Commissioner initiated investigation into Clearview AI, Inc. (Privacy) [2021] AICmr 54 (14 October 2021)

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

Respondent	Clearview AI, Inc.
Decision date	14 October 2021
Case reference number	CII20/00006
Catchwords	Privacy — *Privacy Act 1988* (Cth) — Australian Privacy Principles — APP 3.3 – APP 3.5 – APP 5 – APP 10.2 – APP 1.2 – extraterritorial jurisdiction – whether sensitive information collected without consent – whether personal information collected by fair means – whether reasonable steps taken to notify individuals of collection of personal information – whether reasonable steps taken to ensure personal information disclosed is accurate, having regard to purpose of disclosure – whether reasonable steps taken to implement practices, procedures and systems to ensure compliance with the APPs – breaches substantiated – cease collecting and destroy Australians' facial images and biometric templates

Determination

1. I find that the respondent, Clearview AI, Inc.:

   a. failed to comply with the requirement in Australian Privacy Principle (**APP**) 1.2 in Schedule 1 of the *Privacy Act 1988* (Cth) (**Privacy Act**), to take reasonable steps to implement practices, procedures and systems relating to the entity's functions or activities, that will ensure compliance with the APPs.

   b. interfered with the privacy of Australian individuals, by failing to:

      i. collect sensitive information about an individual only where the individual consented to the collection (and the information was reasonably necessary for one

or more of the entity's functions or activities) (APP 3.3) in circumstances where no other exceptions applied to permit the collection (APP 3.4)

ii. collect personal information only by lawful and fair means (APP 3.5)

iii. take such steps (if any) as were reasonable in the circumstances to notify individuals of the collection of personal information (APP 5)

iv. take such steps (if any) as were reasonable in the circumstances to ensure that the personal information it used or disclosed was, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant (APP 10.2).

Declarations

2. I declare, under s 52(1A) of the Privacy Act, that the respondent:

   a. must not repeat or continue the acts and practices that I have found are an interference with the privacy of one or more individuals

   b. must cease to collect Scraped Images, Probe Images, Scraped Image Vectors, Probe Image Vectors and Opt-out Vectors (see paragraphs 5 and 11) from individuals in Australia in breach of APPs 3.3, 3.5 and 5

   c. within 90 days of the date of this determination, must destroy all Scraped Images, Probe Images, Scraped Image Vectors, Probe Image Vectors and Opt-out Vectors it has collected from individuals in Australia, and

   d. within 90 days of the date of this determination, must provide written confirmation to my Office that the respondent:

      i. is no longer collecting images and vectors as required in paragraph 2(b)

      ii. has destroyed images and vectors as required in paragraph 2(c).

Findings and Reasons

Background

3. The respondent provides a facial recognition search tool (the **Facial Recognition Tool**) for registered users. This is available through a mobile and web application.

4. The Facial Recognition Tool allows users to upload a digital image of an individual's face and run a search against the respondent's database of more than 3 billion images.[1] The Tool displays likely matches and associated source information to the user, to enable identification of the individual.

Facial Recognition Tool

5. The respondent's Facial Recognition Tool functions in five steps:

[1] Letter from the respondent to the OAIC dated 25 February 2020 (**respondent's response dated 25 February 2020**) p 2.

- **Automated image scraper** – The tool functions as a web crawler, collecting images of individuals' faces from publicly available sources across the internet (including social media) (the **Scraped Images**). The web crawler also collects the source webpage URL,[2] and any associated metadata that was not stripped by the source website[3] (including the webpage title).[4] The images and associated information are stored in a database on the respondent's servers.
- **Creation of vectors** – The tool generates a mathematical representation of the Scraped Image (**Scraped Image Vector**) using a machine-learning algorithm[5] and stores this in the respondent's database.
- **Image uploaded** – A registered user uploads an individual's image through the app or website (the **Probe Image**). The tool analyses the Probe Image and generates a mathematical representation of the Probe Image (the **Probe Image Vector**).
- **Matching process** – The tool compares the Probe Image Vector against all Scraped Image Vectors. These, in turn, are linked back to any Scraped Images that appear to show the same individual.
- **Matched images** – If the tool identifies sufficiently similar Scraped Images, **Matched Images** are displayed alongside the Probe Image on the user's screen as 'search results'.[6] Each Matched Image is displayed in the form of a thumbnail image and a link to the source URL. The user must then click the associated URL to be re-directed to the web page where the image was originally collected, to obtain additional information from that web page.

Respondent's customers

6. The respondent submitted that it currently offers its service to government customers for law enforcement and national security purposes only.[7] Its website states that its product helps law enforcement agencies to 'accurately and rapidly identify suspects, persons of interest, and victims to help solve and prevent crimes'.[8]
7. The Facial Recognition Tool has a broader capability. The respondent's US and international patent applications describe ways to apply its facial recognition software to the private sector, including:
    - to learn more about a person the user has just met, such as through business, dating, or other relationship
    - to verify personal identification for the purpose of granting or denying access for a person, a facility, a venue, or a device
    - to accurately dispense social benefits and reduce fraud (by a public agency).[9]

---

[2] Letter from the respondent to the OAIC dated 19 August 2020 (**respondent's response dated 19 August 2020**) p 2.
[3] Respondent's response dated 19 August 2020 p 1.
[4] Respondent's response dated 25 February 2020 p 3.
[5] Respondent's response dated 4 August 2020 p 2.
[6] Letter from the respondent to the ICO and OAIC dated 26 September 2020 (**respondent's response dated 26 September 2020**) p 4.
[7] Letter from the respondent to the ICO dated 3 June 2021 (**respondent's response dated 3 June 2021**) p 1.
[8] Respondent's website, available at: https://clearview.ai/ (accessed on 30 August 2021).
[9] US Patent and Trademark Office, *United States Patent Application*, 20210042527, Thon-That, Cam-Hoan, filing date 7 August 2020, publication date 11 February 2021; World Intellectual

8. From October 2019 to March 2020, the respondent offered free trials to the Australian Federal Police (**AFP**), Victoria Police, Queensland Police Service and South Australia Police (**Australian police agencies**). Members from each of these Police services used the Facial Recognition Tool on a free trial basis.[10] Police members uploaded Probe Images to test the functionality of the Facial Recognition Tool, and in some cases, to try to identify suspects and victims in active investigations.[11] The Probe Images included images of children.[12]

9. The respondent submitted that by the end of March 2020, it had terminated all of its trial users in Australia and had instituted a policy of refusing all requests for accounts from Australia.[13] There is no evidence of new Australian trial users or account holders since March 2020. [Redacted][14]

10. The respondent has not taken any steps (other than the opt-out mechanism referred to below which, during the course of the investigation ceased to be available to Australians), to stop collecting Scraped Images of Australians, generating image vectors from those images, and disclosing any Australians in Matched Images to its registered users. The respondent's website and form for requesting access to the Facial Recognition Tool remain accessible to Australian IP addresses.

Opt-out requests

11. On 29 January 2020, the respondent established the following process for Australian residents to opt out of the respondent's search results:

    - **Opt-out request** – individuals submit a request to opt out by:
        - clicking on a hyperlink on the respondent's homepage, 'Privacy Request Forms'
        - clicking on a hyperlink, 'Data Deletion Request Form' (under the heading, 'For Residents of the EU, UK, Switzerland, and Australia'). This page was titled 'EU/UK/Switzerland/Australia Opt-Out' and stated that it 'is designed to enable members of the public to request to opt-out of Clearview search results'[15]
        - click 'Start' and complete the Request Form.

      The request form required individuals to submit a valid email address and a facial image.

Property Organisation, International Patent Application, WO202103017, filing date 7 August 2020, publication date 18 February 2021, available at: https://patentscope.wipo.int/search/en/detail.jsf?docId=WO2021030178&tab=PCTBIBLIO.

[10] Respondent's response dated 25 February 2020 p 2; Respondent's response dated 19 August 2020, p 2.

[11] Letter from the AFP to the OAIC dated 21 April 2020 (**AFP response dated 21 April 2020**) p 3-6; AFP response dated 21 April 2020, Annexure D, p 13-20; Letter from the Queensland Police Service to the OAIC dated 7 August 2020 (**Queensland Police response dated 7 August 2020**) p 1-5; Email from Victoria Police to the OAIC, 29 June 2020, Attachment titled "1. Combined".

[12] Victoria Police Issue Cover Sheet on the use of Clearview, undated p.1.

[13] Letter from the respondent to the ICO and OAIC dated 2 November 2020 (**respondent's response dated 2 November 2020**) p 2.

[14] Respondent's response dated 2 November 2020 p 2.

[15] https://clearview.ai/privacy/requests (accessed on 1 February 2021).

- **Creation of vector** – the respondent generated a mathematical representation of the submitted image (the **Opt-out Vector**) and permanently retained the Opt-out Vector.[16]
- **Matching process** – the respondent searched for the Opt-out Vector against the Scraped Image Vectors, to identify any sufficiently similar Scraped Images. The respondent would block images of that individual from appearing in future search results, and would prevent further collection of Scraped Images of that individual.[17]

12. However, during my investigation, the respondent removed the online form for Australians to opt-out described above. For Australian residents, the respondent now only processes requests for opt-out that it receives via email.[18]

Investigation by the OAIC

13. On 21 January 2020, the OAIC sent preliminary inquiries to the respondent under s 42(2) of the Privacy Act. The respondent provided a written response on 25 February 2020.

14. On 4 March 2020, I notified the respondent that I had commenced an investigation under subsection 40(2) of the Privacy Act and would consider whether the respondent had met the requirements of APPs 3.2, 3.3, 3.5, 3.6, 5, 6, 8, 10, 11.1, 11.2 and 1.2.

15. On 7 July 2020, the OAIC and the UK Information Commissioner's Office (the **ICO**) wrote to the respondent to formally inform the respondent of the intention to jointly investigate the respondent's data processing practices.

16. The joint letter set out that:

- In support of the international co-operation mechanisms, in recognition of the international nature of the processing understood to be taking place, and as contemplated in the Memorandum of Understanding (**MOU**) between the ICO and the OAIC, the OAIC is conducting this investigation, commenced on 4 March 2020, jointly with the ICO.[19]
- In conducting a joint investigation, the ICO and the OAIC intend to assist the respondent in managing multiple requests from data protection authorities which pertain to the same or substantially similar questions or subject matter.
- The ICO and the OAIC intend to share and collaborate in relation to the respondent's responses to investigative inquiries in this matter, in accordance with the MOU and the Global Cross Border Cooperation Enforcement Arrangement.[20]
- The respondent's responses provided to the ICO will be considered in the context of its compliance or otherwise with the EU General Data Protection Regulation and the *Data Protection Act 2018*. Those provided to the OAIC will be considered in the context of the respondent's compliance with the Privacy Act.

---

[16] Respondent's response dated 26 September 2020 p 9-10.
[17] Ibid.
[18] Respondent's response dated 3 June 2021, p 2.
[19] In March 2020, the ICO and OAIC entered into a Memorandum of Understanding which provides for the sharing of information and documents between the regulators including for the purposes of joint investigations, available at: https://www.oaic.gov.au/about-us/our-corporate-information/memorandums-of-understanding/mous/mou-with-ico/).
[20] For more information about the Global Privacy Assembly's Global Cross Border Cooperation Enforcement Arrangement, see: https://globalprivacyassembly.org/participation-in-the-assembly/global-cross-border-enforcement-cooperation-arrangement-list-of-participants/

17. Following the conclusion of the joint evidence-gathering phase, the OAIC sent its preliminary view to the respondent on 21 May 2021, setting out preliminary findings, reasons and draft declarations. The respondent provided a response to the preliminary view on 10 June 2021, which I have considered in making this determination.

Law

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

19. 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**).

20. '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
- the information or opinion is recorded in a material form or not.'[21]

21. Section 15 prohibits an APP entity from doing an act, or engaging in a practice, that breaches an APP.

22. The APPs relevant to the investigation are:

- APP 1.2
- APP 3.3
- APP 3.5
- APP 5
- APP 10.2

23. In my letter of 4 March 2020, I also notified the respondent that the OAIC was investigating the respondent's compliance with APPs 3.2, 3.6, 6, 8 and 11. I have not made findings in relation to these APPs.

24. The relevant APPs are set out in full at **Attachment A.**

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

- a declaration that the act or practice is an interference with the privacy of an individual and must not be repeated or continued
- 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
- 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
- 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

[21] s 6(1) of the Privacy Act.

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

26. Section 5B establishes the extra-territorial operation of the Privacy Act.

Material considered

27. In making this determination, I have considered information and submissions provided by the respondent, information provided by third parties in response to requests for information issued under the Privacy Act, and information obtained from online sources by OAIC officers, up to the date of issuing the preliminary view on 21 May 2021.

28. I have also considered the Australian Privacy Principles Guidelines, February 2014 (**APP Guidelines**)[22], the OAIC's Privacy Regulatory Action Policy[23] and the OAIC's Guide to Privacy Regulatory Action (July 2020).[24]

29. While not legally binding, the APP Guidelines outline the mandatory requirements of the APPs, how I will interpret the APPs, and matters I may take into account when exercising my functions and powers under the Privacy Act.

Jurisdiction – Australian link

Law

30. The Privacy Act applies to an act done, or a practice engaged in, by an organisation in Australia.

31. By operation of s 5B(1A), the Privacy Act also applies to an act done, or practice engaged in, outside Australia by an organisation that has an 'Australian link'.

32. As the respondent is incorporated in the State of Delaware in the United States,[25] for the respondent to have an 'Australian link', both of the following conditions in s 5B(3) of the Privacy Act must apply:

- The organisation carries on business in Australia.
- The personal information was collected or held by the organisation in Australia either before or at the time of the act or practice.

Paragraph 5B(3)(b): the organisation carries on business in Australia

33. The phrase 'carries on business in Australia' in s 5B(3)(b) is not defined in the Privacy Act. The Explanatory Memorandum explains that 'entities … who have an online presence (but no physical presence in Australia) and collect personal information from people who are physically in Australia, carry on a 'business in Australia or an external Territory''.[26]

---

[22] As at July 2019. Available online at: https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/

[23] Available online at: https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/

[24] Available online at: https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/

[25] Respondent's response dated 25 February 2020 p 1.

[26] Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, Schedule 4, Item 6.

34. The phrase also arises in other areas of law, including corporations and consumer law. Guidance may be drawn from judicial consideration of the phrase in those contexts.[27]

35. The relevant principles with respect to the phrase 'carries on business in Australia', within the meaning of s 5B(3)(b) of the Privacy Act, were described by Thawley J in *Australian Information Commissioner v Facebook Inc (No 2)* (***Facebook No 2***).[28] In particular:

- In *Campbell v Gebo Investments (Labuan) Ltd* (**Gebo Investments**), the Court considered whether the mere solicitation of business transactions via the internet was insufficient to constitute carrying on business in Australia in the context of winding up provisions in the *Corporations Act 2001 (Cth)*. Barrett J held that the receipt of a communication in Australia, where all uploading activity occurred outside Australia, was not sufficient to constitute carrying on business in Australia. Barrett J considered that:
  - Case law makes it clear that the territorial concept of carrying on business involves acts within the relevant territory that amount to or are ancillary to transactions that make up or support the business.[29]
  - There is a need for some physical activity in Australia through human instrumentalities, being activity that itself forms part of the course of conducting business.[30]
- In *Valve Corporation v Australian Competition and Consumer Commission*,[31] the Full Federal Court (Dowsett, McKerracher and Moshinsky JJ) considered the phrase 'carrying on business within Australia' within the meaning of s 5(1)(g) of the *Competition and Consumer Act 2010*. The Court broadly agreed with the observations of Barrett J in *Gebo Investments* outlined above. However, they did not accept that there is an 'inflexible rule or condition' that carrying on business in Australia requires 'some physical activity in Australia through human instrumentalities.' Rather, the Court emphasised that 'the territorial concept of carrying on business involves acts within the relevant territory that amount to, or are ancillary to, transactions that make up or support the business'.[32]
- In *Tiger Yacht Management Ltd v Morris,*[33] the Full Federal Court (McKerracher, Derrington and Colvin JJ) considered the expression 'carrying on business in Australia' under the *Corporations Act 2001 (Cth)*. The Court considered that the phrase may have different meanings in different contexts, though when it is used to ensure a jurisdictional nexus, its meaning will be informed by the requirement to ensure there is a sufficient connection with the country asserting jurisdiction. It requires resort to the ordinary meaning of the phrase and invites a factual inquiry. The Court further noted that:
  - In order to be carrying on business, the activities must form a commercial enterprise.[34]

---

[27] APP guidelines [B.13].
[28] [2020] FCA 1307 (***Facebook No 2***) at [40]-[46].
[29] (2005) 190 FLR 209 (***Gebo Investments***) at [30]-[31].
[30] *Gebo Investments* at [33].
[31] (2017) 258 FCR 190 (***Valve Corporation***).
[32] *Valve Corporation* at [149].
[33] *Tiger Yacht Management Ltd v Morris* [2019] FCFCA 8 at [50] (**Tiger Yacht**).
[34] *Tiger Yacht* at [51]

- The words 'carrying on' imply the repetition of acts and activities which suggest a permanent character rather than participating in a single transaction or a number of isolated transactions.[35]
- A company may be carrying on business in Australia even though it does not have an identifiable place of business within Australia.[36]

36. Thawley J stated that 'the present context is the application of Australian privacy laws to foreign entities ... the present statutory context includes the object of protecting the privacy of individuals and the responsible handling of personal information collected from individuals in Australia.'[37] Section 2A of the Privacy Act identifies the following as express statutory objects:
    - to promote the protection of the privacy of individuals (s 2A(a))
    - to recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities (s 2A(b))
    - to promote responsible and transparent handling of personal information by entities (s 2A(d))
    - to facilitate the free flow of information across national borders while ensuring that the privacy of individuals is respected (s 2A(f))
    - to provide a means for individuals to complain about an alleged interference with their privacy (s 2A(g))
    - to implement Australia's international obligation in relation to privacy (s 2A(h)).

Paragraph 5B(3)(c): the personal information was collected or held in Australia

37. 'Collects' is defined in s 6(1) of the Privacy Act as follows:

> an entity ***collects*** personal information only if the entity collects the personal information for inclusion in a record or generally available publication.

38. Relevantly, s 6(1) defines 'record' to include an electronic or other device.

39. The concept of 'collection' applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means, including from, relevantly:
    - individuals
    - other entities
    - biometric technology, such as voice or facial recognition.[38]

40. Subsection 5B(3) of the Privacy Act includes a territorial limitation, namely that the collection must occur 'in Australia'. As noted above, the collection of personal information 'in Australia' under s 5B(3)(c) includes the collection of personal information

---

[35] *Tiger Yacht* at [52]
[36] *Tiger Yacht* at [53]
[37] *Facebook No 2* at [42].
[38] OAIC APP guidelines, Chapter B, available online at https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/#collects (6 September 2021)

from an individual who is physically within the borders of Australia or an external territory, by an overseas entity.[39]

41. '[T]he personal information' referred to in s 5B(3)(c) concerns the personal information that is the subject of the determination.[40]

42. 'Holds' is defined in s 6(1) of the Privacy Act as follows:

> an entity ***holds*** personal information if the entity has possession or control of a record that contains the personal information.

Consideration

Does the respondent carry on business in Australia?

43. The respondent has repeatedly asserted that it is not subject to the Privacy Act.[41]

44. According to the respondent:

- The respondent was founded in, is based in, and conducts its business in the United States of America. None of the respondent's business is conducted within Australia.
- None of the respondent's business relates to Australian individuals in any way that can be determined.
- No person operating in Australia holds an authority to use any aspect of the respondent's product.
- No information or images are stored inside Australia. The servers that house the images the subject of the investigation are in the United States of America.
- The respondent takes no steps to confirm the presence or absence of location data, Australian or otherwise.
- To the extent that an image in the respondent's database originated either from Australia or within Australia, that image was published without requiring a password or other security on the open web, and as a consequence, published within the United States of America where the respondent conducts its business.[42]
- The respondent collects images without regard to geography or source.[43]
- The respondent conducts its business with no interaction or relationship with Australian individuals.[44]
- The act of downloading an image in the United States of America cannot be considered as carrying on business in Australia.[45]

---

[39] Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth), p 218.
[40] *Facebook No 2* at [164] and [172].
[41] Respondent's response dated 19 August 2020 p 4; Respondent's response dated 26 September 2020 p 12; Respondent's response dated 2 November 2020 p 1-2.
[42] Respondent's response dated 19 August 2020 p 4.
[43] Respondent's response dated 19 August 2020 p 2.
[44] Letter from the respondent to the ICO and OAIC dated 10 June 2021 (**Respondent's response dated 10 June 2021**) p 6.
[45] Respondent's response dated 10 June 2021 p 6. The respondent referenced Gebo Investments [30] – [31] (see paragraph 35(a) of the Determination).

45. The respondent admitted that it provided trials and demonstrations of its products to several Australian police agencies inside Australia, and did so at the request of personnel in those agencies.[46] However, it asserted that this has not resulted in a continuing business relationship with any person within Australia, and the respondent has not undertaken any marketing activities or business activities inside Australia since that time.[47]

46. I consider that the circumstances of this matter clearly demonstrate that the respondent carries on business in Australia, not only while trial services were provided to certain Australian police services, but also throughout the entire period the respondent has been indiscriminately scraping facial images from the internet for its Facial Recognition Tool.

47. In the period October 2019 to March 2020 (the **Trial Period**), the respondent provided trials of the Facial Recognition Tool to the Australian police agencies, whose members used the service (the agencies used the service for different periods of time within the Trial Period).[48]

48. The fact that none of the Australian police agencies became paying customers is immaterial. The respondent's activities were commercial in nature, and the evidence shows that the trials existed for the express purpose of enticing the purchase of accounts.

49. In the Trial Period, the respondent undertook multiple activities to support its provision of the Facial Recognition Tool to the Australian police agencies, including actively marketing its service for commercial purposes. For example:

- In the Trial Period, the respondent repeatedly encouraged Australian users to use the service and undertake searches, by sending emails which included:

  > 1. **Search a lot.** Your Clearview account has **unlimited** searches. Don't stop at one search. See if you can reach 100 searches. It's a numbers game. Our database is always expanding and you never know when a photo will turn up a lead. Take a selfie with Clearview or search a celebrity to see how powerful the technology can be.[49]

- The respondent emailed some Australian police agency users upon sign up to the trial, encouraging them to sign up to a paid account, stating:

  > 3. **Get Clearview for the long haul.** If you like Clearview at the end of your trial period and it's helping you solve cases, put us in touch with the appropriate person at your organization who can proceed with procurement.[50]

- The respondent emailed some Australian police agencies encouraging them to refer other law enforcement officers to try out the Facial Recognition Tool, stating:

---

[46] Respondent's response dated 19 August 2020 p 3.
[47] Respondent's response dated 19 August 2020 p 3.
[48] AFP response dated 21 April 2020, Annexures A-D; AFP response dated 22 May 2020, Attachment A; Queensland Police response dated 7 August 2020, pp 3, 39; Letter from South Australia Police to the OAIC dated 14 July 2020 (**South Australia Police response dated 14 July 2020**), p 2; Email from Victoria Police to the OAIC, 29 June 2020, Attachment titled "1. Combined".
[49] AFP response dated 21 April 2020, Annexure C, p 1; AFP response dated 22 May 2020, Attachment A, p 3; Queensland Police response dated 7 August 2020, p 56, p 66, p 79; Email from Victoria Police to the OAIC, 29 June 2020, Attachment titled "1. Combined", p 14. (Emphasis in original)
[50] Ibid.

> Do you know any law enforcement officers who should try out Clearview? Just click or tap "Invite User" on the left-hand side of the screen when you're logged in to Clearview on desktop or mobile to refer them.
>
> We'll get them set up with a free Clearview demo account immediately. Feel free to refer **as many officers and investigators** as you want. No limits. The more people searching, the more successes.
>
> You can also send them the link to our website at www.clearview.ai and tell them to click the "Request Access" button, or send us their names and e-mail addresses by replying to this email or by sending an email to help@clearview.ai and we'll set them up. [51]

and

> Here are three important tips for using Clearview:
>
> …
>
> 2. **Refer your colleagues.** The more people that search, the more successes. We want to make this advanced technology available to as many investigators as possible. If you think your colleagues might want to try Clearview out for themselves, just send their names and e-mail addresses to help@clearview.ai and we'll sign them all up too.
>
> … [52]

- The respondent submitted that '[o]bviously, the purpose of a free trial is to sell the product'.[53]
- A Queensland Police internal email states the price of purchasing a licence to use the respondent's Facial Recognition Tool and states the following about the respondent: 'They are providing free demos for trialling and stated that "when you start solving cases with it is when we will start to ask you to pay"'.[54]
- The email also states that 'one of the creators of the Clearview ID tool, advised that the respondent is only selling licenses to 5 eyes countries (Australia, Canada, New Zealand, UK and US)'.[55]
- The respondent's brochure, provided to an Australian police agency user, included a page headed 'RAPID INTERNATIONAL EXPANSION'. The page included a map of the world with certain countries highlighted and labelled, including Australia.[56]
- The respondent sent advertising emails to users of Crimedex in Australia.[57]

50. In the Trial Period, the respondent also collected Probe Images in Australia from Australian police agency users as part of the trials and collected Scraped Images from the internet for inclusion in its database (see paragraphs 58-61 below).[58]

---

[51] Queensland Police response dated 7 August 2020 p 41, 83.
[52] Queensland Police response dated 7 August 2020 p 56.
[53] Respondent's response dated 26 September 2020 p 11.
[54] Queensland Police response dated 7 August 2020 p 12.
[55] Ibid.
[56] AFP response dated 21 April 2020, Annexure C, p 8.
[57] Respondent's response dated 26 September 2020 p 10.

51. For these reasons, I am satisfied that during the Trial Period, the respondent carried on business in Australia within the meaning of s 5B(3)(b).

52. In reaching this conclusion, I have considered all relevant circumstances, particularly the nature of the enterprise conducted by the respondent, and the objects of the Privacy Act, which include promoting the protection of the privacy of individuals, promoting the responsible and transparent handling of personal information by entities, and recognising that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities.[59]

53. The respondent submitted that since the Trial Period, it has made some changes to its business practices. It claimed that it no longer undertakes marketing activities in Australia, and that by the end of March 2020, it had instituted a policy of refusing all requests for accounts from Australia.[60] [Redacted]

54. The respondent's website and form for requesting access to the Facial Recognition Tool remain accessible to Australian IP addresses. I accept, however, that there is no evidence of the respondent more actively marketing its services in Australia, or that it has had any Australian users since March 2020.

55. Notwithstanding these changes (to the extent they were in fact made), the respondent admitted that it continues to collect images from the internet without regard to geography or source.[61] The evidence shows that the exact number of images derived from individuals in Australia is unknown, as, according to the respondent, it does not routinely determine the location or nationality of individuals depicted in images it holds.[62]

56. Having regard to the indiscriminate nature of the respondent's scraping, and the size of the respondent's database (which contains at least 3 billion images),[63] I consider that the respondent has collected, and continues to collect Australians' facial images,[64] and uses them to derive image vectors for its database and to market the Facial Recognition Tool to law enforcement agencies.

57. The respondent asserted that 'the act of downloading an image in the USA' is not carrying on business in Australia. The respondent also appeared to suggest that collecting Scraped Images is 'mere solicitation of business transactions by the internet'[65] and emphasised that there is no relationship or interaction with Australians. These submissions downplay the importance to the respondent's business of collecting Scraped Images and generating vectors from these images.

---

[58] AFP response dated 21 April 2020 p 3-6; and AFP response dated 19 March 2021 p 1-2; Queensland Police response dated 7 August 2020 p 1-5; South Australia Police response dated 14 July 2020 p 1-4; Victoria Police Issue Cover Sheet on the use of Clearview, undated (**Victoria Police Report**) p 1-2.

[59] s 2A of the Privacy Act.

[60] Respondent's response dated 2 November 2020 p 2.

[61] Respondent's response dated 19 August 2020 p 2.

[62] Respondent's response dated 19 August 2020 p 2-4.

[63] Respondent's response dated 25 February 2020 p 2.

[64] As at January 2021 Facebook reportedly had 16.5 million monthly active users, YouTube had 16 million monthly active users, LinkedIn had 6.5 million monthly active users, and Twitter had 5.8 million monthly active users in Australia: https://www.socialmedianews.com.au/social-media-statistics-australia-january-2021/

[65] Respondent's response dated 10 June 2021 p 5, citing *Campbell v Gebo Investments (Labuan) Ltd* (2005) 190 FLR 209.

58. The evidence shows that image scraping from publicly available sources across a global internet is not 'mere solicitation of business transactions on the internet'. Rather, this is an integral part of the respondent's business, as it enables the respondent to build and expand its database, attract customers by marketing the size of its database relative to its competitors, train its algorithm/s, and share and monetize the Scraped Images with users for profit.[66]

59. For example, in emails from the respondent to some Australian police agency users, the respondent stated:

> **What's Clearview**
>
> Clearview is like **Google search for faces**. Just upload a photo to the app and instantly get results from mug shots, social media and other publicly available sources.
>
> Our technology combines the **most accurate** facial identification software worldwide with the **single biggest** proprietary database of facial images to help you find the suspects you're looking for. (Emphasis in original)[67]

60. In another email to Australian police agency users, the respondent stated:

> Our proprietary database is the biggest in the world and it gets bigger every day. Every new day means more potential results from Clearview.[68]

61. In addition, an Australian police agency user was advised by one of the 'creators of the Clearview ID tool' that Clearview was hoping to have 30 billion images indexed by the end of 2020.[69]

62. As stated above, the expression 'carrying on business' may have a different meaning in different contexts and, where used to ensure jurisdictional nexus, the meaning will be informed by the requirement for there to be sufficient connection with the country asserting jurisdiction.[70] The present statutory context includes the object of protecting the privacy of individuals and the responsible handling of personal information collected from individuals in Australia.[71] The Privacy Act is also intended to apply to entities that are based outside of and have no physical presence in Australia, and which collect information from individuals in Australia via a website hosted outside Australia.[72]

63. While in some cases the collection of personal information from Australia may not be sufficient to satisfy the 'carries on business' requirement in s 5B(3)(b), the facts and circumstances outlined above support such a finding in this case. The respondent's activities in Australia involve the automated, repetitious collection of sensitive

---

[66] As noted above at paragraph 11, the respondent filed a provisional patent application in the US on 9 August 2019 which was then followed by filing of both US and international patent applications on 7 August 2020, titled "Methods for Providing Information about a Person Based on Facial Recognition."

[67] AFP response dated 22 May 2020, Attachment A, p 1; Email from Victoria Police to the OAIC, 29 June 2020, Attachment titled "1. Combined", pp 1, 19, 24-27 and 36.

[68] Queensland Police response dated 7 August 2020, pp 25, 27; Email from Victoria Police to the OAIC, 29 June 2020, Attachment titled "1. Combined", pp 16 and 32.

[69] Queensland Police response dated 7 August 2020, p 12.

[70] *Tiger Yacht* at [50].

[71] s 2A of the Privacy Act

[72] Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth), p 218.

information from Australians on a large scale for profit. These transactions are fundamental to the respondent's commercial enterprise.

64. For these reasons, I consider that the respondent has been carrying on business in Australia within the meaning of s 5B(3)(b), and continues to carry on business in Australia as at the date of this determination.

Does the respondent hold personal information in Australia?

65. There is no evidence before me to contradict the respondent's submission that it does not hold information or images in Australia.[73]

66. Accordingly, the information provided to date does not support a finding that the respondent holds personal information in Australia within the meaning of s 5B(3)(c).

Does the respondent collect personal information in Australia?

67. As stated in paragraph 41, for s 5B(3)(c) to be satisfied, 'the personal information' collected (or held) in Australia is the personal information that is the subject of the determination.[74]

68. I consider each type of personal information the subject of this determination, separately below.

Probe images and vectors

69. The evidence shows that during the Trial Period, the respondent collected Probe Images uploaded to the Facial Recognition Tool by registered Australian users (including suspects, victims of crime and members of Australian police agencies who searched themselves or individuals known to them)[75] and vectors generated from those images.

70. Based on the available information, I am satisfied that during the Trial Period, the respondent collected Probe Images and vectors of individuals in Australia, within the meaning of s 5B(3)(c).

Scraped images and vectors

71. The respondent repeatedly asserted that it does not identify whether images of Australians are included in its database.[76] The respondent also submitted that Scraped Images are 'published without requiring password or other security on the open web and as a consequence, published within the USA where [the respondent] conducts its business'.[77]

72. I am also satisfied that the respondent has been collecting Scraped Images, and vectors generated from those images, in Australia at least since October 2019, for the following reasons:

---

[73] Respondent's response dated 19 August 2020, p 3.

[74] *Facebook No 2* at [164] and [172].

[75] AFP response dated 21 April 2020, pp 3-6; AFP response dated 21 April 2020, Annexure D, pp 13-20; AFP response dated 19 March 2021, pp 1-2; Letter from Queensland Police Service to the OAIC dated 26 February 2021 (**Queensland Police response dated 26 February 2021**), pp 1-3; Queensland Police response dated 7 August 2020 pp 4, 22-23, 49, 50; South Australia Police response dated 14 July 2020, pp 2-3.

[76] Respondent's response dated 19 August 2020 p 4; Respondent's response dated 26 September 2020 p 3-4.

[77] Respondent's response dated 10 June 2021 p 4.

- The respondent submitted that it maintains a database of more than 3 billion facial images that it has collected from various publicly available websites.
- The respondent submitted that it indexes Scraped Images and URLs from the internet without targeting particular countries, and is not aware of the location or nationality of individuals depicted in Scraped Images in its database.[78] It therefore does not routinely exclude images based on the location of those individuals.
- The respondent was targeting Australia as a market for their services until March 2020. In doing so, Clearview provided free trials of the service to Australian police agency users, some of whom used the service to upload images depicting individuals located in Australia to find Matched Images.[79]
- For some Australian police agency members who used the respondent's Facial Recognition Tool, the Facial Recognition Tool displayed Matched Images[80] including Matched Images of unknown persons of interest located in Australia.[81]
- Some Australian police agency users, who were Australian residents, searched for and identified images of themselves in the respondent's database.[82]
- The respondent's website previously contained information directed specifically to individuals in Australia, and provided them with the option to opt-out of the respondent's search results.[83]
- Information on the respondent's website previously gave Australians (along with EU, Swiss and UK residents) the option to view search results relevant to themselves.[84]

73. As regards the respondent's submission that it publishes information in the USA (see paragraph 71), the test in s 5B(3)(c) is whether the respondent collected the personal information in Australia before or at the time of the act or practice, not whether personal information was 'published' in Australia or overseas as submitted by the respondent. The Explanatory Memorandum clarifies that collection 'in Australia' includes the collection of personal information from an individual who is physically within the borders of Australia by an overseas entity.[85] It does not matter if the collecting entity is based overseas or if the collection was done for an overseas purpose.

74. Taking into account the indiscriminate nature of the respondent's scraping (including from social media platforms), the size of the respondent's database (which contains at

[78] Respondent's response dated 26 September 2020, p 6.

[79] South Australia Police response dated 14 July 2020, pp 1-4; Queensland Police response dated 26 February 2021, pp 1-3; Queensland Police response dated 7 August 2020 at pp 17, 22; AFP response dated 21 April 2020, pp 3-6; AFP response dated 21 April 2020, Annexure D, pp 13-20; AFP response dated 19 March 2021, pp 1-2.

[80] Victoria Police Report p 1.

[81] Queensland Police response dated 7 August 2020 at p 49 (internal email stating that the author 'had a lot of success identifying unknown POIs and always from Instagram scraping'); Queensland Police response dated 26 February 202, p 3; AFP response dated 19 March 2021 p 2.

[82] Queensland Police response dated 26 February 2021 p 1-3; AFP response dated 19 March 2021 p 1-2.

[83] Respondent's website, Privacy Request Forms: https://clearview.ai/privacy/requests (accessed 17 December 2020)

[84] Ibid.

[85] Explanatory Memorandum to the *Privacy Amendment (Enhancing Privacy Protection) Bill 2012*, Schedule 4, Item 6.

least 3 billion images),[86] and the fact that members of the Australian police agencies have conducted successful searches of the Facial Recognition Tool using facial images of individuals located in Australia,[87] I am satisfied that the respondent's web crawler has collected, and continues to collect, images of many individuals located in Australia for inclusion in its database. I am also satisfied that the respondent collected vectors by generating these from Scraped Images (noting that 'collects' includes collection by 'creation' which may occur when information is created with reference to, or generated from, other information the entity holds).[88]

75. Based on the available information, I am satisfied that the respondent collects Scraped Images and image vectors of individuals in Australia within the meaning of s 5B(3)(c).

Opt out images and vectors

76. As outlined in paragraphs 11 – 12 above, to request an opt-out, the respondent invited individuals, including Australians, to submit a valid email address and an image of themselves which is converted into an image vector. As at the date of this determination, the online form for Australians to opt-out described below is no longer available.

EU/UK/Switzerland/Australia Opt-Out

> This form is designed to enable members of the public to request to opt-out of Clearview search results.
>
> **Why do we need this information?**
>
> Clearview does not maintain any sort of information other than publicly available photos. To find any Clearview search results that pertain to you (if any), we cannot search by name or any method other than image--so we need an image of you.
>
> **What will we do with this information?**
>
> When we are done processing your request, the photo of yourself you shared to facilitate the request is de-identified. You will not appear in any Clearview search results. We will maintain a record of your request as specified by relevant law.[89]

77. For Australian residents, the respondent now only processes requests for opt-out that it receives via email.[90]

78. In response to questions from the OAIC about the number of opt-out and access requests from Australian residents, the respondent submitted that it 'does not track requests by national origin, and so we are unable to answer questions related to the volume of requests, kinds of requests or resolution of requests received from residents of … Australia'.[91]

---

[86] Respondent's response dated 25 February 2020 p 2.
[87] For example, Queensland Police response dated 26 February 2021 p 1-3; Queensland Police response dated 7 August 2020 p 49; AFP response dated 19 March 2021, p 1-2.
[88] https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles/#s2-2-collection-of-personal-information-app-3
[89] Respondent's opt-out form: https://clearviewai.typeform.com/to/zqMFnt
[90] Respondent's response dated 3 June 2021 p 2
[91] Respondent's response dated 26 September 2020 p 8-9.

79. I am satisfied that the respondent also collected the email addresses and images of Australians seeking to make an opt-out request, and vectors generated from those images.

APP entity

Law

80. The Privacy Act regulates the acts and practices of 'APP entities'. An 'APP entity' is either an organisation or an 'agency'.[92]

81. An 'organisation' includes a body corporate that is not a 'small business operator'.[93] A small business operator (**SBO**) includes a body corporate that carries on one or more 'small businesses' and does not carry on a business that is not a small business (and is not excluded from the definition of SBO).[94] A 'small business' is a business that has an annual turnover for the previous financial year that is $3 million AUD or less.[95]

82. Certain entities are excluded from the definition of SBO, including an organisation or body corporate that discloses personal information about another individual to anyone else for a benefit, service or advantage, without the individual's consent or as required or authorised by or under legislation.[96]

Consideration

83. The respondent submitted that:

- It is a small business operator with an annual turnover of less than $3 million AUD.
- It has not had an annual turnover of greater than $3 million AUD in any financial year, and is not related to any business that has had such an annual turnover.
- It does not disclose personal information about individuals for a 'benefit, service or advantage'. The respondent has not established any ongoing relationship with any Australian agency, organisation, body or entity subsequent to providing demonstrations to several Australian police agencies. No personal information was disclosed during those demonstrations, but if it had been, no benefit, service or advantage was received.[97]

84. Despite written requests by the OAIC, the respondent provided no evidence to support its submission that it has not had an annual turnover of greater than $3 million AUD in any financial year, and is not related to any business that has had such an annual turnover.[98]

85. In the absence of any verifiable evidence to the contrary, an inference can be drawn that the respondent is not a small business operator as defined in s 6D of the Privacy Act.

86. Even if the respondent has not had an annual turnover of greater than $3 million AUD in any financial year (and is not related to any business that has had an annual turnover of greater than $3 million AUD), I consider that the exception in s 6D(4)(c) applied during the Trial Period and as at the date of this determination.

---

[92] S 6(1) of the Privacy Act
[93] S 6C of the Privacy Act
[94] s 6C of the Privacy Act.
[95] S 6D(1) of the Privacy Act
[96] S 6D(4)(c) of the Privacy Act
[97] Respondent's response dated 19 August 2020 p 3-4.
[98] Ibid.

87. The evidence shows that during the Trial Period the respondent disclosed Scraped Images about Australian individuals (and associated source URLs), to Australian police agencies as part of the free trials.[99] The purpose of those disclosures was part of a deliberate marketing strategy to attract paying customers.[100]

88. The respondent also continues to disclose Scraped Images of Australians for a benefit, service or advantage, as it has ongoing paid contracts with a number of US government agencies for use of its Facial Recognition Tool.[101] It is reasonable to infer that the respondent discloses Scraped Images of Australians to those registered users, in circumstances where it takes no steps to prevent the search and display of Australians' images (other than through an opt-out mechanism described in paragraph 11 above).

89. The Scraped Images are personal information, collected without consent (see paragraphs 99 to 103 and 150 to 161 below).

90. For these reasons, I am satisfied that even if the respondent had an annual turnover of $3 million AUD or less, the respondent is not a 'small business operator' as the respondent discloses personal information for a benefit, service or advantage, without consent or authorisation by law (s 6C(4)(d)).[102]

'Personal information'

Law

91. The Privacy Act applies to entities that handle 'personal information'.

92. 'Personal information' is defined in s 6(1) as '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'.

93. 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

[99] See, for example, Queensland Police responses dated 26 February 2021 and dated 7 August 2020 that Queensland Police Service members conducted successful searches of individuals in Australia. See also the AFP response dated 19 March 2021 that shows AFP members conducted successful searches of individuals in Australia.

[100] Respondent's response dated 26 September 2020 p 11: 'Obviously, the purpose of a free trial is to sell the product.'

[101] https://www.businessinsider.com.au/ice-clearview-ai-sign-contract-facial-recognition-2020-8?r=US&IR=T; https://www.biometricupdate.com/202008/clearview-ai-wins-biometrics-contract-with-u-s-immigration-and-customs-enforcement-amidst-ongoing-controversy; PIPEDA Report of Findings

[102] s 6D(7)-(8) of the Privacy Act; https://www.oaic.gov.au/privacy/privacy-for-organisations/trading-in-personal-information/.

> "about an individual" it might be about the individual when combined with other information.[103]

94. 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.[104]

95. Whether a person is 'reasonably identifiable' is an objective test that has practical regard to the context in which the particular information is handled.

96. Generally speaking, an individual is 'identified' when, within a group of persons, that person is 'distinguished' from all other members of a group.[105] Certain information may be unique to a particular individual, and may, on its own, establish a link to the particular 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.[106] This means that even if an organisation that collects or holds information does not know the subject person's identity, they may be handling 'personal information' because the individual is reasonably identifiable by another person (or machine) other than the subject themselves.

97. An individual will be 'reasonably' identifiable where the process or steps for that individual to be identifiable are reasonable to achieve. The context in which the data is held or released, and the availability of other datasets or resources to attempt a linkage, are key in determining whether an individual is reasonably identifiable.[107]

Consideration

98. The respondent submitted that it does not collect or handle any personal information. It submitted that:

- It collects publicly available images, from the open web.
- No data is maintained in relation to the images other than the actual image itself, webpage title and the URL of the site on which the image was sourced.
- It does not store associated information with the image, concerning the identification of the subject matter in the image.[108]
- When a customer searches the Facial Recognition Tool, the identity of the individual in the Probe Image and any Matched Image may remain unknown. This is comparable to *WL v La Trobe University* [2005] VCAT 2592 (*La Trobe University*), in which Deputy President Coghlan stated:

---

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

[104] 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.

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

[106] 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/.

[107] 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/.

[108] Respondent's response dated 19 August 2020 p 2, 4.

> Even allowing for the use of external information, the legislation requires an element of reasonableness about whether a person's identity can be ascertained from the information and this will depend upon all the circumstances in each particular case.[109]

- Whilst it is possible that an individual could be identified by a 'single click on the URL', there is no evidence to suggest that an individual can or is likely to be identified by a single click on the URL.[110] Therefore, Scraped Images and Probe Images are not reasonably identifiable.
- Image vectors provide a mechanism to distinguish one image from another (rather than to identify an individual). An image vector cannot be used independently to derive information about a person's physical characteristics; it is a numerical abstraction of an image generated by a neural network. Whilst an image vector in the hands of the respondent or its customer may be used to then distinguish one image from which it is derived, it does not in itself identify the subject individual contained in the image. The identification of the subject individual will still require additional steps of inquiry. Image Vectors are therefore not personal information under the Privacy Act as they are not 'about' the individuals but are about the way in which the respondent delivers its services (see *Telstra Corporation Limited and Privacy Commissioner* [2015] AATA 991). [111]
- [Redacted][112]

Scraped Images and Probe Images

99. As Scraped Images and Probe Images show individuals' facial images, I am satisfied that those images are 'about' an individual, under the definition of 'personal information.'

100. I am also satisfied that an individual is reasonably identifiable from their facial image under the definition of 'personal information' 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 processes the Scraped Images and Probe Images for the purpose of biometric identification (see paragraphs 137 to 142).
- Members of Victoria Police, Queensland Police Service and the AFP conducted successful searches of the Facial Recognition Tool.[113]

101. As regards the Tribunal's findings in *La Trobe University*, this decision involved differences in facts and law. The Tribunal applied the Victorian *Information Privacy Act 2000 (Vic)* (**IP Act**), in force at the time. The definition of 'personal information' under that law differs from the definition of 'personal information' in the Privacy Act.[114] Under the

---

[109] *WL v La Trobe University* [2005] VCAT 2592 at [52].
[110] Respondent's response dated 10 June 2021 p. 3
[111] Respondent's response dated 10 June p 3–4.
[112] Respondent's response dated 2 November 2020 p 4.
[113] Victoria Police Report, Queensland Police response dated 26 February 2021 p 1-2; Queensland Police response dated 7 August 2020 p 23; AFP response dated 19 March 2021 p 1-2.
[114] Section 3 of the Information Privacy Act 2000 defined personal information as information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is

Privacy Act, 'personal information' extends to information about 'an individual who is reasonably identifiable', whereas under the IP Act, 'personal information' extended to information about an individual whose identity 'can reasonably be ascertained, from the information or opinion'.

102. In addition, the 'personal information' considered in *La Trobe University* did not involve facial images, biometric information or facial recognition systems.

103. For these reasons, I am satisfied that Probe Images and Scraped Images constitute information about a reasonably identifiable individual, and accordingly, that they are 'personal information' as defined in s 6(1) of the Privacy Act.

Image vectors

104. The respondent submitted that information in image vectors is not 'about' individuals, but about the way in which the respondent delivers its services. The respondent referenced Deputy President Fogie's analysis in *Telstra Corporation Limited and Privacy Commissioner* (*Telstra and Privacy Commissioner*)[115] in support of this submission.

105. In an appeal from this decision to the Federal Court,[116] the full Federal Court (Dowsett, Kenny and Edelman JJ) also considered 'about an individual' under the definition of 'personal information' that applied at the time. Kenny and Edelman JJ 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. However, in every case it is necessary to consider whether each item of personal information requested, individually or in combination with other items, is about an individual. This will require an evaluative conclusion, depending upon the facts of any individual case, just as a determination of whether the identity can reasonably be ascertained will require an evaluative conclusion.[117]

106. That is, image vectors can have multiple subject matters. They could be about the way the respondent delivers its services, as well as about the individual from whose image they are generated.

107. Whether information is 'about' an individual is a question of fact depending on the context and the circumstances of each particular case. These digital templates are also clearly about an individual, as they are direct representations of a particular individual's facial features generated from facial images. A Probe Image Vector is a mathematical representation of information in a Probe Image. A Scraped Image Vector is a

---

apparent, or can reasonably be ascertained, from the information or opinion, but does not include information of a kind to which the Health Records Act 2001 applies'.

[115] [2015] AATA 991 at [112] to [113].

[116] *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 (19 January 2017).

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

mathematical representation of information in a Scraped Image (see above at paragraph 5).[118]

108. The respondent also submitted that an image vector cannot be used independently to derive information about a person's physical characteristics, and does not in itself identify the subject individual contained in the image.[119]

109. 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 individual can be identified from available information, including, but not limited to, the information in issue.[120] I have found that these vectors are used in an automated biometric identification system, for the reasons set out at paragraphs 137 to 141. In this context, I am also satisfied that individuals depicted in these vectors are reasonably identifiable.

110. For these reasons, I am satisfied that Probe Image Vectors and Scraped Image Vectors constitute information about a reasonably identifiable individual, and that they are 'personal information' as defined in s 6(1) of the Privacy Act.

Opt-out Vectors

111. The respondent collects a facial image and an email address from individuals that submit a request to opt out of search results (see paragraph 11 above). From this image, the respondent generates a mathematical representation of that person's image. The respondent subsequently deletes the image.[121]

112. However, the respondent retains the Opt-out Vector (and an anonymised hash of the email address) permanently, in order to prevent images of the individual requesting opt-out from being returned in search results and to prevent further collection of any images of that person. Where there is a match, the respondent omits any images in its database showing the individual depicted in that vector from future search results.[122]

113. Through this process of linking and comparing datasets, an individual in an Opt-out Vector is uniquely distinguishable from all other individuals in the respondent's database. It is irrelevant that the respondent does not retain the original image from which the vector was generated.

114. For these reasons, I am satisfied that Opt-out Vectors constitute information about a reasonably identifiable individual, and that they are 'personal information' as defined in s 6(1) of the Privacy Act.

Findings on breach

115. As noted at paragraphs 13 and 17, my findings are based on evidence gathered during the period of my Office's preliminary inquiries and investigation (from 21 January

---

[118] Letter from the respondent to the ICO dated 4 August 2020 (**respondent's response dated 4 August 2020**) p 2.

[119] Respondent's response dated 10 June p 3–4.

[120] 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/.

[121] Respondent's response dated 26 September 2020 p 10.

[122] Respondent's response dated 26 September 2020 p 9-10.

2020 to 21 May 2021), and the respondent's response to the preliminary view dated 10 June 2021.

APP 3.3

Law

116. APP 3.3 requires an APP entity not to collect sensitive information about an individual unless:

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

117. The requirements in APP 3.3 apply, even if personal information is collected from a publicly available source.

Collection

118. An APP entity collects personal information 'only if the entity collects the personal information for inclusion in a record or generally available publication' (s 6(1) of the Privacy Act). The term 'record' is defined in s 6(1) and includes a document or an electronic or other device.

119. The term 'collects' applies broadly, and includes gathering, acquiring or obtaining personal information from any source and by any means, including from biometric technology, such as voice or facial recognition.[123] It includes collection by 'creation' which may occur when information is created with reference to, or generated from, other information the entity holds.[124]

Sensitive information and biometrics

120. The definition of 'sensitive information' 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 'biometric templates'.[125]

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

122. 'Biometrics' encompass a variety of different technologies that use probabilistic matching to recognise a person based on their biometric characteristics. Biometric characteristics can be physiological features (for example, a person's fingerprint, iris, face or hand geometry), or behavioural attributes (such as a person's gait, signature, or keystroke pattern).[126] These characteristics cannot normally be changed and are persistent and unique to the individual.

123. 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

[123] APP Guidelines [B.23]-[B.28].

[124] https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-data-analytics-and-the-australian-privacy-principles/#s2-2-collection-of-personal-information-app-3

[125] s 6(1) of the Privacy Act.

[126] 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.*

biometric system.[127] 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.

124. '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.

Consent

125. 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.[128]

126. 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.[129]

127. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity.[130]

128. It is only appropriate to infer consent from an opt-out mechanism in limited circumstances, as the individual's intention in failing to opt-out may be ambiguous. An APP entity will be in a better position to establish the individual's implied consent the more that the following factors, where relevant, are met:

- The opt-out option was clearly and prominently presented.
- It is likely that the individual received and read the information about the proposed collection, use or disclosure, and the option to opt-out.
- The individual was given information on the implications of not opting out.
- The opt-out option was freely available and not bundled with other purposes.
- It was easy for the individual to exercise the option to opt out, for example, there was little or no financial cost or effort required by the individual.
- The consequences of failing to opt-out are not serious.
- An individual who opts out at a later time will, as far as practicable, be placed in the position as if they had opted out earlier.[131]

Exceptions to APP 3.3

129. There are a number of exceptions to APP 3.3.

130. These relevantly include an exception where there is a serious threat to life, health or safety:

---

[127] 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).
[128] APP Guidelines [B.35]
[129] APP Guidelines [B.41].
[130] APP Guidelines [B.37].
[131] APP Guidelines [B.40].

> An APP entity may collect sensitive information if:
>
> (a) it is unreasonable or impracticable to obtain the individual's consent to the collection, and
>
> (b) the entity reasonably believes the collection is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.[132]

131. For this exception to apply, there must be a reasonable basis for the belief, and not merely a genuine or subjective belief.[133] It is the responsibility of an APP entity to be able to justify its reasonable belief. A collection, use or disclosure would not be considered necessary where it is merely helpful, desirable or convenient.[134]

Consideration

Does the respondent 'collect' personal information as defined in s 6(1)?

132. The respondent submitted that it 'gathers images and links from the open web (respecting robots.txt) and from public-facing portions of social media sites (respecting user-enabled privacy settings)'.[135] [Redacted][136]

133. On that basis, I am satisfied that the respondent 'collects' the Scraped Images, as that term is defined in s 6(1) of the Privacy Act (see paragraphs 118 to 119 above).

134. The respondent's Facial Recognition Tool analyses Scraped Images, Probe Images and Opt-Out images to produce a vector for each image. As collection under the Privacy Act includes creation of personal information from existing information, I am also satisfied that the respondent 'collects' these vectors under the Privacy Act (see paragraphs 118 to 119 above).

Does the respondent collect 'sensitive information'?

Scraped and Probe Images and associated vectors

135. The respondent made the following submissions:

- The respondent collects publicly available images, including images of individuals.[137] The images are processed for facial recognition.[138]
- The respondent's algorithm, which is premised on complex mathematical formulas, generates image vectors [redacted][139] from Scraped and Probe Images by measuring certain characteristics of an individual's face.[140]

---

[132] APP 3.4(b), section 16A(1), Item 1.
[133] APP Guidelines, [B.111].
[134] APP Guidelines [C.8].
[135] Letter from the respondent to the ICO dated 21 July 2020 (**respondent's response dated 21 July 2020**) p 2.
[136] Respondent's response dated 26 September 2020 p 7.
[137] Respondent's response dated 19 August 2020 p 2.
[138] Respondent's response dated 25 February 2020 p 2.
[139] Respondent's response dated 2 November 2020 p 5.
[140] Respondent's response dated 26 September 2020 p 7.

- The Facial Recognition Tool compares Probe Image Vectors against Scraped Image Vectors. If the Image Vectors are sufficiently similar, the Scraped Image will be returned as a search result.[141]

136. In subsequent submissions the respondent sought to explain that an image vector is not a biometric measure in the ordinary sense, but a 'numerical abstraction of an image generated by a neural network'.[142]

137. I am satisfied that, consistent with the definition of 'biometrics' in paragraph 122, Scraped and Probe Images show physiological features of an individual's face. The vectors generated from these images record information about measurements of an individual's facial characteristics. For each kind of information, the recorded characteristics pertaining to an individual are persistent, cannot normally be changed and are unique to that individual. For these reasons, Scraped and Probe Images collected by the respondent, and the vectors generated from these images, are 'biometric information'.

138. The respondent's Facial Recognition Tool compares an unknown person's biometric characteristic (in the Probe Image and Probe Vectors) to other characteristics of the same type in its database (Scraped Images and Scraped Vectors). The tool is based on an algorithm developed through machine learning technology.[143] The purpose of this one-to-many system is to identify any Scraped Images that match the Probe Image and display those matches to the user.[144]

139. I am satisfied that this is an automated process. Biometric characteristics are used to distinguish an individual from all other individuals depicted in Scraped Images in the respondent's Database in order to display Matched Images to registered users.[145] This allows the user to identify that individual.

140. The evidence before me shows that members of Victoria Police, Queensland Police Service and the AFP conducted successful searches with the Facial Recognition Tool.[146]

141. On this basis, I am satisfied that Scraped and Probe Images and vectors generated from these are 'biometric information that is to be used for the purpose of automated biometric identification.'

142. Furthermore, Scraped and Probe Image Vectors are derived from facial images by using an algorithm, which is premised on complex mathematical formulas, to measure certain characteristics of an individual's face.[147] That is, the respondent creates representations of individuals' biometric information and stores these in a biometric

---

[141] Respondent's response dated 10 June 2021 p 2-3.
[142] Respondent's response dated 10 June 2021 p 3.
[143] Respondent's response dated 4 August 2020 p 3.
[144] The respondent's response of 19 August 2020 p 2: 'The goal of Clearview is to provide a research tool for use by law enforcement agencies, one which can assist them in their processes of inquiry to identify or investigate perpetrators and victims of crime.'
[145] The evidence shows that some searches of the respondent's Facial Recognition Tool conducted by Australian police force users, resulted in the display of Matched Images for individuals located in Australia. See Queensland Police response dated 7 August 2020 p 23; Queensland Police response dated 26 February 2021 p 1-3; AFP response dated 19 March 2021 p 1-2.
[146] Victoria Police Report, Queensland Police response dated 26 February 2021 p 1-2; Queensland Police response dated 7 August 2020 p 23; AFP response dated 19 March 2021 p 1-2.
[147] Respondent's response dated 26 September 2020 p 7.

identification system. On that basis, I am satisfied that these kinds of vectors are 'biometric templates'.

Opt-out vectors

143. As discussed at paragraph 11, the respondent's Facial Recognition Tool generates Opt-Out Vectors from facial images uploaded by individuals. It then applies automated algorithmic analysis to compare the biometric characteristics in the Opt-Out Vector against other image vectors it holds in its database. Where the comparison finds a match, the Facial Recognition Tool excludes matched images from a user's search results.

144. Consistent with the definition and explanations above, I am satisfied that Opt-Out Vectors are biometric information that is to be used for the purpose of automated biometric verification or biometric identification' and 'biometric templates'.

145. Therefore, I am satisfied that Scraped and Probe Images and vectors derived from these images, as well as Opt-out Vectors, are sensitive information under the Privacy Act. Accordingly, the respondent must obtain consent before collecting these kinds of sensitive information (unless an exception in APP 3.4 applies).

Did individuals consent to the collection of their sensitive information?

146. I accept the respondent's submission that it does not obtain express consent to collect images from the Internet. There is also no evidence that the respondent obtained express consent to collect Probe Images or any image vectors.

147. While entities should generally not rely on implied consent when collecting sensitive information,[148] I have considered whether individuals impliedly consented to the collection of their personal information.

Probe Images and Probe Image Vectors

148. I am not aware of any basis for inferring the consent of witnesses, suspects and victims depicted in Probe Images (and vectors derived from those images), to the collection of their sensitive information by the respondent from the Australian police agencies.

149. On this basis, I am not satisfied that these individuals consented to the collection of their images and vectors derived from their images during the Trial period.

Scraped Images and Scraped Image Vectors

150. I have considered whether individuals impliedly consented to the collection of their Scraped Images and derived vectors, in the following circumstances:

- The respondent asserted that it collects Scraped Images from publicly viewable webpages.
- The respondent submitted that it does not collect any images protected by user enabled privacy settings, such as those associated with certain social media accounts, or from pages that enabled 'robots.txt'. [149]
- During my investigation, the respondent provided some information in its Privacy Policy (available on its website), about its collection of public images. In particular:

[148] APP Guidelines [B.41].

[149] Respondent's response dated 21 July 2020 p 2; Respondent's response dated 4 August 2020 p 3, 5.

- The respondent's Privacy Policy dated 29 January 2020 stated:

  Under the heading, 'What data do we collect?':

  > Publicly available images: Clearview uses proprietary methods to collect publicly available images from various sources on the Internet.

  Under the heading, 'Why do we collect data and how do we use it?':

  > Clearview collects publicly available images and shares them, along with the source of the image, in a searchable format with our users, who are all law enforcement, security and anti-human trafficking professionals in the United States. This enables users to: Facilitate law enforcement investigations of crimes; Investigate and prevent fraud and identity theft Clearview does not compile, analyze, combine with other data, or otherwise process the images we collect in order to link them to real persons on behalf of users.

- The respondent's Privacy Policy dated 20 March 2021 stated:

  Under the heading, 'What Data Do We Collect?':

  > Information derived from publicly available photos: As part of Clearview's normal business operations, it collects photos that are publicly available on the Internet. Clearview may extract information from those photos including geolocation and measurements of facial features for individuals in the photos.

  Under the heading, 'Why Do We Collect Data?':

  > The publicly available images collected by Clearview are shared, along with the source of the image, in a searchable format with our users, who are all law enforcement, security and national security professionals. Personal information derived from users is not shared by Clearview with its users.

151. For the reasons set out below, I am not satisfied that consent can be implied in these circumstances, as any such consent would not have met the requirements outlined at paragraphs 125 to 128 above.

152. Consent may not be implied if an individual's intent is ambiguous or there is reasonable doubt about the individual's intention.[150] I consider that the act of uploading an image to a social media site does not unambiguously indicate agreement to collection of that image by an unknown third party for commercial purposes. In fact, this expectation is actively discouraged by many social media companies' public-facing policies, which generally prohibit third parties from scraping their users' data.[151] Moreover, consent could certainly not be inferred where an individual's image is uploaded by another individual (including individuals depicted in the background of a Scraped Image) or where an individual inadvertently posts content on a social media website without changing the public default settings.

153. Consent also cannot be implied if individuals are not adequately informed about the implications of providing or withholding consent. This includes ensuring that an individual is properly and clearly informed about how their personal information will be handled, so they can decide whether to give consent.[152] The respondent's publicly

[150] APP Guidelines [B.39].

[151] See Twitter's terms of service at section 4, available at: Twitter Terms of Service; LinkedIn's User Agreement at section 8.2, available at: https://www.linkedin.com/legal/user-agreement.

[152] APP Guidelines [B.47].

accessible policy documents did not provide clear information about image vectors. Although the 20 March 2021 Privacy Policy referred to extracting 'measurements of facial features for individuals', I consider that this was insufficient to enable individuals to understand that image vectors were being collected, the purpose of collection and how they would be handled by the respondent. Any consent purported to be provided through these policy documents would not have been adequately informed.

154. Even if these policy documents had referred to the creation of biometric templates, an APP entity cannot infer consent simply because it has published a policy about its personal information handling practices.[153] 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.[154] Any such consent would not be current and specific to the context in which that information is being collected, and bundles together different uses and disclosures of personal information.

155. Consent also cannot be implied from the fact that individuals did not make a request to opt out. The opt-out mechanism was bundled with the collection of further personal and sensitive information (including images, email addresses and an Opt-out Vector). The onus cannot be entirely on the individual to find out about the respondent's practices, locate this opt-out mechanism, and submit their sensitive information to the respondent for processing, particularly in circumstances where failure to opt-out may have serious consequences for the individual (see APP 3.5 discussion below from paragraph 168).

156. There is also no evidence that the respondent gave any consideration to whether individuals from whom it collects Scraped Images and associated image vectors, including children, had the capacity to understand and communicate their consent.

157. Accordingly, I am not satisfied that individuals consented to the collection of their Scraped Images and vectors created from those images.

Opt-Out Vectors

158. I have also considered whether individuals consented to the collection of their Opt-out Vectors when following the opt-out process outlined in paragraph 11.

159. I acknowledge that the respondent's opt-out request form sought consent from individuals to share a photo of themselves and the purpose for which it will be used. In addition, the respondent's Privacy Policy includes some information about the kind of personal information collected for this purpose, and how that information is processed.

160. However, nowhere on the respondent's opt-out request form, policies or website did the respondent inform individuals that it would collect an Opt-out Vector through algorithmic analysis of their facial image.

161. Accordingly, I am not satisfied that individuals consented to the collection of their Opt-out Vectors.

Exceptions to APP 3.3

162. I have considered whether the exceptions in APP 3.4 applied.

---

[153] *Flight Centre Travel Group (Privacy)* [2020] AICmr 57 (25 November 2020), [53].
[154] *Flight Centre Travel Group (Privacy)* [2020] AICmr 57 (25 November 2020), [55].

163. While the respondent did not raise any exception in APP 3.4, given the respondent offers its services to law enforcement agencies, I have considered whether the 'serious threat to life, health or safety' exception applied to permit the collection of Australians' sensitive information in the circumstances. For this exception to apply, a condition that must be met is that the respondent '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'.[155]

164. I consider that there was no reasonable basis to support such a belief.

165. The respondent's database includes at least 3 billion images. The vast majority of those individuals have never been and will never be implicated in a crime, or identified to assist in the resolution of a serious crime. While some of the information collected might be useful for law enforcement at different times, there is no evidence that the collection of this information is necessary, as opposed to merely desirable or convenient, for that purpose. The exception does not authorise the automated mass collection of Australians' data merely because some of this data might be useful to law enforcement at a future point in time.

166. On that basis, I am not satisfied that there was a reasonable basis for any belief that collection of Australian individuals' sensitive information by the respondent was necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety. Accordingly, the exception in APP 3.4(b), s 16A(1), Item 1, did not apply.

Finding – APP 3.3

167. I find that the respondent interfered with the privacy of the following groups of Australian individuals by collecting sensitive information without consent in breach of APP 3.3:

- individuals whose Scraped Images and derived vectors were collected by the respondent in Australia
- individuals such as witnesses, victims and suspects, whose Probe Images were collected by the respondent in Australia during the Trial Period
- individuals whose Opt-out Vectors were collected by the respondent for the purpose of actioning a deletion or opt-out request during the period the opt-out mechanism was available to Australians.

APP 3.5

168. An APP entity must collect personal information by fair means. A 'fair means' of collecting information is one that does not involve intimidation or deception, and is not unreasonably intrusive.[156] Collection may also be unfair where an entity misrepresents the purpose or effect of collection.[157]

169. When assessing whether a collection is 'unfair' for the purposes of APP 3.5, all the circumstances must be considered.[158] For example, it would usually be unfair to collect

---

[155] APP 3.4(b), s 16A, item 1.

[156] Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth), p 77.

[157] APP Guidelines [3.63].

[158] *'LP' and The Westin Sydney (Privacy)* [2017] AICmr 53 (7 June 2017) [33].

personal information covertly without the knowledge of the individual. However, this may be a fair means of collection if undertaken in connection with a fraud investigation.

Consideration

170. The respondent submitted that it gathers images and links from the open web (respecting robots.txt) and public-facing portions of social media sites (respecting user-enabled privacy settings).[159]

171. The respondent admitted that it does not notify individuals depicted in the images of the collection of their images.[160]

Collection of Scraped Images and Scraped Image Vectors

172. I infer from the evidence that the vast majority of individuals would not have been aware or had any reasonable expectation[161] that their Scraped images and vectors had been collected by the respondent and included in the respondent's database. This is because:

- The respondent does not notify individuals when their image is scraped from a publicly available web page.[162]
- It is likely that many Scraped Images in the respondent's database were not uploaded to the Internet by the individual/s in those images. For example, an image might be uploaded to a publicly available site by a friend, a business such as a newspaper or by another third party.
- The respondent collects images from social media websites, including Facebook and YouTube.[163] The publicly available terms and conditions for these sites, which are made available to users upon registration, each prohibit this kind of scraping (see paragraph 152 above) and a number of social media companies have sent the respondent cease and desist letters in relation to alleged scraping from their sites.[164]
- The respondent's publicly available Terms of Service and Privacy Policies provided limited information about its information handling practices. For example, they did not explain:
  - how the respondent collects Scraped Images or the particular sites they are gathered from[165]
  - that the respondent generates and stores biometric templates (again I note that a reference to extracting 'measurements of facial features for individuals in the photos' in the 20 March 2021 Privacy Policy is insufficient to inform individuals about this practice)
  - how the respondent's algorithm analyses Scraped Images to generate vectors

---

[159] Respondent's response dated 21 July 2020 p 2.
[160] Respondent's response dated 19 August 2020 p 2.
[161] *'LP' and The Westin Sydney (Privacy)* [2017] AICmr 53 (7 June 2017).
[162] Respondent's response dated 19 August 2020, p 2.
[163] Respondent's response dated 25 February 2020 p 2-3.
[164] Correspondence to the OAIC from online platforms, including Twitter and LinkedIn.
[165] Relevantly, the Data Policy only states 'Clearview uses proprietary methods to collect publicly available images from various sources on the Internet. https://clearview.ai/privacy/privacy_policy '

- how vectors derived from Probe Images are used to identify sufficiently similar image vectors
- which third parties may be shown Matched Images, and the countries those third parties are located in.

173. In these circumstances and in the absence of specific and timely information about the respondent's collection practices, I am satisfied that the respondent's collection of Scraped images and vectors constituted covert collection.

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

175. Individuals may also be harmed through misuse of the Facial Recognition Tool for purposes other than law enforcement. For example, the respondent's patent application filed 7 August 2020 demonstrates the capability of the technology to be used for other purposes including dating, retail, granting or denying access to a facility, venue, or device, accurately dispensing social benefits and reducing fraud.[166]

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

177. I acknowledge that in some circumstances covert collection of personal information may not be unfair. While Australia's privacy laws recognise that the protection of individuals' privacy is not an absolute right, any instance of interference, including for law enforcement objectives, must be subject to a careful and critical assessment of its necessity, legitimacy and proportionality.[167]

178. In this case, I do not accept that the impact on individuals' privacy was necessary, legitimate and proportionate, having regard to any public interest benefits of the Facial Recognition Tool. Relevantly:

- Biometric systems, such as the Facial Recognition Tool, capture sensitive and potentially immutable identity information. By its nature, this information may not be reissued or cancelled like other forms of compromised identification information. It may also be replicated for identity theft purposes.
- The respondent collected the personal information of millions of individuals, only a fraction of whom would ever be connected with law enforcement investigations. The evidence shows that this included the information of vulnerable individuals, including victims of crime and children.[168]
- Although some of the information the respondent collected may have been used by Australian and overseas law enforcement agencies, the information was collected for the respondent's private commercial purposes. Specifically, the respondent collected personal information as part of a for-profit commercial enterprise, to train and

[166] US Patent and Trademark Office, *United States Patent Application*, 20210042527, Thon-That, Cam-Hoan, filing date 7 August 2020, publication date 11 February 2021.

[167] 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>.

[168] See Victoria Police Report, p 1.

improve the respondent's algorithm, and monetize the respondent's technology and data holdings through contractual arrangements.

179. Having regard to the kind of information collected by the respondent, the respondent's commercial purposes, and the covert and indiscriminate method of collection, I consider that the covert collection of Scraped images and vectors was unreasonably intrusive.

Finding – APP 3.5

180. I find that the respondent interfered with the privacy of individuals by collecting Australians' Scraped Images and vectors derived from these images, by unfair means in breach of APP 3.5.

APP 5

181. 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 matters referred to in APP 5.2 or to otherwise ensure that the individual is aware of any such matters.

182. Reasonable steps to notify must be taken at or before the time the APP entity collects an individual's personal information. If this is not practicable, the entity must notify as soon as practicable after collection.

183. The matters referred to in APP 5.2 include:

- if 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 (APP 5.2(b), and
- the purposes for which the APP entity collects the personal information (APP 5.2(d).

184. 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 the practicability, including the time and cost of taking measures.[169]

Consideration

185. The respondent submitted that:

- It does not take steps to identify individuals prior to collecting their Scraped Images, and accordingly does not notify those individuals about the collection or the respondent's business activities.[170]
- From 29 January 2020, it began to offer Australian residents an online form to 'opt-out' from its search results (see paragraph 11). Screenshots of the process are at Attachment B. However, during the investigation this form became no longer accessible.
- Its Privacy Policy is accessible through its website.[171]

[169] APP Guidelines [5.4].
[170] Respondent's response dated 19 August 2020 p 2.
[171] Respondent's response dated 21 July 2020 p 3.

- It provided a link to its Data Policy to Australian residents, in response to access requests made through the portal available on its website.[172] As set out at paragraph 12, this portal is longer accessible to Australian residents.

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

186. The respondent's Data Policy and Privacy Policies which applied up to the conclusion of my investigation addressed some of the matters in APP 5.2. However, there were notable deficiencies:

- The policies provided limited information about the circumstances of collecting facial images. They did not explain the method of collection (ie. automated scraping), or the kinds of entities from which information is collected (such as social media companies).
- The policies provided limited information about how image vectors are collected, or that they are collected and retained each time the respondent collects a Scraped Image.

187. There is no evidence that the respondent provided any other information to individuals depicted in Scraped Images or to individuals submitting an opt-out request about the APP 5 matters.

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

188. As noted at paragraph 154, 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 under APP 5 or obtaining consent.

189. Even if the respondent's Privacy Policy and/or Data Policy had included all of the information listed at APP 5.2, I am not satisfied that this would have constituted reasonable steps under APP 5 in circumstances where:

- The respondent's business model involves covertly collecting personal information from third party sources, rather than directly collecting personal information from individuals. It is unlikely that individuals depicted in Scraped Images would have been aware of the respondent's Privacy Policy or would have sought it out, as most of these individuals would have had no direct dealings with the respondent.
- The Data Policy was not easily accessible, as it was only provided when an individual made an access request.
- Some individuals in Scraped Images may have had particular needs, such as children or individuals from a non-English speaking background (noting the evidence at paragraph 178 that the respondent's database includes images of children).
- Noting the sensitivity of the information collected and potential adverse consequences for individuals as a result of the collection (see APP 3.5 discussion), the respondent was required to take more rigorous steps to ensure individuals are notified under APP 5.

[172] Respondent's response dated 26 September 2020 p 6.

Finding – APP 5

190. I find that the respondent interfered with the privacy of Australian individuals by failing to take reasonable steps to notify individuals about the fact and circumstances of collecting, and the purpose of collecting, Scraped Images and Scraped Image vectors in breach of APPs 5.2(b) and (d).

191. I also find that during the period the respondent offered the opt-out mechanism referred to in paragraph 11, the respondent interfered with the privacy of individuals by failing to take reasonable steps to notify individuals about the fact and circumstances of collecting, and the purpose of collecting, Opt-out image vectors in breach of APPs 5.2(b) and (d).

APP 10

192. APP 10.2 requires an APP entity to take such steps (if any) as are reasonable in the circumstances to ensure that the personal information it uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant (**quality factors**).

193. An APP entity 'discloses' personal information where it makes it accessible to others outside the entity and releases the information from its effective control.[173]

194. Personal information is inaccurate if it contains an error or defect as well as if it is misleading.[174]

195. The fact that there has been an incident of personal information being disclosed where it does not meet the quality factors does not mean that the APP entity has not complied with APP 10.2. The requirement is that an entity take reasonable steps.

196. Reasonable steps that an entity should take depend upon the circumstances, including the sensitivity of the personal information; the entity's size, resources and business model; possible adverse consequences for the individual if quality is not ensured; and the practicability, including the time and cost of taking measures. [175]

197. In their Report of Findings into the respondent's activities in Canada, Canadian Data Protection Authorities outline a range of considerations that I also consider relevant to assessing the accuracy of facial recognition technologies:

> Despite advances in the sophistication of facial recognition technology through the increase of computational capacity, the improvement of underlying algorithms and the availability of huge volumes of data, such technologies are not perfect and can result in misidentification. This can be the result of a variety of factors, including the quality of photos/videos and the performance of algorithms used to compare facial characteristics. In particular, our Offices take note of claims of accuracy concerns stemming from a variety of studies and investigations of facial recognition algorithms found in a number of technology solutions.
>
> Accuracy issues in facial recognition technology can take two general forms: (i) failure to identify an individual whose face is recorded in the reference database, referred to as a "false-negative"; or (ii) matching faces that actually belong to two different individuals, referred to as a "false positive." While the former is an issue primarily for the users of facial recognition technology, the latter presents

[173] APP guidelines [B.64]
[174] APP guidelines [10.12].
[175] APP guidelines [10.6].

compelling risks of harm to individuals, particularly when facial recognition is used in the context of law enforcement.[176]

In particular, we refer to reports that facial recognition technology has been found to have significantly higher incidences of false positives or misidentifications when assessing the faces of people of colour, and especially women of colour, which could result in discriminatory treatment for those individuals.[177] For example, research conducted by NIST (National Institute of Standards and Technology) found that the rate of false positives for Asian and Black individuals was often greater than that for Caucasians, by a factor of 10 to 100 times.[178] Harms resulting from such misidentification can range from individuals being excluded from opportunities, to individuals being investigated and detained based on incorrect information.[179]

Consideration

What steps did the respondent take to ensure the accuracy of personal information it disclosed?

198. During my investigation, the respondent made the following public representations about the accuracy of the Facial Recognition Tool:

- The respondent's Code of Conduct stated: 'The Clearview app is neither designed nor intended to be used as a single-source system for establishing the identity of an individual, and users may not use it as such.'[180]
- The respondent's website stated:
  - 'Clearview AI's technology empowers agencies to quickly, accurately, and efficiently identify suspects, persons of interests and victims of crime.'[181]
  - 'Clearview AI's mission is to deliver the most comprehensive identity solutions in the world … We provide a revolutionary set of facial identification products which feature world-class accuracy and unmatched scale.'[182]
  - 'Independently Assessed For Accuracy An independent panel of experts assessed the accuracy of Clearview AI's search results and found no errors.'[183]

---

[176] Angwin, J. *et al.*. "Machine Bias," *ProPublica*, May 23, 2016.

[177] See "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," *National Institute of Standards and Technology* (NIST), December 2019; "Black and Asian faces misidentified more often by facial recognition software," *CBC News*, December 2019, and "Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use," *Washington Post*, December 2019.

[178] "Face Recognition Vendor Test, Part 3: Demographic Effects," *National Institute of Standards and Technology* (NIST), December 2019.

[179] Joint investigation by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec (CAI), the Information and Privacy Commissioner for British Columbia (OIPC BC), and the Information and Privacy Commissioner of Alberta (OIPC AB), PIPEDA Report of Findings #2021-001 (2 February 2021), available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/#fn56

[180] Clearview Code AI Code of Conduct, available at: https://clearview.ai/help/code_of_conduct#:~:text=Our%20User%20Code%20of%20Conduct,these%20essential%20rules%20of%20use.

[181] https://clearview.ai/

[182] https://clearview.ai/overview

- In emails to prospective trial users, the respondent stated: 'Our technology combines the **most accurate** facial identification software worldwide with the **single biggest** proprietary database of facial images to help you find the suspects you're looking for.' (emphasis in original)[184]

199. [Redacted][185]

200. The respondent also relevantly stated:

> Clearview search results are indicative, not definitive. They do not purport to be a "match" between the individual in the user-uploaded probe image and the search result. … To mitigate the risks associated with false positives, Clearview's terms of service require users to independently verify any information or investigative lead obtained through a Clearview search result. Clearview instructs its users to not rely solely on the search results they receive.[186]

201. The respondent submitted the accuracy of the Facial Recognition Tool was evaluated by an 'Independent Review Panel'. In support, the respondent provided a copy of a report titled, *Clearview AI Accuracy Test* Report dated October 2019 (the **Accuracy Report**), which describes the accuracy test performed by the independent panel (the **October 2019 test**).[187]

202. The October 2019 test involved comparing publicly available headshots of 834 US legislators against the respondent's database of 2.8 billion images (at the time).

203. For each individual in the test, the two top-ranked matches returned from the respondent's database were compared with the submitted image.

204. According to the respondent, the three panel members reviewed the Matched Images and assessed whether the matches were accurate. The panel confirmed that 'Clearview rated 100% accurate'.[188]

205. An extract of the Accuracy Report, including a summary of the methodology, conclusion and descriptions of the panel members, was sent to the AFP.[189]

206. The respondent otherwise declined to respond to the OAIC's questions about reasonable steps taken to ensure accuracy in a notice issued under s 44 of the Privacy Act on 7 July 2020.[190]

Did the respondent take reasonable steps to ensure the accuracy of the personal information disclosed?

207. The respondent's business offers a facial recognition service to law enforcement for profit. As part of this service, the Facial Recognition Tool discloses Matched Images to registered users (see paragraph 5).

208. The respondent handles a substantial and rapidly expanding volume of personal information, from which serious decisions may be made by its law enforcement users. In

---

[183] https://clearview.ai/legal
[184] Queensland Police response dated 7 August 2020 p 32, 38, 58, 63, 73, 81.
[185] Respondent's response dated 4 August 2020 p 3.
[186] Respondent's response dated 4 August 2020 p 3.
[187] Respondent's response dated 26 September 2020 Attachment B.
[188] Respondent's response dated 26 September 2020 response p 16.
[189] AFP response dated 21 April 2020, Annexures Part 1, Annexure C, p 15.
[190] OAIC s 44 notice dated 7 July 2020, questions 57 and 58, p 15.

circumstances where a variety of studies have uncovered concerns with the accuracy of different facial recognition technologies, and significant harm may flow from misidentification (see paragraph 197), the steps needed to ensure accurate disclosures, should be robust, demonstrable, independently verified and audited.

209. I give little weight to the respondent's claims that it does not guarantee accuracy. The statements on the respondent's website during my investigation and its statements to prospective users, outlined in paragraph 198 above, clearly indicate that the purpose of displaying Matched Images alongside Probe Images following a search request, was to enable the user to identify the individual in the Probe Image. Having regard to this purpose, reasonable steps must be taken to ensure any matches disclosed to the user, are accurate.

210. I am not satisfied that the steps the respondent took to ensure the accuracy of Matched Images it disclosed, were reasonable in the circumstances.

211. The respondent's submissions only provided evidence of a single accuracy test – the October 2019 test.

212. According to the respondent, this test was based on a test conducted by the American Civil Liberties Union (ACLU) in July 2018.[191] The ACLU test assessed the accuracy of a different facial recognition technology, by searching a database of 25,000 mugshots against public photos of all members of the House and Senate. The ACLU's test incorrectly matched 28 members of Congress. The false matches were disproportionately people of colour.[192]

213. There is no evidence that the respondent designed, or engaged an independent expert to design, a methodology tailored to assess the accuracy of the respondent's proprietary technology. Instead, the methodology was adapted from a test designed for a different facial recognition technology. In comparison to the respondent's dataset of at least 3 billion images scraped from the Internet, the ACLU test involved a point-in-time dataset of 25,000 images that was compared to professional images of public figures.

214. I consider that this led to material limitations in the testing methodology, including, for example:

- The October 2019 test compared the top two ranked search results with the submitted image. However, when a user searches the Facial Recognition Tool, all Matched Images and associated URLs in the respondent's database are displayed as search results.
- The respondent trains and populates its database by using an automated web crawler to scrape facial images from the internet. US legislators are public figures whose facial images are accessible on the websites of the applicable legislatures, their own websites, media articles, and social media platforms. Individuals depicted in Probe Images may have less of an online presence, which may affect accuracy.
- Based on the biographies included in the Accuracy Report,[193] it is unclear that the panel members who participated in the October 2019 test had appropriate expertise or qualifications in facial recognition. It is not necessarily a prerequisite to have particular expertise or qualifications. However, if the panel members were being

[191] Respondent's response dated 26 September 2020 p 16.

[192] https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

[193] Respondent's response dated 26 September 2020 p 19-20.

presented by the respondent as an 'independent panel of experts' [194] and tasked with designing a program for assessing the accuracy of the Facial Recognition Tool, it would have been reasonable for them to have had a demonstrated conceptual and/or technical understanding of facial recognition systems and the circumstances in which common risks associated with such systems, such as inaccuracy, may manifest.

215. There is no evidence that the respondent engaged independent experts to conduct subsequent accuracy tests.

216. There is also no evidence that the respondent implemented mechanisms to train and improve its algorithm based on false positive results. [Redacted][195]

217. Having regard to the sensitivity of the data, the risk of harm to individuals in disclosing inaccurate images to its users, and the well-documented potential for accuracy issues with facial recognitions systems, I am not satisfied that the respondent took reasonable steps to ensure the accuracy of Matched images disclosed to users.

Finding – APP 10.2

218. I find that the respondent interfered with the privacy of individuals whose Matched Images it disclosed to its users, by not taking reasonable steps to ensure that the Australians' personal information it discloses was accurate, having regard to the purpose of disclosure, in breach of APP 10.2.

APP 1.2

219. 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.

220. APP 1.2 imposes a distinct and separate obligation on APP entities, as well as being a general statement of its 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 a constant one. An entity could consider keeping a record of the steps taken to comply with APP 1.2, to demonstrate that personal information is managed in an open and transparent way.[196]

221. The reasonable steps that an APP entity should take will depend upon the circumstances, including the nature of the personal information held and the service provided, and the possible adverse consequences for an individual if their personal information is not handled as required by the APPs. The practicability of such steps is also a relevant consideration (including the 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.[197]

222. Examples of practices, procedures and systems that an APP entity should consider implementing include:

- procedures for identifying and managing privacy risks at each stage of the information lifecycle, including collection, use, disclosure, storage, destruction or de-identification

---

[194] Respondent's response dated 26 September 2020 p 10, 15-20; https://www.clearview.ai/legal

[195] Respondent's response dated 4 August 2020 p 3.

[196] APP Guidelines [1.5].

[197] APP Guidelines [1.6].

- 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 Privacy Impact Assessment (**PIA**) for new projects in which personal information will be handled, or when a change is proposed to information handling practices. A PIA is a written assessment of an activity or function that identifies the impact that the activity or function might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact. 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
- 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.[198]

Consideration

Procedures for de-identification/ destruction of personal information

223. As part of complying with APP 1.2, APP entities must put in place practices, procedures and systems to support compliance with APP 11.2. APP 11.2 requires an entity that no longer needs personal information it holds for a purpose permitted under the APPs, to take reasonable steps to de-identify or destroy the information. It is the responsibility of an APP entity to be able to justify that reasonable steps were taken.

224. [Redacted][199] The respondent otherwise declined to respond to the OAIC's questions about any practices, procedures or systems it has in place to identify images that are no longer needed for any purpose for which the personal information may be used or disclosed under the APPs.[200] The respondent also declined to respond to questions about the steps it takes to destroy images in its database after those images have been identified.[201]

225. Although the respondent emphasised that it gathers images and links from the open web and from public-facing portions of social media sites, there is no evidence that the respondent takes proactive steps to identify when information it previously collected is no longer public. For example, the respondent does not proactively identify when:

- the source webpage from which the respondent originally collected an individual's information has been taken down from the internet.
- an individual has changed the privacy settings of their information on a social media website such that the information is no longer publicly available.

226. There is no evidence of other relevant measures implemented by the respondent.

---

[198] APP Guidelines [1.7].

[199] Respondent's response dated 21 July 2020 p 3.

[200] Section 44 notice issued to the respondent on 7 July 2020 asked the respondent to 'advise what steps Clearview takes to destroy images in its database after the images have been taken down from the website of origin, whether pursuant to Clearview's forms and processes at https://clearview.ai/privacy/requests or otherwise' (at question 67, p 17).

[201] Section 44 notice issued to the respondent on 7 July 2020 asked the respondent to advise what: 'a. practices procedures and systems Clearview has in place to identify images that are no longer needed for any purpose for which the personal information may be used or disclosed under the APPs; and b. steps Clearview takes to destroy images in its database after those images have been identified' (at question 66, p 17).

227. As I have discussed in paragraphs 172-180 above, I consider that the respondent collected Australians' personal information in breach of the APPs. It follows that there is no purpose for which that personal information may be retained under the APPs.

228. Even if the respondent were permitted to use and disclose the information under the Privacy Act, at a minimum, it would have been reasonable for the respondent to take additional steps in the circumstances, including implementing a data retention policy, that:

- enabled the respondent to proactively identify personal information that must be destroyed or de-identified under APP 11.2
- ensured that such information was destroyed, or de-identified as required
- documented how the policy would be implemented, including through ongoing staff training and monitoring and auditing compliance.

A commitment to conducting a privacy impact assessment for new projects in which personal information will be handled

229. For many new projects or updated projects involving personal information, undertaking a PIA may be a reasonable step under APP 1.2.[202] Whether conducting a PIA is a reasonable step, will depend on a project's size, complexity and scope, and the extent to which personal information will be collected, used or disclosed. The greater the project's complexity and privacy scope, the more likely it is that a comprehensive PIA will be required, to determine and manage the privacy impacts of the project.

230. There is no evidence that the respondent conducted a systematic assessment of measures and controls that should be implemented to identify and mitigate the risks associated with the Facial Recognition Tool.

231. In assessing whether undertaking a PIA was a reasonable step in the circumstances before deploying the Facial Recognition Tool, the following considerations are relevant:

- The Facial Recognition Tool is a novel technology developed by the respondent, which involves a new way of handling personal information.
- The Facial Recognition Tool handles a very large amount of personal information. An essential element of the Facial Recognition Tool is the ongoing, automated collection, use and disclosure of personal information.
- Sensitive information, which is generally afforded a higher level of privacy protection under the APPs than other personal information, is involved.
- The handling of sensitive information through the Facial Recognition Tool has the potential to adversely affect individuals (see paragraph 174).
- There is likely to be a significant public interest in the privacy aspects of the Facial Recognition Tool and its potential to lead to increased surveillance and monitoring of individuals.[203]

232. In these circumstances, I am satisfied that conducting a PIA before allowing user access to the Facial Recognition Tool, would have been a reasonable step under APP 1.2.

---

[202] OAIC Guidance and advice, *Australian Entities and the EU General Data Protection Regulation (GDPR)* available at: https://www.oaic.gov.au/privacy/guidance-and-advice/australian-entities-and-the-eu-general-data-protection-regulation/

[203] https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/

Finding – APP 1.2

233. I acknowledge that there appear to have been some positive developments in the respondent's practices, procedures and systems in Australia since the OAIC first made contact with the respondent on 21 January 2020, as outlined at paragraph 53 above.

234. Despite these changes, I have identified a range of limitations in the current steps taken to comply with APP 1.2. For the reasons set out above, I find that the respondent did not take reasonable steps to implement practices, procedures and systems relating to the entity's functions or activities that would ensure that it complied with the APPs, in breach of APP 1.2.

Remedies

235. There are a range of regulatory options that I may take following an investigation commenced on my own initiative. For example, I have powers to accept an enforceable undertaking, make a determination (which may include declarations requiring the entity to take certain steps), or apply to the court for a civil penalty order.

236. In determining what form of regulatory action to take, I have considered the factors outlined in the OAIC's Privacy Regulatory Action Policy[204] and the OAIC's Guide to Privacy Regulatory Action.[205] The following factors weigh in favour of making a determination that finds the respondent has interfered with individuals' privacy and breached APP 1.2, and must not repeat or continue the conduct:

- The objects in s 2A of the Privacy Act include promoting the protection of the privacy of individuals and promoting responsible and transparent handling of personal information by entities.
- The conduct is serious:
  - Although the exact number of affected Australians is unknown, that number is likely to be very large, given that it may include any Australian individual whose facial images are publicly accessible on the internet.
  - The matter involves the sensitive biometric information of all the affected Australian individuals.
  - The evidence suggests that the respondent collects the personal information of vulnerable groups, including victims of crime and children (see paragraph 178).
- The burden on the respondent likely to arise from the regulatory action is justified by the risk posed to the protection of personal information.
- There is specific and general educational, deterrent or precedential value in making a determination in this matter.
- There is a disagreement about whether an interference with privacy has occurred, and this determination allows this question to be resolved.
- There is a likelihood that the respondent will continue to contravene Australian privacy law in the future if a determination is not made.

[204] Privacy Regulatory Action Policy [38].
[205] Guide to Privacy Regulatory Action [4.9].

237. I consider there is a public interest in making a determination setting out my reasons for finding that an interference with privacy and breach of APP 1.2 have occurred, and the appropriate response by the respondent.

Declarations

238. In considering what declarations should be made under s 52(1A), I have had regard to the respondent's current activities in Australia, and the steps it has taken to withdraw from the Australian market.

239. I accept that the respondent has instituted a policy of refusing all requests for user accounts from Australia[206] and that there is no evidence of Australian users since March 2020. I acknowledge the respondent's submissions that the respondent no longer offers trials of the Facial Recognition Tool to Australian users, [redacted] and has redesigned its website to no longer provide an access or opt-out mechanism to Australian residents.[207]

240. However, these steps do not address the ongoing acts or practices that I have found are interferences with privacy and a breach of APP 1.2. During my investigation the respondent provided no evidence that it is taking steps to cease its large scale collection of Australians' sensitive biometric information, or its disclosure of Australians' Matched Images to its registered users for profit. These ongoing breaches of the APPs carry substantial risk of harm to individuals, which I have outlined at paragraphs 174 to 178.

241. For these reasons, I consider it reasonable and appropriate to make the declarations in paragraphs 2(a) – (b) under s 52(1A)(a)(ii) of the Privacy Act. These require the respondent not to repeat or continue the acts or practices that I have found to be an interference with privacy. They also require the respondent to cease to collect images and vectors for the Facial Recognition Tool, from individuals in Australia. Paragraph 2(d)(i) requires the respondent to confirm such collections have ceased, within 90 days of the date of this determination.

242. I also consider it reasonable and appropriate to make the declarations in paragraph 2(c) under s 52(1A)(b) of the Privacy Act requiring the respondent to destroy all Scraped Images, Probe Images, Scraped Image Vectors, Probe Image Vectors and Opt-out Vectors it has collected from individuals in Australia in breach of the Privacy Act. In the circumstances of this case, I am not satisfied that de-identification is a viable step for the respondent to take to ensure compliance with the APPs, noting that the purpose of the Facial Recognition Tool is to enable automated biometric identification of individuals. Paragraph 2(d)(ii) requires the respondent to confirm it has destroyed these images and vectors as required, within 90 days of the date of this determination.

Angelene Falk
Australian Information Commissioner and Privacy Commissioner

22 October 2021

[206] Respondent's response dated 2 November 2020 p 2.
[207] Respondent's response dated 3 June 2021 p 2.

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.

Attachment A

Relevant Law – *Privacy Act 1988* (Cth)

Determination powers

52 Determination of the Commissioner

(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.

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.

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

1.1 The object of this principle is to ensure that APP entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

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.

APP Privacy policy

1.3 An APP entity must have a clearly expressed and up-to-date policy (the ***APP privacy policy***) about the management of personal information by the entity.

1.4 Without limiting subclause 1.3, the APP privacy policy of the APP entity must contain the following information:

(a) the kinds of personal information that the entity collects and holds;

(b) how the entity collects and holds personal information;

(c) the purposes for which the entity collects, holds, uses and discloses personal information;

(d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;

(e) how an 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;

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

(g) if the entity is likely to disclose 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 policy.

Availability of APP privacy policy etc.

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

(a) free of charge; and

(b) in such form as is appropriate.

Note: An APP entity will usually make its APP privacy policy available on the entity's website.

1.6 If a person or body requests a copy of the APP privacy policy of an APP entity in a particular form, the entity must take such steps as are reasonable in the circumstances to give the person or body a copy in that form.

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.

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;

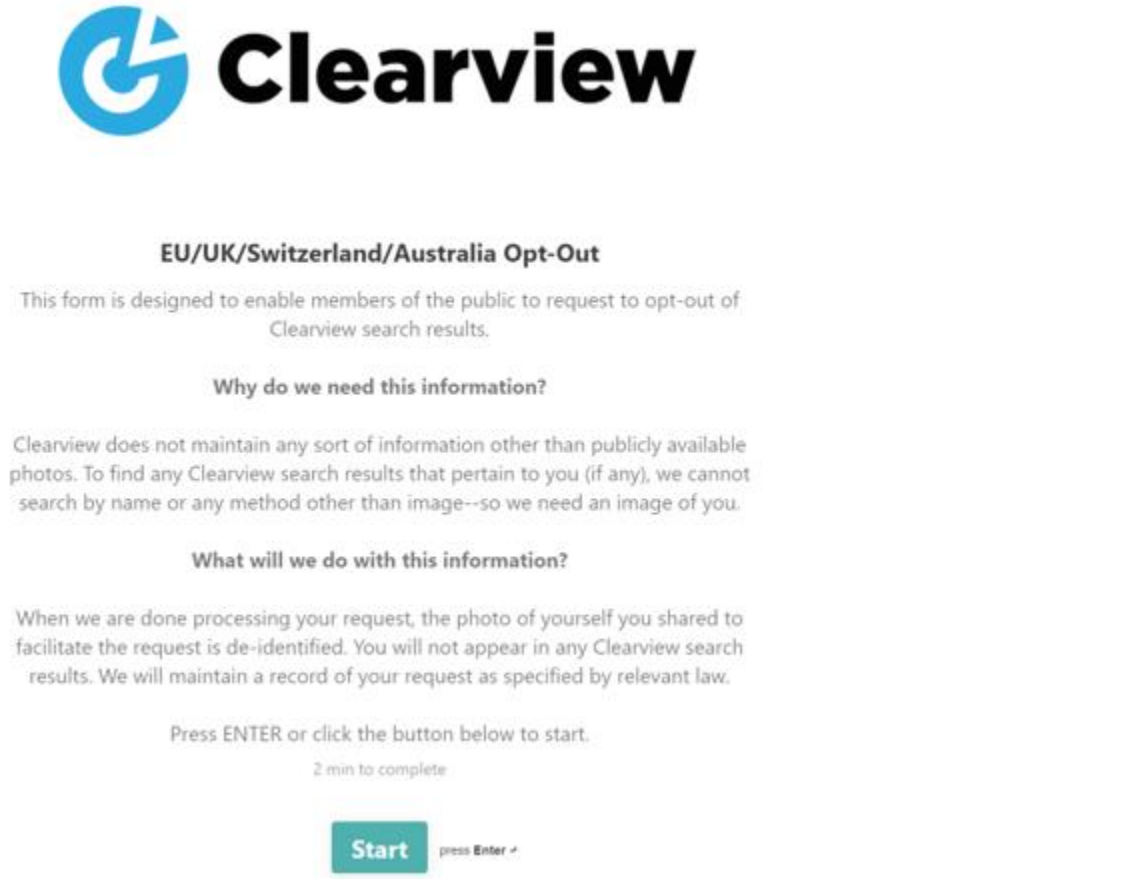
(j) if the APP entity is likely to disclose the personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the notification or to otherwise make the individual aware of them.

Australian Privacy Principle 10—quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

Attachment B



Clearview

EU/UK/Switzerland/Australia Opt-Out

This form is designed to enable members of the public to request to opt-out of Clearview search results.

Why do we need this information?

Clearview does not maintain any sort of information other than publicly available photos. To find any Clearview search results that pertain to you (if any), we cannot search by name or any method other than image--so we need an image of you.

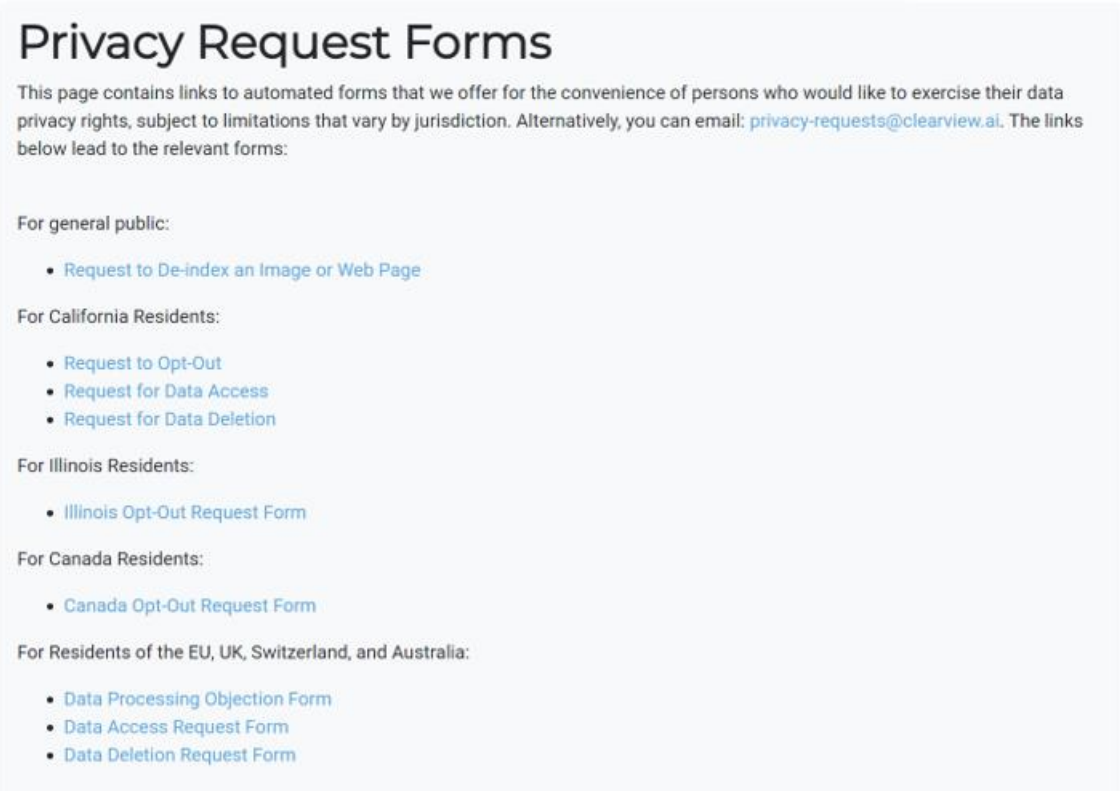
What will we do with this information?

When we are done processing your request, the photo of yourself you shared to facilitate the request is de-identified. You will not appear in any Clearview search results. We will maintain a record of your request as specified by relevant law.

Press ENTER or click the button below to start.

2 min to complete

Start press Enter



Privacy Request Forms

This page contains links to automated forms that we offer for the convenience of persons who would like to exercise their data privacy rights, subject to limitations that vary by jurisdiction. Alternatively, you can email: privacy-requests@clearview.ai. The links below lead to the relevant forms:

For general public:

- Request to De-index an Image or Web Page

For California Residents:

- Request to Opt-Out
- Request for Data Access
- Request for Data Deletion

For Illinois Residents:

- Illinois Opt-Out Request Form

For Canada Residents:

- Canada Opt-Out Request Form

For Residents of the EU, UK, Switzerland, and Australia:

- Data Processing Objection Form
- Data Access Request Form
- Data Deletion Request Form