 1988* (Cth) — Australian Privacy Principles — APP 1.2 — Privacy (Australian Government Agencies – Governance) APP Code 2017 – whether a privacy impact assessment was conducted for a high privacy risk project – whether reasonable steps taken to implement practices, procedures and systems to ensure compliance with the Code – breaches substantiated – independent review required.

Determination

1. I find that the Australian Federal Police (**Respondent**), interfered with the privacy of individuals whose personal information was disclosed to a third party facial recognition service provider, within the meaning of the *Privacy Act 1988* (Cth), by:
   a. failing to conduct a privacy impact assessment (**PIA**) for a high privacy risk project in breach of clause 12 of the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (the **Code**)
   b. failing to comply with the requirement in Australian Privacy Principle (**APP**) 1.2 in Schedule 1 of the Privacy Act, to take reasonable steps to implement practices, procedures and systems relating to the entity's functions or activities, to ensure compliance with clause 12 of the Code.

Declarations

2. I make the following declarations under the Privacy Act:
    a. I declare under s 52(1A)(a)(i) that the Respondent interfered with the privacy of individuals by breaching APP 1.2 and clause 12 of the Code in the manner described at paragraph 1.
    b. I declare under s 52(1A)(a)(ii) that the Respondent must not repeat or continue the acts and practices referred to at paragraph 1.
    c. I declare under s 52(1A)(b) that the Respondent must take the following steps to ensure that the acts and practices are not repeated or continued:
        i. within 3 months of the date of this determination, engage an independent third party assessor, with demonstrated capacity in assessing the requirements for compliance with the Privacy Act
        ii. engage the assessor to review the Respondent's practices, procedures and systems (including changes made since use of the third party facial recognition service) against the requirement in APP 1.2 to take reasonable steps in the circumstances to implement practices, procedures and systems (including training) relating to the entity's functions or activities that will ensure compliance with clause 12 of the Code. The assessor is to consider the deficiencies outlined in paragraphs 95 – 105 and the reasonable steps outlined in paragraphs 106 – 109
        iii. require the assessor to complete its review and prepare a written report within 6 months of the date of this determination, which specifies:
            A. any deficiencies in the reasonable steps taken by the Respondent to implement practices, procedures and systems (including training) to ensure compliance with clause 12 of the Code
            B. actions for the Respondent to take to address the deficiencies (if any)
        iv. provide the Office of the Australian Information Commissioner (**OAIC**) with a copy of the report, within 2 weeks of receiving the report
        v. provide the OAIC with a timeline for implementing any actions set out in the report (and any other actions proposed by the Respondent), within 4 weeks of receiving the report
        vi. implement the actions set out in the report within the timeframes specified, but in any event, within 10 months of the date of this determination, and provide notification to the OAIC when all actions are complete
        vii. within 12 months of the date of the determination, ensure that all personnel that handle personal information and are employed by, or in the service of, the Respondent, have completed an updated privacy training program which addresses the deficiencies outlined in paragraphs 99 – 103
        viii. engage the assessor to assess whether the actions in its report have been implemented, and within 12 months of the date of this determination, provide a supplementary report to the OAIC specifying whether the actions have been implemented, including the training referred to in paragraph vii.

Findings and reasons

Background

3. The Respondent is an Australian government agency whose role is to enforce criminal law at the Commonwealth level.

4. The Respondent leads the Australian Centre to Counter Child Exploitation (**ACCCE**), which brings together resources from government, law enforcement agencies, non-government organisations and other partners to prevent and disrupt exploitation of children, and particularly, organised child sexual exploitation networks operating in the online environment.[1]

5. The Respondent submitted that members of the ACCCE became aware that other law enforcement agencies had used a third party's facial recognition tool (the **Facial Recognition Tool**), to successfully identify several individuals.[2] On that basis, in the period 2 November 2019 to 22 January 2020 (the **Trial Period**), 10 members of the ACCCE registered for trial accounts, and 7 of these members used the Facial Recognition Tool to conduct searches (the **Trial participants**).[3]

6. The Facial Recognition Tool was provided by a third party based in the United States. Registered users could upload a facial image and run a search against that image. The tool displayed possible matches to the uploaded image (as well as associated source information), after searching its database of more than 3 billion images.[4]

7. The third party provided the tool to the Respondent on a 'free trial' basis. The Respondent did not adopt the Facial Recognition Tool as an enterprise product and did not enter into any formal procurement arrangements with the third party service provider.[5]

Searches using the Facial Recognition Tool

8. Trial participants uploaded publicly available images (such as from media articles) and images of ACCCE members, to the Facial Recognition Tool. They also uploaded images that were derived from images distributed using underground marketplaces on the internet (such as the dark web).[6] The images were uploaded to test the efficacy of the tool, and to investigate serious child exploitation offences.[7]

---

[1] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 1.
[2] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 2.
[3] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 2, 4; R5 – Letter from the Respondent to the OAIC dated 1 June 2021 p 4.
[4] R2 – Attachment A to the letter from the Respondent to the OAIC dated 14 August 2020 p 2, 7 – 9; R2.1 – Letter from the Respondent to the OAIC dated 14 August 2020. See also *Commissioner Initiated Investigation into Clearview AI Inc.* (Privacy) [2021] AICmr54 (14 October 2021) at [4]
[5] Submission to Parliamentary Joint Committee on Intelligence and Security, *Review of Mandatory Data Retention Regime*, submission 15.1, p 5, available online at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Dataretentionregime/Submissions
[6] R5 – Letter from the Respondent to the OAIC dated 1 June 2021 p 4.
[7] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 2.

9. At the time of the OAIC investigation, the Respondent did not hold any logs recording details of access and/ or use of the Facial Recognition Tool by the Trial participants. For many uploaded images, the Respondent also did not have a record of the particular image that had been uploaded. Based on the information provided, the Trial participant's searches included images of possible persons of interest, an alleged offender, victims, members of the public and members of the Respondent.[8]

10. The Respondent did not undertake a privacy impact assessment (**PIA**) in relation to the Facial Recognition Tool before or during the Trial Period.[9] A PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.

11. Outside of the ACCCE operational command, there was no visibility of this limited trial.[10]

Awareness about use of the Facial Recognition Tool

12. On 18 January 2020, a media article was published about the Facial Recognition Tool and its use by law enforcement agencies.[11]

13. On 21 January 2020, a spokesperson for the Respondent was reported to have advised media that the Respondent does not use the Facial Recognition Tool.[12] In a subsequent internal email to the ACCCE Coordinator of Operations, a member of the Respondent referred to the media article and noted that the ACCCE was using the Facial Recognition Tool.[13]

14. Later that day the ACCCE Coordinator of Operations sent an email requesting information on the ACCCE's use of the Facial Recognition Tool, including details of who had approved the use of the software, and what validation process was followed to ensure information security. The email states: 'For clarity there should be no software used without the appropriate clearance for use.'[14]

15. The Respondent received three requests under the *Freedom of Information Act 1982* (**FOI Act**), seeking documents it held relating to the Facial Recognition Tool.[15] In processing the requests, the Respondent initially did not identify any information relating to the third party service provider and accordingly, refused the FOI requests on 14 February 2021.[16]

---

[8] R5 – Letter from the Respondent to the OAIC dated 1 June 2021 pp 12-16.
[9] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 6.
[10] R5 – Letter from the Respondent to the OAIC dated 1 June 2021 p 6-7.
[11] Hill, K. 'The Secretive Company that Might End Privacy as We Know It,' *New York Times,* 18 January 2020, available at: https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html
[12] R5.3 – Attachment C to the letter from the Respondent to the OAIC dated 1 June 2021 p 2. News Article available online at: https://www.gizmodo.com.au/2020/0l/facial-recognition-australian-federal-police-afp-clearview-ai/
[13] R5.3 – Attachment C to the letter from the Respondent to the OAIC dated 1 June 2021 p 2.
[14] R5.3 – Attachment C to the letter from the Respondent to the OAIC dated 1 June 2021 p 2.
[15] Submission to Parliamentary Joint Committee on Intelligence and Security *Review of Mandatory Data Retention Regime*, submission 15.1 (**PJCIS submission**) p 6, available online at: https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Dataretentionregime/Submissions
[16] PJCIS submission p 6.

The Respondent subsequently found that the ACCCE held information relevant to the third party, which had not been identified in response to the earlier FOI requests.[17]

Steps to address issues since the Trial

16. The Respondent submitted that in March 2020, it engaged a third party to review the handling of personal information by Trial participants and report whether the application interfered with individuals' privacy. The review identified that the collection, use and disclosure of personal information by Trial participants was for legitimate purposes relating to the Respondent's statutory functions as a law enforcement agency, or otherwise with the consent of the individual concerned.[18]

17. On 22 May 2020, the Respondent wrote to the third party service provider requesting confirmation that all user accounts associated with the Respondent had been deleted. [19]

18. On 16 June 2020, the third party service provider confirmed in writing that all user accounts associated with the Respondent had been deleted, and all user data relating to those accounts (including any associated images) had been removed from its systems.[20]

19. The Respondent also submitted that:

- It is undertaking a review of existing internal governance processes and documents to specifically address the use of free trials in the online environment.[21]
- It has commissioned a broader review of the Respondent's privacy governance with the assistance of an external legal services provider, which included preparing an updated privacy management framework.[22]
- Its training module is currently under review to ensure operational relevance to all staff by including sufficient context and explanation.[23]
- It has appointed a dedicated position within the ACCCE, who is responsible for undertaking software evaluations of similar kinds of applications in future.[24]

The Law

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

21. 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.

22. The Respondent is an 'agency' under s 6(1) of the Privacy Act.

23. The Code commenced on 1 July 2018. It is a written code of practice about information privacy, that was developed under section 26G of the Privacy Act. It sets out how APP 1.2

[17] PJCIS submission p 6.
[18] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 3.
[19] R5 – letter from the Respondent to the OAIC dated 1 June 2021 pp 4-8.
[20] R5.4 – Attachment D to the letter from the Respondent to the OAIC dated 1 June 2021 p 1-4.
[21] R6 – Letter from the Respondent to the OAIC dated 12 July 2021 p 2.
[22] R6 – Letter from the Respondent to the OAIC dated 12 July 2021 p 2.
[23] R5 – letter from the Respondent to the OAIC dated 1 June 2021 p 10.
[24] R6 – Letter from the Respondent to the OAIC dated 12 July 2021 p 2.

is to be complied with by agencies (in addition to complying with the Code, an agency may need to take additional steps in order to satisfy its obligations under APP 1.2.)[25]

24. The Code is a binding legislative instrument under the Privacy Act. It applies to all Australian Government agencies subject to the Privacy Act (except for Ministers).[26] This includes the Respondent.

25. An act or practice of an APP entity is an interference with the privacy of an individual if the act or practice breaches an APP in relation to personal information about the individual, or the act or practice breaches a registered APP code that binds the entity in relation to personal information about the individual (s 13(1) of the Privacy Act).

26. The provisions relevant to my determination are APP 1.2, and clause 12 of the Code. The relevant provisions are set out in full at **Attachment A.**

27. Section 52(1A) provides that, after investigating an act or practice of a person or entity under s 40(2), I may make a determination that includes one or more of the following:

    a. 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[27]

    b. 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[28]

    c. 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[29]

    d. 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[30]

    e. a declaration that it would be inappropriate for any further action to be taken in the matter.[31]

Investigation by the OAIC

28. On 7 July 2020, the OAIC sent preliminary inquiries to the Respondent under s 42(2) of the Privacy Act. The Respondent provided a written response on 14 August 2020.

29. On 29 March 2021, the OAIC notified the Respondent under s 43(1) that the Commissioner would commence an investigation under s 40(2) of the Privacy Act.

30. On 30 March 2021 the Commissioner notified the Respondent that the Commissioner had commenced an investigation under s 40(2).

31. The investigation focused on whether the following acts and practices by the Respondent breached clause 12 of the Code and/or APP 1.2:

    - the Respondent's handling of personal information in relation to the Trial
    - the Respondent's internal practices, procedures, and systems in relation to conducting PIAs

---

[25] *Privacy (Australian Government Agencies – Governance) APP Code 2017*, clause 8.
[26] *Privacy (Australian Government Agencies – Governance) APP Code 2017*, clause 7.
[27] *Privacy Act 1988* (Cth) (**Privacy Act**), s 52(1A)(a).
[28] Privacy Act, s 52(1A)(b).
[29] Privacy Act, s 52(1A)(c).
[30] Privacy Act, s 52(1A)(d).
[31] Privacy Act, s 52(1A)(e).

- the Respondent's failure to undertake a PIA before undertaking the Trial.

32. Following the conclusion of this investigation, the OAIC sent its preliminary view to the respondent on 29 June 2021, setting out preliminary findings, reasons and draft declarations. The respondent provided a response to the preliminary view on 12 July 2021, which I have considered in making this determination.

Material considered

33. In making this determination, I have considered:

- 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**) [32]
- the OAIC's Privacy Regulatory Action Policy[33]
- the OAIC's Guide to Privacy Regulatory Action, July 2020. [34]

34. While not legally binding, the APP Guidelines outline the mandatory requirements of the APPs, how the Information Commissioner will interpret the APPs, and matters the Information Commissioner may consider when exercising their functions and powers under the Privacy Act.

Findings on breach

Clause 12 of the Code – conduct a PIA

Law

35. The Respondent is required to conduct a privacy impact assessment in the following circumstances under clause 12 of the Code:

> 12 Conduct of privacy impact assessment (PIA)
>
> 1. An agency must conduct a PIA for all high privacy risk projects.
>
> 2. For the purposes of this section, a project may be a high privacy risk project if the agency reasonably considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.
>
> Note: 'Privacy impact assessment' is defined in section 33D of the Act. This section of the Act also requires an agency to conduct a PIA if directed to do so by the Commissioner.

36. Section 33D of the Privacy Act states:

---

[32] APP Guidelines (updated 22 July 2019), available online at Australian Privacy Principles guidelines — OAIC.

[33] The Privacy Regulatory Action Policy is available online at: https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/.

[34] OAIC Guide to Privacy Regulatory Action (updated June 2020), available online at Guide to privacy regulatory action — OAIC.

> (3) A privacy impact assessment is a written assessment of an activity or function that:
>
> > (a) identifies the impact that the activity or function might have on the privacy of individuals; and
> >
> > (b) sets out recommendations for managing, minimising or eliminating that impact.

37. The OAIC has published general guidance about PIAs, as well as guidance explaining when agencies need to conduct a PIA.[35]
38. The OAIC's general guidance explains that a PIA is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.
39. It notes that undertaking a PIA is an essential tool in adopting a 'privacy by design' approach to innovation, and can assist entities to:
    - describe how personal information flows in a project
    - analyse the possible impacts on individuals' privacy
    - identify and recommend options for avoiding, minimising or mitigating negative privacy impacts
    - build privacy considerations into the design of a project
    - achieve the project's goals while minimising the negative and enhancing the positive privacy impacts.
40. The OAIC's guidance for agencies includes information about threshold assessments:

> A threshold assessment is a preliminary assessment to help you determine your project's potential privacy impacts and give you a sense of the risk level, including whether it could be a 'high privacy risk project' requiring a PIA under the Code.
>
> You should undertake a threshold assessment if your project involves new or changed ways of handling personal information.
>
> A threshold assessment is not intended to establish the actual level of risk – that is the job of the PIA to assess in more detail. Instead, the purpose is to screen for factors that point to the potential for a high privacy risk, which will require a PIA to be conducted under the Code.
>
> Not every project will need a PIA. A threshold assessment will quickly and easily identify projects with no, or minimal, information privacy implications.

[35] OAIC guide to undertaking privacy impact assessments, available online: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/ and OAIC guide, 'When do agencies need to conduct a privacy impact assessment?', available online at: https://www.oaic.gov.au/privacy/guidance-and-advice/when-do-agencies-need-to-conduct-a-privacy-impact-assessment/.

> Regardless of whether you proceed to a PIA, you should keep a record of the threshold assessment. [36]

Submissions

41. The Respondent submitted:

- Since the commencement of the Code, the Respondent's usual practice is to record assessments of privacy risk in a designated PIA. The Respondent did not prepare a PIA prior to or during the Trial. In this instance, the members of ACCCE considered privacy issues through other risk assessment mechanisms.[37]
- The risk assessment mechanisms it applied were:

> In this instance, relevant members of the ACCCE considered use of the Application for a limited trial taking into account that framework, as well as their duties and responsibilities as law enforcement officers responsible for child protection operations.[38]

- The Trial was a 'limited trial' because:
  - A limited cohort of members within the ACCCE registered for the trial (rather than all members of the ACCCE or the Command more broadly).
  - The Facial Recognition Tool was only used for a short period of time (less than three months).
  - The Facial Recognition Tool was only used for a specific purpose – to ascertain the accuracy and effectiveness of the algorithm, particularly in the context of side profile photographs.
  - The Facial Recognition Tool was only used in a few instances (not for every investigation during the period or adopted for broad operational use) and not all trial accounts were used.
  - The images that were used during the Trial had been distributed using underground marketplaces on the internet (such as the dark web), were publicly available (such as from media articles), or were provided directly by the individual depicted in the image with their consent.[39]
- Use of the Facial Recognition Tool in these circumstances can be distinguished from any formal procurement of the tool as an enterprise product. If the Trial proved successful and the Respondent decided to adopt the application as an enterprise product, the prescribed procurement process would have been actioned. That process would have required a formal and comprehensive PIA to be completed.[40]
- The Trial participants considered that the risks were manageable in the context of the 'limited trial', and were outweighed by the need to share intelligence and information

[36] OAIC guide, 'When do agencies need to conduct a privacy impact assessment?', available online at: https://www.oaic.gov.au/privacy/guidance-and-advice/when-do-agencies-need-to-conduct-a-privacy-impact-assessment/ .
[37] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 6.
[38] R5 – Letter from the Respondent to the OAIC dated 1 June 2021 p 8.
[39] R5 – Letter from the Respondent to the OAIC dated 1 June 2021 p 4.
[40] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 6.

to best identify offenders and remove children from harm, and to respond to such matters in a timely manner.[41]

- It has not identified any document(s) recording any contemporaneous risk assessment.[42]
- When asked about whether the Privacy Officer had been consulted at any time prior to, at the time of, and/or after the Trial, the Respondent advised that 'outside of the ACCCE operational command, there was no visibility this limited trial had commenced'.[43]

42. The Respondent provided copies of relevant policies that applied during the Trial period. These included:

- the AFP National Guideline on privacy, which stated:
  - The Privacy Code requires the AFP to conduct PIAs for all new or changed projects with a high privacy risk.
  - In order to determine whether a new project has a high privacy risk and requires a PIA to be conducted, AFP personnel should conduct a threshold assessment for a PIA.
  - AFP personnel may also contact the Privacy Officer for assistance in determining whether a PIA is required.[44]
- the 'Better Practice Guide - Undertaking Privacy Impact Assessments', which:
  - referenced and hyperlinked to the OAIC's 'Guide to undertaking Privacy Impact Assessments' (**OAIC PIA Guide**), and recommended that the AFP Guide be read in conjunction with the OAIC PIA Guide[45]
  - referenced paying the costs of any external support required to complete a PIA
  - referenced the Code requirement for agencies to undertake a written PIA for all 'high privacy risk' projects or initiatives that involve new or changed ways of handling personal information (and noted the definition of project should be taken broadly)
  - included a PIA template which provides employees with guidance on developing a PIA
  - provided contact details of the Respondent's Privacy Officer, who, according to the guide, is available to provide guidance on matters associated with PIAs
  - noted that undertaking a threshold assessment is the first step in the PIA process to assist in determining whether a PIA is necessary for a new project, and should be 'routinely conducted for every high privacy impact project undertaken by the AFP'

[41] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 8.
[42] R5 – Letter from the Respondent to the OAIC dated 1 June 2021 p 8.
[43] R5 – Letter from the Respondent to the OAIC dated 1 June 2021 p 6-7.
[44] R5.8 – Attachment H to the letter from the Respondent to the OAIC dated 1 June 2021 p 9.
[45] OAIC Guide to undertaking Privacy Impact Assessments available online at: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/

- included a link to a document entitled 'Threshold Assessment for undertaking a PIA' which outlined the considerations involved in undertaking a Threshold Assessment
- noted that the project manager should complete and keep a record of the threshold Assessment for any new AFP project with high privacy risks, regardless of whether a PIA is undertaken after the PIA threshold assessment has been completed
- referred to the project's complexity and privacy scope as having an impact on the likelihood that a comprehensive PIA is required to determine and manage its privacy impacts. [46]

- The Respondent also provided other documents, such as an all-staff communication, Privacy Management Plan and National Manager's forum paper, which referred to the obligation to conduct a PIA.[47]

Consideration

43. The Respondent acknowledged and I am satisfied that it did not undertake a PIA before the Trial, or at any point during the Trial.

44. Having regard to the Respondent's submissions outlined above, I do not accept that a PIA was not required under the Code in the circumstances.

45. Clause 12 of the Code requires agencies to conduct a PIA for all high privacy risk projects. This applies irrespective of whether a high privacy risk project involves paid services or a free trial.

46. The specific requirements of the Code are addressed below.

Was the Respondent's use of the Facial Recognition Tool a 'project' under the Code?

47. The term 'project' is not defined in the Code or the Privacy Act.

48. OAIC guidance explains that a 'project' covers the full range of activities and initiatives undertaken by agencies that may have privacy implications.[48] This could include new or changed programs or activities, implementing IT systems or databases, new or changed methods or procedures for service delivery or information handling, or implementing artificial intelligence technologies.[49]

[46] R2.7 – Attachment G to the letter from the Respondent to the OAIC dated 14 August 2020 pp 2-3.

[47] R5.9 – Attachment I to the letter from the Respondent to the OAIC dated 1 June 2021; R5.10 – Attachment J to the letter from the Respondent to the OAIC dated 1 June 2021.

[48] OAIC guide, 'When do agencies need to conduct a privacy impact assessment?', available online at: https://www.oaic.gov.au/privacy/guidance-and-advice/when-do-agencies-need-to-conduct-a-privacy-impact-assessment/

[49] OAIC guide, 'When do agencies need to conduct a privacy impact assessment?', available online at: https://www.oaic.gov.au/privacy/guidance-and-advice/when-do-agencies-need-to-conduct-a-privacy-impact-assessment/.

49. The Trial participants used the Facial Recognition Tool to upload images received or collected by the Respondent, to a third party application for the purposes of searching a facial recognition database.[50]

50. I consider that this activity was a 'project' under clause 12 of the Code.

Did the project involve the handling of 'personal information'?

51. 'Personal information' means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not, and
- whether the information or opinion is recorded in a material form or not.[51]

52. 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.[52]

53. 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.[53]

54. 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.

55. 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.[54] An individual can be reasonably identifiable, by any person (or machine) other than the subject themselves.

---

[50] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 2, 7-9; R2.1 – Attachment A to the letter from the Respondent to the OAIC dated 14 August 2020. See also the third party's website, available online at: https://clearview.ai/ and 'How Does Clearview AI's Facial Search Technology Work?' https://clearview.ai/law-enforcement.

[51] Privacy Act, s 6(1).

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

[53] 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.

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

56. In this case, the images uploaded to the Facial Recognition Tool depicted individuals. As these images show individuals' facial images, I am satisfied that they were 'about' an individual.

57. Also, considering the circumstances in which the images were obtained by the Respondent, and in some cases, other information held by the Respondent about the individuals depicted in the images, I consider that the images revealed information about, or enable an opinion to be formed about, whether the individual in the image was a suspect, a possible victim, a person of interest, or member of the Respondent.

58. I am also satisfied that an individual is '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.
- As noted above at paragraphs 8 - 9, the Respondent used the Facial Recognition Tool for the purpose of identifying unknown individuals, including persons of interest and victims of crime.[55] Possible matches or matches were displayed on at least 7 occasions.[56]

59. For these reasons, I consider that images uploaded by Trial participants to the Facial Recognition Tool, as well as images disclosed to the Respondent by that tool, were 'personal information' as defined in s 6(1) of the Privacy Act.

Did the Respondent undertake a threshold assessment?

60. As stated in paragraph 35, clause 12 of the Code requires an agency to conduct a PIA for all high privacy risk projects.

61. For projects involving new or changed ways of handling personal information, entities need to screen for factors pointing to potential for a high privacy risk. A threshold assessment is a preliminary assessment which helps entities determine a project's potential privacy impacts and provides a sense of the risk level (not the actual level of risk, which is considered in a PIA).[57]

62. Under the Respondent's written policies, the project manager was responsible for completing and documenting a threshold assessment.[58]

63. However, the Respondent provided no evidence that any project manager or Trial participant conducted a threshold assessment to determine whether a PIA was required.

64. There is no evidence that Trial participants were aware that a threshold assessment should be conducted for a project involving new or changed personal information handling, to determine whether a PIA is required.

65. On the contrary, the Respondent submitted that privacy issues were assessed by Trial participants through 'other risk assessment mechanisms'. However, the Respondent

---

[55] See the third party's website available online at: https://clearview.ai/law-enforcement

[56] R5 – Letter from the Respondent to the OAIC dated 1 June 2021 p 12-16.

[57] R5.8 – Attachment H to the letter from the Respondent to the OAIC dated 1 June 2021 p 9; R2.7 – Attachment G to the letter from the Respondent to the OAIC dated 14 August 2020 p 2-3.

[58] R2.7 – Attachment G to the letter from the Respondent to the OAIC dated 14 August (AFP *Better Practice Guide – Undertaking Privacy Impact Assessments)*

could not identify any documents recording any such assessments.[59] There is no evidence that the Trial participants, or any other members of the Respondent, systematically assessed factors pointing to the potential for a high privacy risk before or during the Trial.

66. For the above reasons, I am not satisfied that the Respondent undertook a threshold assessment to determine whether a PIA was required under the Code.

Did the project involve new and changed ways of handling personal information?

67. The evidence shows that:

- The Facial Recognition Tool is a novel technology involving a new way of handling personal information. Its users can upload a digital image of an individual's face and run a search against it. The third party service provider applies its facial recognition algorithm to the image and runs the result against its database, which contains more than 3 billion images, to identify and display likely matches and associated source information.[60]
- The Respondent acknowledged that part of the rationale for testing the Facial Recognition Tool was to use 'new and innovative solutions' to meet challenges posed by offenders evolving their operating methods to avoid detection.[61]

68. Having considered the above factors, I am satisfied that the Trial involved new and changed ways of handling personal information.

Was the project likely to have a significant impact on the privacy of individuals?

69. A privacy impact is anything that could adversely affect individuals' information privacy, including interferences such as the collection of new or additional types of personal information, or when the handling of personal information results in an individual losing control over their personal information.

70. An impact on the privacy of individuals will be 'significant' if the consequences of the impact are considerable, having regard to their nature and severity.[62]

71. I consider that the following factors should have indicated that the project was likely to have a significant impact on individuals' privacy:

- The Trial participants disclosed individuals' images to a third party that is located and incorporated overseas,[63] without assessing the third party's security practices or the accuracy of its Facial Recognition Tool.

---

[59] R5 – Letter from the Respondent to the OAIC dated 1 June 2021 p 8.

[60] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 2, 7-9; R2.1 – Letter from the Respondent to the OAIC dated 14 August 2020 Attachment A. See also *Commissioner Initiated Investigation into Clearview AI Inc.* (Privacy) [2021] AICmr54 (14 October 2021) [4]

[61] R5 – Letter from the Respondent to the OAIC dated 1 June 2021 p 2; R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 1.

[62] OAIC guide, 'When do agencies need to conduct a privacy impact assessment?', available online: https://www.oaic.gov.au/privacy/guidance-and-advice/when-do-agencies-need-to-conduct-a-privacy-impact-assessment/#part-2-determining-whether-there-is-the-potential-for-a-high-privacy-risk

[63] See the third party's website, available online at: https://clearview.ai/ and https://clearview.ai/law-enforcement.

- The Respondent did not enter a Commonwealth contract[64] with the third party, before participants used the Facial Recognition Tool. If it had entered a Commonwealth contract with that third party, the Privacy Act would have required the contract to include contractual measures to ensure that the contracted service provider does not do an act, or engage in a practice, that would breach an APP if done or engaged in by the agency.[65] In the absence of a Commonwealth contract, no such contractual measures were in place to ensure Australians' privacy was protected in the event the third party service provider did not comply with the Act.
- The Respondent should reasonably have surmised, based on the nature of the Facial Recognition Tool, that the third party service provider may handle sensitive biometric information.[66] Sensitive information is generally afforded a higher level of privacy protection under the APPs than other personal information, in recognition of the adverse consequences that may arise from inappropriate handling.[67]
- There was a significant risk of adversity for Australians whose sensitive information was uploaded to the Facial Recognition Tool, including a loss of control of personal information where an Australian law enforcement agency sent an individual's facial image to an overseas company; a risk of identity fraud if their immutable biometric information was compromised; harms arising from the potential misidentification of a victim, suspect or person of interest by law enforcement (such as loss of rights or freedoms and reputational damage); and the risk of reputational damage that may flow from a data breach of information linking a person to a law enforcement search.
- While the Privacy Act recognises that the protection of individuals' privacy is not an absolute right, instances of interference, including for law enforcement objectives, must be subject to a careful and critical assessment of necessity, reasonableness and proportionality.[68] During the investigation, the Facial Recognition Tool reportedly included more than 3 billion images of individuals,[69] the majority of whom are not suspected of any criminal activity. The Respondent's use of this tool without a careful assessment of its privacy impacts, could heighten community concerns about proportionate surveillance techniques.

72. More generally, I do not accept the Respondent's submission that as this was a limited trial, it was not required to undertake a PIA.[70] There is no evidence that the Respondent took steps before or during the Trial to systematically limit the scope or duration of the trial. Contrary to the Respondent's assertions that it used the Facial Recognition Tool specifically to ascertain the accuracy and effectiveness of the algorithm,[71] the Respondent did not limit searches to only those necessary for that purpose. Even if, as submitted by the Respondent, the images searched were only derived from underground

---

[64] Commonwealth contract is defined in s 6(1) of the Privacy Act.

[65] Privacy Act, s 95B.

[66] As noted in s 6(1) of the Privacy Act, 'sensitive information' relevantly includes (d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; and (e)biometric templates.

[67] APP Guidelines [B.141].

[68] Office of the United Nations High Commissioner for Human Rights, The Right to Privacy in the Digital Age UN Doc A/HRC/27/37 (2014), paragraph 23, <https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx>

[69] *Commissioner Initiated Investigation into Clearview AI Inc.* (Privacy) [2021] AICmr54 (14 October 2021) at [4]. The Clearview AI website now states that its database includes more than 10 billion facial images <https://www.clearview.ai/>

[70] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 6.

[71] R6 – Letter from the Respondent to the OAIC dated 12 July 2021 p 2.

marketplaces on the internet, publicly available sources, or from the individual concerned with their consent (see paragraph 41), the evidence shows that Trial participants used the Facial Recognition Tool to search for victims, suspects and persons of interest in connection with active investigations.[72]

73. For the reasons set out in paragraphs 47 to 72 above, I consider that the Respondent's use of the Facial Recognition Tool was a high privacy risk project requiring a PIA under the Code.

Threat to life, health or safety

74. Clause 12 of the Code does not expressly exempt agencies from the requirement to conduct a PIA, in circumstances where the agency believes the handling of personal information is necessary to lessen or prevent a threat to life, health or safety to individuals.[73] However, I accept that law enforcement may occasionally need to use or disclose personal information for this purpose, before it has finalised a PIA. In these circumstances, a PIA should be undertaken early enough in the development of a project that it can influence the project design or, if there are significant negative privacy impacts, reconsider proceeding with the project. [74]

75. In this case, while one search was conducted to protect a person from imminent risk of harm,[75] the Respondent did not commence a PIA at any point prior to, or during the Trial.[76] The fact that one search was conducted for this purpose, does not excuse the Respondent from its obligations under clause 12 when its members used the Facial Recognition Tool for multiple searches over months.

Finding

76. I find that the Respondent interfered with the privacy of individuals whose facial images were disclosed to the third party service provider, by failing to undertake a PIA for a high privacy risk project in breach of Clause 12 of the Code.

APP 1.2

Law

77. APP 1.2 requires an APP entity to take reasonable steps to implement practices, procedures and systems relating to the entity's functions or activities that will ensure the entity complies with the APPs and a registered APP code (if any) that binds the entity.

78. Underpinning the accountability requirements in APP 1.2, is a 'privacy by design' approach to information management. 'Privacy by design' builds privacy into projects from the design stage onwards and is a fundamental component of effective data protection. It involves identifying privacy risks and mitigating those risks. In applying this approach, entities take steps at the outset of a project that minimise risks to an

---

[72] R5 – Letter from the Respondent to the OAIC dated 1 June 2021 p 12-16.

[73] APPs 3, 6, 8 and 9 include an exception where the entity reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety (s 16A, Item 1).

[74] OAIC Guide to undertaking privacy impact assessments, available online: https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/.

[75] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 2.

[76] R5.11 – Attachment K to the letter from the Respondent to the OAIC dated 1 June 2021 p 1.

individual's privacy. PIAs are essential tools in a 'privacy by design' approach to innovation.

79. In accordance with 'privacy by design' principles, privacy should be incorporated into business planning, staff training, priorities, project objectives and design processes, in line with APP 1.[77]

80. APP 1.2 imposes a distinct and separate obligation on APP entities, as well as being a general statement of the obligation to comply with the other APPs. Its purpose is to require an entity to take proactive steps to establish and maintain internal practices, procedures and systems that ensure compliance with the APPs. The obligation is enduring. An entity that keeps a record of the steps taken to comply with APP 1.2, is more able to demonstrate that personal information is managed in an open and transparent way.[78]

81. Agencies should also take steps to ensure compliance with their policies and procedures, including by providing regular, adequate training to staff on how to adhere to the procedures. Training should cover all requirements of the policies and procedures that are relevant to the identified risks.

82. The reasonable steps that an APP entity should take will depend upon circumstances that include:

- the nature of the personal information held
- the possible adverse consequences for an individual if their personal information is not handled as required by the APPs
- the nature of the APP entity
- the practicability, including time and cost involved. However, an entity is not excused from implementing particular practices, procedures, or systems by reason only that it would be inconvenient, time-consuming or impose some cost to do so.[79]

83. The following are given as examples of practices, procedures, and systems that an APP entity should consider implementing:

- procedures for identifying and managing privacy risks at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction, or de-identification
- procedures for identifying and responding to privacy breaches, handling access and correction requests and receiving and responding to complaints and inquiries
- a commitment to conducting a PIA for new projects in which personal information will be handled, or when a change is proposed to information handling practices. Whether a PIA is appropriate will depend on a project's size, complexity and scope, and the extent to which personal information will be collected, used, or disclosed[80]

---

[77] The OAIC's *Guide to securing personal information.* Available online at https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-securing-personal-information/.

[78] APP Guidelines, [1.5].

[79] APP Guidelines, [1.6].

[80] Further information about Privacy Impact Assessments is contained in OAIC, *Guide to Undertaking Privacy Impact Assessments* (including an e-learning tool), available at: https://www.oaic.gov.au.

- regular staff training and information bulletins on how the APPs apply to the entity, and its practices, procedures and systems developed under APP 1.2.[81]

Submissions

84. The Respondent submitted that the actions taken by the ACCCE in this matter were isolated, and the circumstances are not indicative of a systemic privacy compliance issue.[82]

85. The Respondent outlined steps it had taken prior to the Trial Period, to implement practices, procedures, and systems for the procurement of technology-based investigative capabilities to ensure compliance with the APPs and the Code.[83] These included implementing a formal Governance Instrument Framework, which established practices and procedures for identifying and managing privacy risks. Relevant instruments in the framework were:

- AFP National Guideline on privacy (undated)
- AFP National Guideline on managing child abuse (15 March 2012)
- AFP National Guideline on information management (15 October 2014)
- AFP National Guidelines on information security (8 January 2018)
- Better practice guide to undertaking privacy impact assessments (29 June 2018)
- Commissioner's orders on Governance (CO1) (26 September 2018)
- Information Management Handbook (7 June 2019)
- Privacy management plan (1 July 2018 – 30 June 2019)
- Interactive privacy management plan (1 July 2019 – 30 June 2020).

86. The Respondent submitted that it had taken steps to implement these policies by making staff aware of the framework on commencement, prominently positioning the governance framework on the intranet, and requiring all of its members to undertake privacy training as part of induction and annually to encourage good privacy practice.[84]

87. The Respondent advised that it does not have a formal internal compliance framework in place, but provided general information about its internal assurance activities to mitigate the risk of non-compliance with its policies, procedures and legislation.[85]

88. The Respondent provided a copy of its privacy training module to the OAIC, which referenced the need to conduct PIAs for all high privacy risk projects. The module also instructed staff who were undertaking a project that 'may be a high privacy risk project' to contact the Respondent's privacy team for advice on how to conduct a PIA or refer to the Respondent's National Guideline on Privacy and related online resources.[86]

89. The Respondent submitted that its online training was supplemented by face-to-face training provided to the Respondent's business and operational areas as needed, and all-staff communications from the Respondent's Privacy Champion at least annually. The

---

[81] APP Guidelines, [1.7].
[82] R6 – Letter from the Respondent to the OAIC dated 12 July 2021 p 2.
[83] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 3.
[84] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 5.
[85] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 5.
[86] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 3, 5. and R5.9 – Attachment I to the letter from the Respondent to the OAIC dated 1 June 2021 p 10.

Respondent provided the OAIC with an all-staff communication from the Privacy Champion and a National Manager's forum paper that referenced the obligation to conduct a PIA.[87]

90. The Respondent acknowledged that its guidelines, policies and instruments did not specifically address officers using a free trial of an online application for investigations or activities involving personal information.[88] For this reason, the Respondent considered that use of the Facial Recognition Tool did not contravene existing governance or approval processes.

Consideration

Did the Respondent take reasonable steps in the circumstances?

91. I accept that during the Trial Period, the Respondent had a range of policies and processes in place designed to ensure compliance with the APPs and the Code, and that some steps had been taken to implement these (see paragraphs 84 – 90).

92. I acknowledge that the Respondent's policies contained useful information about the requirement to undertake a PIA for high privacy risk projects under clause 12 of the Code. This included guidance on assessing privacy impacts, an outline of the process for conducting a PIA, information about responsibility for conducting and keeping records of PIAs and threshold privacy assessments, contact details for the Privacy Officer (noting they could be contacted for assistance in determining whether a PIA was required) and a PIA template.[89]

93. I also acknowledge that some steps had been taken to implement these policies by making relevant policies available on the intranet, mandating privacy training and issuing agency-wide communications about privacy requirements.

94. While recognising the steps already taken to embed a culture that respects privacy, I consider that some of the Respondent's practices, procedures and systems that were in place during the Trial Period, require further development to ensure compliance with clause 12 of the Code.

Systems and policies

95. A critical foundation in identifying whether a PIA must be conducted under clause 12 of the Code, is ensuring that staff with experience and skills in assessing privacy risk, are aware of new or planned projects that may involve high privacy risk. This investigation has shown significant gaps in the Respondent's systems for identifying these kinds of projects, and documenting privacy risk assessments. In particular:

- There was no visibility of the Trial outside of the ACCCE operational command (including by the Respondent's designated Privacy Officer).[90]
- The Respondent has not identified any document(s) recording any contemporaneous privacy risk assessment about use of the Facial Recognition Tool.[91]

---

[87] R5 – Letter from the Respondent to the OAIC dated 1 June 2021 p 10.
[88] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 6.
[89] R5.8 – Attachment H to the letter from the Respondent to the OAIC dated 1 June 2021; R2.7 – Attachment G to the letter from the Respondent to the OAIC dated 14 August 2020.
[90] R5 – Letter from the Respondent to the OAIC dated 1 June 2021 p 6-7.
[91] R5 – Letter from the Respondent to the OAIC dated 1 June 2021 p 8.

- According to a media article dated 21 January 2020, a spokesperson for the Respondent had advised at that time that it did not use the Facial Recognition Tool (see paragraph 13).
- The Respondent refused 3 FOI requests on 13 February 2020 on the basis that no information relating to the third party service provider had been identified, notwithstanding that the Facial Recognition Tool had been used by several Trial participants (see paragraph 15).
- There were limited records of how this novel technology was used. For example, the dates of registration for 3 Trial participants are unknown;[92] the Respondent did not have logs recording details of access and/ or use of the Facial Recognition Tool; and for many uploaded images, the Respondent had no record of the particular image that had been uploaded.[93]

96. I am not satisfied that during the Trial Period, the Respondent had appropriate systems in place to identify, track and accurately record its use of new investigative technologies to handle personal information.

97. I consider that the Respondent should have instituted a more centralised approach to identifying and assessing new and emerging investigative techniques or technologies that handle personal information. This would have assisted the Respondent to identify new high privacy risk projects within its organisation and take a consistent approach to risk assessment. It would also have supported the Respondent's compliance with APP 1.2 in future, by enabling it to explain why a new or changed way of handling personal information did not have the potential to be high privacy risk (noting that it is the responsibility of each agency to be able to demonstrate whether a new or changed way of handling personal information was a high privacy risk project).[94]

98. In addition, the Respondent's policies should have specifically addressed the use of free trials and other freely available online search applications, for investigative purposes. The privacy risks of using such applications (such as those outlined in 69 to 73), were foreseeable given that search tools and applications are easily accessible on the internet, and noting the ACCCE's commitment to exploring 'new and innovative solutions' to meet challenges posed by offenders evolving their operating methods to avoid detection.[95] The policies should have explained how attendant privacy risks should be assessed to enable compliance with Clause 12 of the Code, and the controls and approval processes in place to support such privacy risk assessments.

Privacy training

99. Under the Respondent's written policies that applied during the Trial Period, functional areas were responsible for ensuring that PIAs were undertaken for all high privacy risk projects. The policies clearly stated that personnel could contact the Privacy Officer for assistance in determining whether a PIA is required, and included their contact details.[96]

---

[92] R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 2.

[93] R5 – Letter from the Respondent to the OAIC dated 1 June 2021 p 12-16.

[94] OAIC guide, 'When do agencies need to conduct a privacy impact assessment?', available online at: https://www.oaic.gov.au/privacy/guidance-and-advice/when-do-agencies-need-to-conduct-a-privacy-impact-assessment/ .

[95] R5 – Letter from the Respondent to the OAIC dated 1 June 2021 p 2; R2 – Letter from the Respondent to the OAIC dated 14 August 2020 p 1.

[96] R2.7 – Attachment G to the letter from the Respondent to the OAIC dated 14 August 2020 p 2-3.

100. Notwithstanding this, none of the 10 members of the ACCCE who registered for trial accounts conducted a threshold assessment or a PIA (see paragraph 64). Given this omission, I have considered the steps the Respondent took to implement its written policies about privacy risk assessments, including through staff training and other communications about requirements under the Code.

101. While I recognise that the Respondent's written policies contained some information about requirements to undertake a PIA under clause 12 of the Code, the Respondent's online training module:

- did not include sufficient information to enable staff to identify whether a planned project may involve high privacy risk, such as factors indicating that a project may be high privacy risk, information about the process of conducting threshold assessments and PIAs, or relevant operational examples
- did not set out clear pathways and triggers for functional areas to consult with appropriate legal and technical experts, before engaging in new or changed personal information handling practices
- did not clearly identify who was responsible for undertaking threshold assessments and PIAs, and for keeping relevant records[97]
- did not include information about the potential privacy risks of novel high privacy-impact technologies, or the risks to individuals of uploading personal information held by the agency to a third party service provider in the absence of a Commonwealth contract[98] (as discussed in paragraph 71).

102. The Respondent's submissions also indicate that at least 3 of the Trial participants had not received privacy training in the 12 months leading up to the Trial Period.[99]

103. Based on the Respondent's submissions and documentation provided, I cannot be satisfied that adequate training was provided to functional areas about how to undertake such an assessment, when to do so, and when to involve the Privacy Officer or other privacy experts.

PIA

104. In addition to being a discrete obligation under the Code, an example of the practices, procedures and systems that an APP entity should consider implementing to comply with APP 1.2, is a commitment to conducting a PIA for new projects in which personal information will be handled or when a change is proposed to information handling practices.[100] A PIA can assist in identifying the practices, procedures or systems that will be reasonable to ensure that new projects are compliant with the APPs. [101]

105. I have concluded at paragraph 76 above that the Respondent breached clause 12 of the Code by failing to undertake a PIA for a high privacy risk project.

---

[97] R2.7 – Attachment G to the letter from the Respondent to the OAIC dated 14 August 2020 p 2-3.

[98] Privacy Act, s 95B.

[99] R5 – Letter from the Respondent to the OAIC dated 1 June 2021 p 10.

[100] APP Guidelines [1.7].

[101] OAIC Guide to undertaking privacy impact assessments p 4.

What additional steps were reasonable in the circumstances?

106. The requirement in APP 1.2 is to take 'reasonable steps' to implement practices, procedures and systems to ensure compliance with the APPs and the Code.

107. I have considered the seriousness of decisions that may flow from use of the Facial Recognition Tool (see paragraph 71), the fact that the personal information of victims (including children and other vulnerable individuals) was searched, and the likelihood that the Trial involved the handling of sensitive biometric information for identification purposes. I would expect the Respondent to take steps commensurate with this level of risk under APP 1.2, to ensure any privacy risks in using technologies like the Facial Recognition Tool are carefully identified, considered and mitigated against. In some circumstances, the privacy impacts of a high privacy risk project, may be so significant that the project should not proceed.[102]

108. I consider that having regard to these heightened risks and the deficiencies outlined above, the Respondent should have at least taken the following additional steps before the Trial Period:

- The Respondent should have implemented a centralised system to identify, track and accurately record its use of new investigative technologies to handle personal information.
- The Respondent's written policies should have specifically identified the privacy risks of using new technologies to handle personal information as part of its investigative functions (including on a trial basis and when a service is available free of charge) and included controls and approval processes to address these risks.
- The Respondent should have ensured that staff who were responsible for assessing privacy risk received appropriate privacy training on a regular basis, which covered at least the matters outlined at paragraph 101.
- The Respondent should have conducted a PIA in relation to the Trial.

109. I have taken into account the relevant circumstances, including the Respondent's role as a federal law enforcement agency, its use of the Facial Recognition Tool to search for victims, suspects and persons of interest for investigative purposes, the sensitive nature of the biometric information collected and used by the Facial Recognition Tool, and the time and costs of implementing appropriate policies, procedures, and training. Having regard to these circumstances, I am satisfied that the Respondent did not take steps as were reasonable in the circumstances to implement practices, procedures and systems relating to its functions or activities that would ensure that it complied with clause 12 of the Code, as required under APP 1.2.

Finding

110. I find that the Respondent interfered with the privacy of individuals whose images it uploaded to the Facial Recognition Tool, by failing to take reasonable steps under APP 1.2 to implement practices, procedures and systems relating to its functions or activities that would ensure that it complied with Clause 12 of the Code.

[102] OAIC Guide to undertaking privacy impact assessments p 29.

Remedies

111. 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*[103] and the *OAIC's Guide to Privacy Regulatory Action*.[104]

112. I am satisfied 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.[105]

b. The conduct involved personal information that the Respondent should reasonably have assumed was sensitive biometric information.[106]

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.[107]

d. There is specific and general educational, deterrent or precedential value in making a determination in this matter. [108]

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.[109]

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

113. 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.

114. I recognise that the Respondent is proactively working to build the maturity of its privacy governance framework and embed a culture of privacy compliance across the agency. I particularly acknowledge the Respondent's commitment since the Trial Period, to reviewing and strengthening parts of its privacy governance framework. This includes reviewing and updating its privacy management plan (1 July 2021 to 1 July 2022), which identifies specific, measurable privacy goals and targets and sets out how the agency will meet its compliance obligations under APP 1.2.[110]

115. In addition, the Respondent submitted during the investigation that it:

---

[103] Privacy Regulatory Action Policy [38].
[104] Guide to Privacy Regulatory Action [4.9].
[105] Privacy regulatory action policy at [38].
[106] Privacy regulatory action policy at [38].
[107] Privacy regulatory action policy at [38].
[108] Privacy regulatory action policy at [38].
[109] Guide to Privacy Regulatory Action at [4.9].
[110] R5.7 – Attachment G to the letter from the Respondent to the OAIC dated 1 June 2021 p 2-3.

- had appointed a dedicated position within the ACCCE, who would be responsible for undertaking software evaluations of similar kinds of applications in future[111]
- was undertaking a review of existing internal governance processes and documents to specifically address the use of free trials in the online environment[112]
- had commissioned a broader review of the Respondent's privacy governance with the assistance of an external legal services provider[113]
- was reviewing its training module to ensure operational relevance to all staff by including sufficient context and explanation.[114]

116. While these appear to be constructive developments, on the evidence before me, I cannot be satisfied that steps the Respondent has taken to date will ensure that the breaches of clause 12 of the Code and APP 1.2 are not repeated or continued.

117. The Respondent has not provided the OAIC with specific information about how any steps it has taken or is taking, will prevent similar breaches occurring again in the future, by addressing the deficiencies in paragraphs 95 to 105 above. For example, during this investigation, the OAIC was not provided with details of how the Respondent's policies, decision making processes, and approval processes in relation to the use of new technologies have changed since January 2020.[115] In addition, while the OAIC's preliminary view contained findings about additional steps that should have been taken to train staff about privacy impact assessments, the Respondent did not provide any updated information about changes to its training program.[116]

118. Without a more coordinated approach to identifying high privacy risk projects and improvements to staff privacy training, there is a risk of similar contraventions of the Privacy Act occurring in the future. This is particularly the case given the increasing accessibility and capabilities of facial recognition service providers and other new and emerging high privacy impact technologies that could support investigations.

119. For these reasons, I consider that it is reasonable, proportionate and appropriate to make the declarations in paragraph 2(c) of this determination, under s 52(1A)(b) of the Privacy Act, requiring an independent review of the changes made to the Respondent's relevant practices, procedures, systems (including training) since the Trial Period. The declarations will provide the OAIC with ongoing oversight of updates to the Respondent's privacy governance framework. The independent review may also provide additional assurance to Australians that the deficiencies identified in this determination have been addressed. These specified steps will help the Respondent to prevent similar contraventions, and ensure any privacy risks in using high privacy impact technologies are carefully identified, considered and mitigated against.

[111] R6 – Letter from the Respondent to the OAIC dated 12 July 2021 p 2.
[112] R6 – Letter from the Respondent to the OAIC dated 12 July 2021 p 2.
[113] R6 – Letter from the Respondent to the OAIC dated 12 July 2021 p 2.
[114] R5 – letter from the Respondent to the OAIC dated 1 June 2021 p 10.
[115] R5 - Letter from the Respondent to the OAIC dated 1 June 2021 p 7.
[116] R6 – Letter from the Respondent to the OAIC dated 12 July 2021.

120. Taking into account the OAIC's Regulatory Action Policy[117] and Guide to Privacy Regulatory Action[118] I make this determination and declarations as a proportionate response to the interferences with privacy.

Angelene Falk
Australian Information Commissioner and Privacy Commissioner

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

[117] Privacy Regulatory Action Policy is available online at: https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/.

[118] OAIC Guide to Privacy Regulatory Action (updated June 2020), available online at Guide to privacy regulatory action — OAIC.

Attachment A

Relevant Law – *Privacy Act 1988* (Cth)

Determination powers

52 Determination of the Commissioner

(1) …….

(1A) After investigating an act or practice of a person or entity under subsection 40(2), the Commissioner may make a determination that includes one or more of the following:

(a) a declaration that:

(i) the act or practice is an interference with the privacy of one or more individuals; and

(ii) the person or entity must not repeat or continue the act or practice;

(b) a declaration that the person or entity must take specified steps within a specified period to ensure that the act or practice is not repeated or continued;

(c) a declaration that the person or entity must perform any reasonable act or course of conduct to redress any loss or damage suffered by one or more of those individuals;

(d) a declaration that one or more of those individuals are entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice;

(e) 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.
…
Agency means:

(a) a Minister; or

(b) a Department; or

(c) a body (whether incorporated or not), or a tribunal, established or appointed for a public purpose by or under a Commonwealth enactment, not being:

(i) an incorporated company, society or association; or

(ii) an organisation that is registered under the *Fair Work (Registered Organisations) Act 2009* or a branch of such an organisation; or

(d) a body established or appointed by the Governor-General, or by a Minister, otherwise than by or under a Commonwealth enactment; or

(e) a person holding or performing the duties of an office established by or under, or an appointment made under, a Commonwealth enactment, other than a person who, by virtue of holding that office, is the Secretary of a Department; or

(f) a person holding or performing the duties of an appointment, being an appointment made by the Governor-General, or by a Minister, otherwise than under a Commonwealth enactment; or

(g) a federal court; or

(h) the Australian Federal Police; or

(ha) a Norfolk Island agency; or

(k) an eligible hearing service provider; or

(l) the service operator under the *Healthcare Identifiers Act 2010*.

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.

1 Australian Privacy Principle 1—open and transparent management of personal information

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:
(a) will ensure that the entity complies with the Australian Privacy Principles and a registered APP code (if any) that binds the entity; and
(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles or such a code

Clause 12 of the Code

1. An agency must conduct a PIA for all high privacy risk projects.
2. For the purposes of this section, a project may be a high privacy risk project if the agency reasonably considers that the project involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.

Note: 'Privacy impact assessment' is defined in section 33D of the Act. This section of the Act also requires an agency to conduct a PIA if directed to do so by the Commissioner.