

From: [Justin Lodge](#)
To: [s.47G](#)
Cc: [Sophie Higgins](#); [Wendy Tian](#); [Carla Wolnizer](#)
Subject: Joint investigation of Clearview AI Inc. [SEC=OFFICIAL]
Date: Tuesday, 21 July 2020 2:41:00 PM
Attachments: [CII20_00006_210720.pdf](#)
[Attachment 3 - CII20_00006_070720.pdf](#)
[image001.jpg](#)
[image002.png](#)
[image003.png](#)
[image004.png](#)
[image005.png](#)

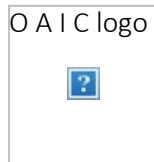
Dear Mr Mulcaire,

I refer to the correspondence of 7 July 2020 from the Information Commissioner's Office UK and the Office of the Australian Information Commissioner (the 'OAIC') advising of a joint investigation of Clearview AI Inc.

Please find attached a response from the OAIC (**Attachment 1**) to your email of 13 July 2020, in which you requested an extension to respond to the the attached notice dated 7 July 2020.

If you have any questions, please feel free to contact us.

Regards



Justin Lodge | A/g Director
Dispute Resolution Branch
Office of the Australian Information Commissioner
GPO Box 5218 Sydney NSW 2001 | oaic.gov.au
+61 2 8231 4203 | Justin.Lodge@oaic.gov.au

 |  |  |  [Subscribe to OAICnet newsletter](#)

From: s 47C
To: [Justin Lodge](#)
Cc: [Sophie Higgins](#); [Wendy Tian](#); [Carla Wolnizer](#)
Subject: Re: Joint investigation of Clearview AI Inc. [SEC=OFFICIAL]
Date: Wednesday, 22 July 2020 5:11:13 AM


CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Hello Mr. Lodge,

I'm currently working on pulling together a response to your Agency's inquiries. Thank you for granting a partial extension. Regrettably, I will not be able to provide the response you've requested by today but we will respond appropriately as soon as possible.

Regards,
Jack Mulcaire
Counsel, Clearview AI

s 47G

From: [Justin Lodge](#)
To: 
Cc: [Sophie Higgins](#); [Wendy Tian](#); [Carla Wolnizer](#)
Subject: RE: Joint investigation of Clearview AI Inc. [SEC=OFFICIAL]
Date: Wednesday, 29 July 2020 2:51:43 PM
Attachments: [image001.jpg](#)
[image002.png](#)
[image003.png](#)
[image004.png](#)
[image005.png](#)

Dear Mr Mulcaire,

Thank you for your email.


We note that the deadline for providing some of the information and documents requested by our office is 4 August 2020. We look forward to receiving the other information and documents as soon as possible.

Regards



Justin Lodge | A/g Director
Dispute Resolution Branch
Office of the Australian Information Commissioner
GPO Box 5218 Sydney NSW 2001 | oaic.gov.au
+61 2 8231 4203 | Justin.Lodge@oaic.gov.au

 |  |  |  [Subscribe to OAICnet newsletter](#)

From: Jack M 
Sent: Wednesday, July 22, 2020 5:11 AM
To: Justin Lodge <justin.lodge@oaic.gov.au>
Cc: Sophie Higgins <sophie.higgins@oaic.gov.au>; Wendy Tian <wendy.tian@oaic.gov.au>; Carla Wolnizer <carla.wolnizer@oaic.gov.au>
Subject: Re: Joint investigation of Clearview AI Inc. [SEC=OFFICIAL]

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Hello Mr. Lodge,

I'm currently working on pulling together a response to your Agency's inquiries. Thank you for granting a partial extension. Regrettably, I will not be able to provide the response you've requested by today but we will respond appropriately as soon as possible.

Regards,
Jack Mulcaire

Counsel, Clearview AI

s 47G [REDACTED]

From: [Sophie Higgins](#)
To: [Carla Wolnizer](#)
Subject: FW: Correspondence from the ICO and the OAIC [SEC=OFFICIAL]
Date: Monday, 14 September 2020 9:27:06 AM
Attachments: **s 33**
[image001.jpg](#)
[image002.png](#)
[image003.png](#)
[image004.png](#)
[image005.png](#)


From: Justin Lodge <justin.lodge@oaic.gov.au>
Sent: Friday, September 11, 2020 6:44 PM
To: Jack M **s 47G**
Cc: Mark Love <Mark.Love@ballawyers.com.au>; Sophie Higgins <sophie.higgins@oaic.gov.au>; David Reynolds <**s 47F**> Ciara Hagan <**s 47F**>
Subject: Correspondence from the ICO and the OAIC [SEC=OFFICIAL]





Dear Jack Mulcaire,

I refer to the joint investigation by the Information Commissioner's Office UK and the Office of the Australian Information Commissioner into the acts or practices of Clearview AI Inc.

Please find attached a letter regarding the matter.

Yours sincerely,

 **Justin Lodge** | A/g Director
Dispute Resolution Branch
Office of the Australian Information Commissioner
GPO Box 5218 Sydney NSW 2001 | oaic.gov.au
+61 2 8231 4203 | Justin.Lodge@oaic.gov.au

 |  |  |  [Subscribe to OAICnet newsletter](#)

 **Sophie Higgins** | Director
Dispute Resolution Branch
Office of the Australian Information Commissioner
GPO Box 5218 Sydney NSW 2001 | oaic.gov.au
02 9284 9775 | sophie.higgins@oaic.gov.au

 |  |  |  [Subscribe to Information Matters](#)

David Reynolds
Lead Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

T. **s 47F** F. 01625 524510 ico.org.uk twitter.com/iconews

Please consider the environment before printing this email
For information about what to do with personal data see our [privacy notice](#)

Ciara Hagan

Lead Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9
5AF

T. s 47F F. 01625 524510 ico.org.uk twitter.com/iconews

Please consider the environment before printing this email
For information about what to do with personal data see our [privacy notice](#)

FOIREQ23/00215 -47-

From: [Justin Lodge](#)
To: [John Molloy](#); [Emi Christensen](#); [Karin Van Eeden](#); [Wendy Tian](#); [Carla Wolnizer](#)
Subject: FW: Response to Inquiries of 11 September 2020 [SEC=OFFICIAL]
Date: Monday, 28 September 2020 9:06:08 AM
Attachments: [Sept 25 Response to ICO and OAIC.pdf](#)

fyi

From: Jack Mulcaire <s 47G>
Sent: Saturday, September 26, 2020 3:05 AM
To: Ciara Hagan <s 47F> David Reynolds <s 47F>
Sophie Higgins <sophie.higgins@oaic.gov.au>; Justin Lodge <justin.lodge@oaic.gov.au>
Subject: Response to Inquiries of 11 September 2020

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Dear Information Commissioner's Office and Office of the Australian Information Commissioner,

Please see the attached .pdf document which contains our response to your most recent letter.

Regards,
Jack Mulcaire
Counsel, Clearview AI
s 47G



Information Commissioner's Office

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Via Email

Dear Ms. Hagan, Mr. Reynolds, Mr. Lodge and Ms. Higgins,

I write to respond to your inquiry of 11 September 2020. While Clearview AI continues to cooperate with the ICO and OAIC's investigation, we must again emphasize our belief that Clearview AI is not subject to the jurisdiction of your offices. Clearview AI does not offer its product in the United Kingdom or Australia, does not have any operations in the United Kingdom or Australia, and does not monitor the whereabouts, preferences or behaviors of residents in either country. Absent any jurisdiction, we are unaware of any legal basis upon which your organizations could take enforceable actions against Clearview AI.

Nevertheless, in an effort to demonstrate our interest in operating as a good corporate citizen, which is mindful of the importance of individuals' privacy rights, Clearview AI continues to respond to your inquiries, and has voluntarily extended certain privacy rights to residents of the United Kingdom and Australia. These actions are not in any way a concession that Clearview AI is subject to the jurisdiction of either the United Kingdom or Australia.

Below we address the questions raised in your letter of 11 September.

s 33





s 33

2. We wish to address the following question again, as we were unable to gain a detailed understanding from your previous response. As such, please provide a detailed breakdown of Clearview AI Inc's current company structure, including the location of any Clearview offices.

Clearview AI is a privately-held corporation, incorporated in the State of Delaware, USA. Clearview AI's headquarters are located at 214 W. 29th St. 2nd Floor, New York N.Y. 10001, USA. Clearview AI has two wholly-owned U.S. subsidiaries, Rocky Mountain Data Analytics LLC and Insight Camera LLC, which have no employees, assets or operations.

3. Within the response to Q7 you have confirmed that you presently do not offer your services to users/clients within the UK. You have also confirmed that Clearview does not monitor the behavior of data subjects within the European Union. Please explain how Clearview is able to ensure that the service does not collect images (and the URL where Clearview found the image) of European and/or Australian data subjects, and more specifically, of Australian and UK data subjects.

Please see response to Question 5 below.



4. Further to the above, in response to Q15 you have advised that you block IP addresses from countries in which Clearview does not offer its services. Please provide a detailed breakdown of the countries in which IP addresses are blocked.

This response constitutes a confidential business secret as it describes technical security measures necessary to protect the security of our platform from attackers. s 47G

[REDACTED]

5. In response to Q10, you have advised that the Clearview service indexes images of individuals *'without targeting particular countries and without knowledge of their national origin'*. As such, how does Clearview ensure that they do not store images relating to data subjects located in Australia and the UK? Please provide a detailed response.

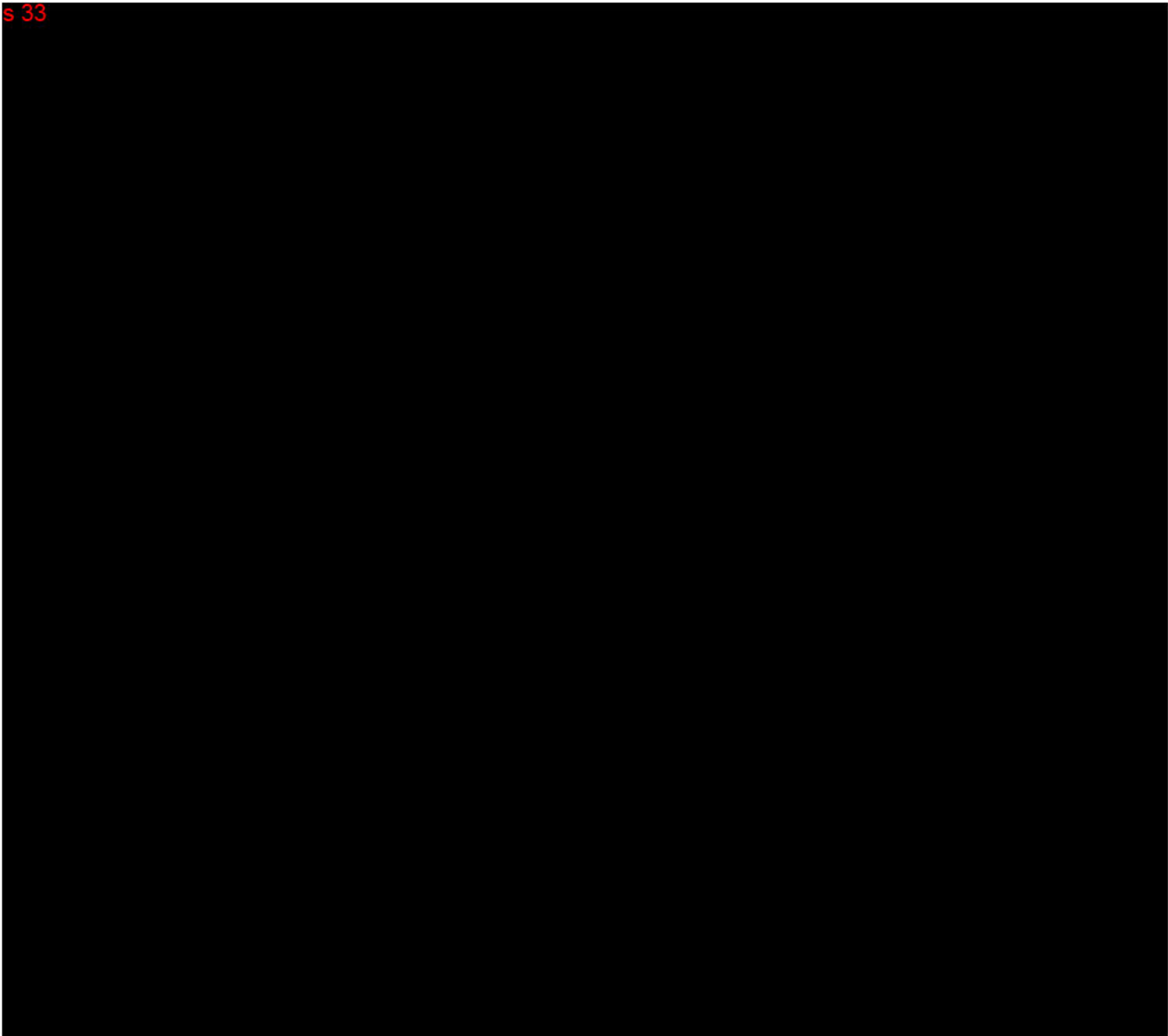
This response constitutes a confidential business secret as it would be to our detriment should competitors or third parties wishing to manipulate the search engine learn more on how our algorithm works. Clearview AI is an image search engine. Clearview AI collects images from the public internet, and makes them available through a proprietary search methodology. The search engine cannot determine the nationality of a person. Hence, we cannot exclude that the search also concerns Australian and UK residents. It is in the nature of the Internet that information made public is accessible through search engines worldwide.

The only data that Clearview AI associates with those images for its users is the URL of the site from which the image was originally retrieved. Despite this common use of publicly available photographs, the premise of this question and question 3 appears to us to presume that Clearview AI's collecting of images from publicly available internet sites constitutes monitoring, as that term is understood in the context of the GDPR. We disagree with that presumption for the following reasons.



Clearview AI's algorithm allows users of Clearview AI's services, which we again note are all based outside of the UK and Australia, effectively to undertake a reverse image search. The user has an image of an individual, and uses the Clearview AI app to locate any publicly available images that the algorithm can potentially match to the original image. If there is a potential match, the user is presented only with the publicly available images in the Clearview AI system and the URLs to the internet pages where those public images reside. No other personal data or information is provided to users. There is no method by which users, for example, could search by an individual's name, address or other personal identifiers.

s 33





s 33

6. In response to Q16 you have provided your 'Data Policy', how and where would a data subject be able to access this document?

Once a data subject makes a request through our publicly available data subject portal, they are sent a response, which contains a link to our Data Policy.

7. Further to the above, you have also supplied a copy of your privacy policy, which includes a section on Clearview's 'legal basis for processing'. In response to Q13 you advised that Clearview has no requirement to 'identify a legal basis under the GDPR/DPA 2018'. Please advise which piece of legislation Clearview are satisfying in stipulating its legal bases for processing within the privacy policy.

As is the case with every privacy policy from every company, not everything contained in a privacy policy is required by a particular law; and that is so with Clearview AI's privacy policy. Clearview AI's privacy policy provides *more* disclosures than are strictly necessary and provides *more* rights to individuals than Clearview AI believes it is legally obligated to provide. We do this in an effort to be transparent with the public as to how we handle data and not because we are compelled to make these disclosures. We are unaware of any law that prevents Clearview AI from providing *more* disclosures and individual rights than the applicable law strictly requires.

8. Does Clearview share any personal data with third party organisations? If so with whom and for what purpose?



This response constitutes a confidential business secret as it describes our technical infrastructure and which must be kept secret from potential attackers and competitors. We understand the question to relate to our product and not to our employees' data (where, for example, we need to share data with fiscal authorities as any other company). In the context of our product, we do not rely on any third party to collect, vectorize, compare or report search results. We do not share personal data with third parties, unless the third party acts according to our instructions and on our behalf. Users who receive search results obtain only a publicly available image and the URL for that image, which itself is publicly available. We understand that this would fall under the category of a "data processor" in the sense of the European law. Examples for such data processors are the provider of our customer relationship management tool, Hubspot, and the provider of our webforms, Typeform. The purpose of these processors is to process personal data on our behalf in order to be able to manage customer relationships, and provide functional webforms to collect information from persons requesting access to our application and from persons submitting data subject requests. s47G

[REDACTED]

9. In a court document, Clearview stated that it algorithmically converts publicly collected photos into mathematical formulas based on facial geometry. Please confirm whether this is correct.

Clearview AI's proprietary algorithm takes images and measures certain characteristics of an individual's face. The method by which the algorithm works is premised on complex mathematical formulas, the precise nature of which are trade secrets of Clearview AI. We otherwise cannot comment on ongoing litigation.

10. Does any organisation carry out any processing (including collection, vectorisation, comparison and reporting search results) of personal data on behalf of Clearview? If so, please provide full details of the organisation and a copy of any contract in place for such processing.



Clearview AI's product does not rely on any third party organization to collect, vectorize, compare or report search results. As described in response to question 8, Clearview AI works with certain service providers who process personal data on our behalf.

s 33

12. Clearview's website includes a form which enables residents of the EU, UK and Australia to request to view Clearview search results relevant to themselves.

Please provide the following information:

- a. The date on which this process was implemented.
- b. Details of the processes Clearview had in place prior to that date.
- c. The number of requests to access search results Clearview has received from UK residents.
- d. Details of how Clearview responded to the access requests, including whether UK residents were provided with access to search results relevant to themselves.
- e. The number of requests to access search results Clearview has received from Australian residents.
- f. Details of how Clearview responded to the access requests, including whether Australian residents were provided with access to search results relevant to themselves.

The form went live on 29 January 2020. Prior to that, Clearview AI permitted data subjects to submit requests via email. As mentioned above, Clearview AI 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 the United Kingdom or Australia.

As a general matter, Clearview AI responds to access requests by providing the requester with a .pdf file containing any images of the requester we were able to locate via our search engine, and a link to our Data Policy. We retain a record of the access request by noting the date it was processed and retaining an anonymized hash of the requester's email address.

13. Clearview's website includes a form which enables residents of the EU, UK and Australia to request to opt-out of Clearview search results. Please provide the following information:
 - a. The date on which this process was implemented.
 - b. The number of requests to opt out Clearview has received from UK residents.
 - c. Details of how Clearview responded to the requests to opt out, including whether UK residents were opted out by Clearview.
 - d. The number of requests to opt out Clearview has received from Australian residents.
 - e. Details of how Clearview responded to the requests to opt out, including whether Australian residents were opted out by Clearview.
 - f. Details of how Clearview ensures that the opt out process is effective and permanent. In particular, please provide details of how Clearview prevents its systems from re-collecting the same images of an individual who has opted out, and from collecting other images of that individual.
 - g. What information (e.g. name, email address, image vector, etc.) Clearview retains about an individual after the individual has opted out, and for how long each type of information is retained.

The first paragraph of our response to question 12 is repeated.

For persons who request deletion or opt-out, Clearview AI retains a vector of that person's image to block them from search results and prevent further collection of any



images of that person. This information must be retained permanently to ensure the effectiveness of the opt-out process. The image the individual shared with Clearview AI to facilitate their request to opt out is deleted, and their opt out request is recorded by noting the date and retaining an anonymized hash of the requester's email address.

14. It is noted in response to Q21 that 'The only affirmative marketing efforts engaged in by Clearview at present is to place advertisements on e-mailing lists for U.S. law enforcement personnel.' Have Clearview previously marketed their services outside of the United States? If so, please provide the following:

- a. The list of countries in which the services have been marketed.
- b. When and for how long these marketing campaigns lasted?
- c. If this list of countries includes the UK and/ or Australia, please provide full details of how the services were marketed.

Clearview AI has from time-to-time placed online advertisements or other advertisements on email lists that are primarily targeted at law enforcement and security personnel in the United States. While we are attempting to determine if there are any additional instances of marketing outside of the United States, an initial review of our records showed the following occasions where advertising emails were transmitted to persons outside the United States:

4 emails were sent to users of [Crimedex.com](https://www.crimedex.com):

- 07/08/19: went to users in USA and Canada
- 10/08/19: went to users in USA and to persons associated with the International Association of Financial Crime Investigators (IAFCI)
- 11/13/19: went to users in USA, Canada, UK, Australia and the IAFCI
- 05/28/20: went to users in USA and IAFCI

15. In response to Q23, Clearview explained that a test was 'performed by a panel of independent experts'. Please provide a copy of any report produced, including details of who comprised the panel.

Clearview AI's accuracy was evaluated by a panel consisting of:



- Judge Jonathan Lippman, who served as Chief Judge of the State of New York from 2009 to 2015, and served as former Chair of the Independent Commission on New York City Criminal Justice and Incarceration Reform
- Dr. Nicholas Cassimatis, who served as the Chief of Samsung's North American AI Research and holds a doctorate and undergraduate degrees from the Massachusetts Institute of Technology, and his masters degree from Stanford University.
- Aaron Renn, who served as Senior Fellow at the Manhattan Institute, a contributing editor of *City Journal*, and an economic development columnist for *Governing Magazine*. He also served as a partner at Accenture where he led the development and testing of multiple software systems for major corporations.

A copy of the report is attached below as Attachment B.

16. The CEO of Clearview recently advised CNN in an interview that ‘...what we do is we give the police agency or federal agency a free trial, maybe 30-60 days, and during their usage investigators solve a lot of cases and we work with them and figure out how they can go through and procure the product.’

- a. Please advise whether this statement accurately reflects the purpose for which Clearview provides free trials to law enforcement.
- b. In respect of the free trials, are the users encouraged to report to Clearview on the outcome of the trial or to provide endorsements of the service?

Our CEO’s statements are related to the use of the product in the US market. They should not be taken out of context. Obviously, the purpose of a free trial is to sell the product. Trial periods often are for 30-60 days, but could be shorter or longer based on specific requests of the test users. At the end of the trial period, users can submit feedback about their user experience via an email address or an in-app feedback form. Providing feedback is not a condition of the test user offering.

* * *

Clearview AI is happy to cooperate with your efforts to understand our technology and business operations to clear up whatever misconceptions about our product there are, and which permeate the online space. While we are open to continuing discussions, we believe it important to again stress that we do not believe that Clearview AI is subject to the jurisdictions of either the United Kingdom or Australia data protection authorities, and look forward to concluding this inquiry in a prompt manner.

Jack Mulcaire

Counsel, Clearview AI

s 47G

Confidential: This attachment constitutes a business secret which Clearview AI is contractually obligated to keep confidential.

Attachment A

S47G

Attachment B

CLEARVIEW AI

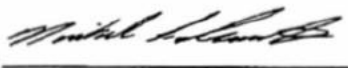
Accuracy Test Report

OCTOBER 2019

Conducted Independently By:



Hon. Jonathan Lippman



Nicholas Cassimatis, PhD



Aaron M. Renn



REPORT SUMMARY

In October 2019, the undersigned Panel conducted an independent accuracy test of Clearview AI, a new image-matching technology that functions as an Internet search engine for faces.

The test was undertaken in order to measure Clearview's performance in terms of accuracy across all demographic groups. For the purposes of this analysis, the Panel used the same basic methodology used by the American Civil Liberties Union (ACLU) in its July 2018 accuracy test of Amazon's Rekognition technology. The ACLU's approach entailed comparing photographs of all 535 members of the U.S. House of Representatives and Senate against a database of 25,000 arrest photos. The test resulted in 28 members of Congress being incorrectly matched to arrestees from the photo database.

It should be noted, however, that the ACLU ran its test using Rekognition's 80% 'default' confidence setting. (The program advises setting the confidence interval at 95% for law enforcement applications.) Even so, the test was highly publicized and might serve to give the general impression that facial recognition technology is inaccurate and/or biased.

With those important concerns in mind, the Panel conducted the same test of Clearview. Along with analyzing all 535 members of Congress, the Panel also analyzed all 119 members of the California State Legislature and 180 members of the Texas State Legislature, for good measure.

The test compared the headshots from all three legislative bodies against Clearview's proprietary database of 2.8 billion images (112,000 times the size of the database used by the ACLU). The Panel determined that Clearview rated **100% accurate**, producing instant and accurate matches for every one of the 834 federal and state legislators in the test cohort.

TEST CONCLUSION:

The Independent Review Panel determined that Clearview rated 100% accurate, producing instant and accurate matches for every photo image in the test. Accuracy was consistent across all racial & demographic groups.



WHAT IS CLEARVIEW AI?

Clearview is a facial-image-matching software system that operates as an Internet search engine for faces. Clearview has indexed the publicly available Internet to create a database of images containing approximately 2.8 billion faces.

With a traditional search engine, users search by typing in search terms. With Clearview, users search by uploading an image containing the face to be searched. If Clearview detects a face in the photo, it matches the face against the images in its database, returning any images containing a face that matches. (If the submitted image contains multiple faces, such as in a group photo, Clearview provides the user with a choice of which face to search for.) The matched face is displayed, along with the hyperlink to the website where the image was found. It is important to note that Clearview only matches faces in images. It does not attempt to determine any characteristics of the person such as sex, age, or race. It only searches for images from the Internet in its database with matching faces.

ACLU TEST

In 2018 the American Civil Liberties Union (ACLU) conducted a well-publicized test of Amazon's facial recognition software, Rekognition.¹ The ACLU used Rekognition to build a database of 25,000 arrest photos. The legal advocacy group then ran a search against that database using pictures of the members of Congress.

In the ACLU test, Rekognition incorrectly matched 28 members of Congress, three in the Senate and 25 in the House of Representatives — and “the false matchers were disproportionately people of color.” The ACLU used the default settings in Rekognition for the test. However, that tool's default confidence interval is only 80%. Amazon recommends setting the confidence interface to 95% for uses involving law enforcement and public safety use.

¹ <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-facerecognition-falsely-matched-28>



CLEARVIEW TEST

The Clearview test was designed and conducted along the same lines as the ACLU test in order to evaluate the accuracy of the Clearview system. To make the test more expansive, in addition to the 535 members of Congress, the test also conducted face searches for every member of the legislatures of the two largest states, California and Texas.

The final list included a total of 834 legislators:

- 100 US Senators
- 435 US House Members
- 79 California State Assembly Members (one seat was vacant)
- 40 California State Senators
- 149 Texas State House Members (one seat was vacant)
- 31 Texas State Senators

Also, instead of searching only 25,000 images, the test searched Clearview's entire database of 2.8 billion. Unlike Amazon's Rekognition, Clearview does not allow the user to set the confidence level, but instead is fixed at 99.6%. Publicly available images of the legislators were processed through Clearview automatically using the Clearview Application Programming Interface (API). Use of the API, versus manual entry, ensured reproducibility and limited the possibility of human error.

For each individual in the test, the two top-ranked matches returned from Clearview's 2.8 billion image database were compared with the submitted image. Results were reviewed by the three members of the Panel for their determination as to whether the matches were accurate.

The evaluation of the accuracy of each match was determined visually and/or by review of the webpage from which the matched photo was originally taken. In some cases, the originating site is no longer available or no longer contains the image. And in some cases, a cached version of the file was used for comparison. No incorrect matches were found. All returned photos contained the person whose photo was originally submitted.

Note: In the case of one member of the Texas State House of Representatives, one member's photo did return matches that included arrest photos. That is because the individual had, in fact, been arrested.



PANEL BIOGRAPHIES

The Honorable Jonathan Lippman

Judge Lippman served as Chief Judge of the State of New York from 2009 to 2015. During his tenure, Chief Judge Lippman authored landmark decisions addressing constitutional, statutory and common law issues that reshaped the major aspects of New York law and the contours of NY State government. In the process, he promoted equal access to justice in New York and around the country, and established permanent funding streams for civil legal services. His work included:

- Making New York the first state in the nation to require 50 hours of law-related pro bono work prior to bar admission and established the Pro Bono Scholars and Poverty Justice Solutions Programs to help alleviate the crisis in civil legal services
- Strengthening the State's indigent criminal defense system
- Addressing the systemic causes of wrongful convictions
- Creating Human Trafficking Courts across New York State
- Reforming New York's juvenile justice, bail and pre-trial justice systems

Judge Lippman received the 2018 William H. Rehnquist Award for Judicial Excellence and the 2016 American Bar Association's John Marshall Award for judicial excellence, integrity, fairness and professional ethics.

The New York Times said Judge Lippman altered the legal profession in New York by using "his authority to promote an ideal of lawyering as a public service." As Chair of the Independent Commission on New York City Criminal Justice and Incarceration Reform, Judge Lippman drafted the blueprint for the closing of the Rikers Island Jail and the conversion of the City's troubled jail system to a network of community-based facilities.

Dr. Nicholas Cassimatis, Ph.D.

Dr. Cassimatis has worked in Artificial Intelligence (AI) his entire career. He is currently the founder of Unitary Labs, a startup that makes software thousands of times faster to build. Previously, he served as the Chief of Samsung's North American AI Research. He was the founder of SkyPhrase, which created a technology that understood more complex natural language with greater precision than had ever before been previously possible. In 2013, SkyPhrase was acquired by Yahoo, where he was the head of the Deep Natural Language Processing team.



Dr. Cassimatis founded SkyPhrase while he was on the faculty of the Cognitive Science and Computer Science Departments at the Rensselaer Polytechnic Institute. While there, he founded the Human-Level Intelligence Laboratory and led its research into learning, cognitive architectures, reasoning, knowledge representation, and computational linguistics. He was a National Research Council Postdoctoral Associate at the Naval Research Laboratory, where he conducted research in robotics and cognitive architecture.

Dr. Cassimatis received his doctorate and undergraduate degrees from the Massachusetts Institute of Technology, and his masters degree from Stanford University.

Aaron M. Renn

Aaron Renn is a Senior Fellow at the Manhattan Institute, a contributing editor of *City Journal*, and an economic development columnist for *Governing Magazine*. He focuses on ways to help America's cities thrive in an ever-more complex, competitive, globalized, and diverse twenty-first century. During Renn's 15-year career in management and technology consulting, he served as a partner at Accenture, where he led the development and testing of multiple software systems for major corporations and directed multimillion-dollar, global-technology implementations. He also developed his own online software company, Telestrian, which provided urban data analytics and mapping.

He has contributed to *The Guardian*, Forbes.com, and numerous other publications. His perspectives on urban issues are regularly cited in the *New York Times*, *Washington Post*, *Time*, *The Economist*, *Daily Telegraph*, and other international media.

Renn holds a B.S. from Indiana University, where he coauthored an early socialnetworking platform in 1991. He has created several widely used, open-source software packages, including the only program for recovering data from corrupted gzip backups. In 1998, Renn launched one of the nation's first blogs, the Weekly Breakdown, to cover the Chicago Transit Authority.

###

From: [Sophie Higgins](#)
To: [Carla Wolnizer](#)
Subject: Fwd: Acknowledgement from the ICO and OAIC
Date: Tuesday, 29 September 2020 10:13:54 PM

Get [Outlook for iOS](#)

From: Ciara Hagan <s 47F [REDACTED]>
Sent: Tuesday, September 29, 2020 9:55 pm
To: Jack M
Cc: David Reynolds; Sophie Higgins; Justin Lodge
Subject: Acknowledgement from the ICO and OAIC

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Dear Jack Mulcaire,

Thank you for your email of 25 September 2020 and the response you have provided to our enquiries. This email is to confirm that we will review the information supplied and respond in due course.

Yours sincerely,

Ciara Hagan
Lead Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

T. s 47F [REDACTED] F. 01625 524510 ico.org.uk twitter.com/iconews

Please consider the environment before printing this email

For information about what to do with personal data see our [privacy notice](#)

From: Jack M s 47G [REDACTED]
Sent: 25 September 2020 18:05
To: Ciara Hagan <s 47F [REDACTED]> David Reynolds <s 47F [REDACTED]> Sophie Higgins <sophie.higgins@oaic.gov.au>; Justin Lodge <justin.lodge@oaic.gov.au>
Subject: Response to Inquiries of 11 September 2020

External: This email originated outside the ICO.

Dear Information Commissioner's Office and Office of the Australian Information Commissioner,

Please see the attached .pdf document which contains our response to your most recent letter.

Regards,

Jack Mulcaire

Counsel, Clearview AI

s 47G

s 22(a)(ii)

From: Ciara Hagan <s 47F [REDACTED]>
Sent: Monday, October 19, 2020 8:38 PM
To: s 47G [REDACTED]
Cc: mark.love@ballawyers.com.au; David Reynolds <s 47F [REDACTED]> Sophie Higgins <sophie.higgins@oaic.gov.au>; Justin Lodge <justin.lodge@oaic.gov.au>
Subject: Correspondence from the ICO and OAIC

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Dear Jack Mulcaire,

Please find attached further enquiries regarding the joint investigation conducted by the Information Commissioner's Office and the Office of the Australian Information Commissioner into Clearview AI Inc.

Yours sincerely,



Ciara Hagan
Lead Case Officer – Civil Investigations
Regulatory Supervision Service

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

T. s 47F [REDACTED] F. 01625 524510 ico.org.uk

twitter.com/iconews

Please consider the environment before printing this email
For information about what we do with personal data see our [privacy notice](#)



David Reynolds
Lead Case Officer, Civil Investigations
Regulatory Supervision Service

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

T. s 47F [REDACTED] F. 01625 524510 ico.org.uk

twitter.com/iconews

Please consider the environment before printing this email
For information about what we do with personal data see

| our [privacy notice](#)



Sophie Higgins | Director
Dispute Resolution Branch
Office of the Australian Information Commissioner
GPO Box 5218 Sydney NSW 2001 | oaic.gov.au
02 9284 9775 | sophie.higgins@oaic.gov.au



 [Subscribe to Information Matters](#)

O A I C logo



Justin Lodge | A/g Director
Dispute Resolution Branch
Office of the Australian Information Commissioner
GPO Box 5218 Sydney NSW 2001 | oaic.gov.au
+61 2 8231 4203 | Justin.Lodge@oaic.gov.au



 [Subscribe to OAICnet newsletter](#)

FOIREQ23/00215 -78-

From: [Sophie Higgins](#)
To: [Carla Wolnizer](#)
Subject: FW: Correspondence from the ICO and OAIC [SEC=OFFICIAL]
Date: Tuesday, 3 November 2020 10:24:30 AM
Attachments: [November 2 2020 Response to ICO and OAIC.pdf](#)

From: Jack Mulcaire <s 47G>
Sent: Tuesday, November 3, 2020 9:40 AM
To: Ciara Hagan <s 47F>
Cc: David Reynolds <s 47F> Sophie Higgins <sophie.higgins@oaic.gov.au>; Justin Lodge <justin.lodge@oaic.gov.au>
Subject: Re: Correspondence from the ICO and OAIC

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Hello Ms. Hagan,

Please see the attached letter responding to your inquiries.

Regards,
Jack Mulcaire
Counsel, Clearview AI
<s 47G>



Information Commissioner's Office
Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Via Email

Dear Ms. Hagan, Mr. Reynolds, Mr. Lodge and Ms. Higgins,

We refer to your letter of October 19, 2020.

Jurisdictional basis for your inquiries

Your offices have yet to provide a clear basis for asserting jurisdiction over Clearview AI, and as we have repeatedly indicated, we believe there is none.

s 33



Australia/OAIC

In relation to Australia, we again fail to understand the jurisdictional basis for the OAIC's inquiries. You have not explained what it is about Clearview AI's process of using images on the open web, which causes that data to be information of the kind over which the OAIC has jurisdiction. Similarly, you have not identified any basis under which Clearview AI ought to be considered an APP. Finally, given that no business or activity is conducted within an Australian jurisdiction, you have not explained why Clearview AI would be subject to OAIC jurisdiction.



Unless the ICO and OAIC can provide a proper statutory basis for jurisdiction, we respectfully repeat that Clearview AI is not subject to oversight by your offices. Clearview AI was founded in, is based in, and conducts its business in the United States of America.

Despite neither the ICO nor the OAIC providing information regarding the statutory basis for their inquiries, Clearview AI has cooperated with your inquiries, and has voluntarily provided information since we first were contacted by your agencies in February 2020. While we have provided responses to your 19 October inquiries below, we do not anticipate providing additional information unless and until your offices can articulate (a) a legal basis on which they purport to have jurisdiction over Clearview AI, (b) the authority pursuant to which they are conducting these inquiries and (c) a timeline for completion of your inquiries. At this juncture, we believe that we must place on record that this continued questioning is unwarranted and without basis. Providing continued responses to questions posed without any articulated jurisdictional basis or anticipated completion date is costly and time-consuming for Clearview AI.

The answers provided below are provided on an entirely voluntary basis and without prejudice to our position that neither the ICO nor the OAIC has jurisdiction over Clearview AI.

1. What date(s) did Clearview undertake action to block United Kingdom (UK) and Australian IP addresses.

s 47G

A large black rectangular redaction box covering several lines of text.

2. In your previous response (received on 25 September 2020), you advised that Clearview cannot exclude the possibility of UK or Australian residents being



captured in any scraping of personal data from sites that are not clearly domiciled in or otherwise associated with these territories, please expand on this point, in order for us to gain an detailed understanding. From the information you have provided, as an example, are Clearview explaining it would not be possible to block the photograph of a UK data subject if their image originated from an IP address of a country which is not on Clearview's blocked IP list?

Clearview AI only collects publicly available Internet images, along with their metadata and the webpage URLs where those images appear. This data does not enable Clearview AI to determine the nationality of persons in the collected images. Clearview AI is not aware of any legal basis that would require it to refrain from collecting images from web pages associated with United Kingdom or Australian IP addresses.

3. In response to Question 1, you stated: s 47G [REDACTED]
[REDACTED]
[REDACTED]. Please advise if Clearview AI has also made a decision to not operate in Australia, and if so, provide the date from which that decision became effective.

Clearview AI has also decided it will not operate in Australia. That decision was made in March 2020.

4. In response to Question 7, you advise that Clearview provides “more rights and disclosures to data subjects (via Clearview’s privacy policy) than Clearview are required to. Which rights do Clearview provide to individuals that they are not required to? Please provide a detailed response.

As outlined in our previous letter, Clearview AI enables residents of the United Kingdom and Australia to submit requests for data access, deletion, opt-out, rectification and portability on a voluntary basis.



5. In a court document, Clearview AI stated that it § 47G [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] Please confirm if this is correct.

We have nothing further to add. This document was produced in relation to ongoing legal proceedings, and speaks for itself.

6. In response to Question 9, you stated: “Clearview AI’s proprietary algorithm takes images and measures certain characteristics of an individual’s face”. Please:
- Advise how many characteristics of an individual’s face the algorithm measures.
 - Explain how these are measured.
 - Confirm whether a template or other geometric representation is created based on the characteristics of an individual’s face.

Clearview AI’s technology is proprietary and its operations constitute a confidential trade secret. We are not able to provide further information, particularly in circumstances where we do not believe there is a jurisdictional basis for your inquiries.

7. Please provide further information regarding the retention of individuals’ information who have opted out of Clearview’s services. Is Clearview’s retention period reviewed periodically? If so, please provide further detail.

We do not understand the premise of this question. For opt-out requests to be effective, an image vector must be retained for an indefinite period by Clearview AI so that the image or similar images can be excluded from future searches. Vectors retained for this purpose are not associated with the original image, which is deleted, or any other identifying information. The vectors are only accessible to Clearview AI employees who are responsible for maintaining Clearview’s web application infrastructure. If Clearview



AI were to change its retention practices with respect to these vectors, Clearview AI would only be able to honor the requested opt-out for a limited period of time, which would defeat the nature of the request in the first instance.

8. In response to Question 13, you stated: “For persons who request deletion or opt-out Clearview AI retains a vector of that person’s image the block them from search results and prevent further collection of any images of that person. This information must be retained permanently to ensure the effectiveness of the opt-out process”. Please:
 - a. Explain the difference between deletion and opt-out.
 - b. Advise whether and how Clearview AI notifies individuals about the consequences of requesting deletion or opt-out, including that Clearview AI will retain a vector of their facial image permanently.
 - c. Explain how Clearview AI ensures that its deletion and opt-out requests are effective and permanent (without referring to particular requests from the UK or Australia). In particular, explain how Clearview uses the vector of an individual requesting deletion or opt-out to prevent its system from re-collecting the same images of that individual and from collecting other images of that individual.

Functionally, Clearview AI treats opt-out and deletion requests in the same way. The webform that UK and Australia residents can use to request deletion/opt-out states that, “When we are done processing your request, the photo of yourself you shared to facilitate the request is de-identified”. This is indeed the case--the retained vector is merely a string of numbers, the image used to generate it is subsequently deleted, and the retained vector is not tied to any other identifying information.

s 33



s 33

10. Reference has been made to 'licensed users' in your response to question 5. Please explain how Clearview recognizes an individual or organisation as a licensed user? For example, do they have to meet a set of criteria or hold a contractual agreement with Clearview to use the service?

"Licensed users" refers to users who have an account with Clearview AI, paid for by the organization for which they work. The account is linked to a registered email address associated with a government agency domain, and users must log into Clearview AI's service in order to access any of its features. Users are required to use a strong password. Licensed users can only access Clearview AI's service pursuant to a contract with Clearview AI, which contractually requires oversight over individual users' search activity by a supervisor at their law enforcement organization and agreement to the Terms of Service and Code of Conduct.

* * *

We trust that this letter answers your outstanding queries and that this line of correspondence is at an end. If that is not correct, before Clearview AI considers responding to any additional inquiries from your offices, please provide by return the requested information concerning the jurisdictional basis for your inquiries and a timeline for their completion.

Regards,

Jack Mulcaire
Counsel, Clearview AI

s 47G

From: [Sophie Higgins](#)
To: [Carla Wolnizer](#)
Subject: FW: Acknowledgement from the ICO and OAIC [SEC=OFFICIAL]
Date: Wednesday, 4 November 2020 10:41:19 AM

From: Ciara Hagan <[s 47F](#)>
Sent: Wednesday, November 4, 2020 4:34 AM
To: Jack M <[s 47G](#)>
Cc: David Reynolds <[s 47F](#)> Sophie Higgins <sophie.higgins@oaic.gov.au>; Justin Lodge <justin.lodge@oaic.gov.au>
Subject: Acknowledgement from the ICO and OAIC

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Dear Jack Mulcaire,

Thank you for providing response to our enquiries. We will review the information supplied and respond in due course.

Yours sincerely,

Ciara Hagan

Lead Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

[s 47F](#) F. 01625 524510 ico.org.uk twitter.com/iconews

Please consider the environment before printing this email

For information about what to do with personal data see our [privacy notice](#)

From: Jack M <[s 47G](#)>
Sent: 02 November 2020 22:40
To: Ciara Hagan <[s 47F](#)>
Cc: David Reynolds <[s 47F](#)> Sophie Higgins <sophie.higgins@oaic.gov.au>; Justin Lodge <justin.lodge@oaic.gov.au>
Subject: Re: Correspondence from the ICO and OAIC

External: This email originated outside the ICO.

Hello Ms. Hagan,

Please see the attached letter responding to your inquiries.

Regards,
Jack Mulcaire
Counsel, Clearview AI

[s 47G](#)

From: [Sophie Higgins](#)
To: s 47G
Cc: [Justin Lodge](#); [David Reynolds](#)
Subject: Correspondence from the UK ICO and OAIC [SEC=OFFICIAL]
Date: Thursday, 20 May 2021 12:26:00 PM
Attachments: [image001.jpg](#)
[image002.png](#)
[image003.png](#)
[image004.png](#)
[image005.png](#)
[OAIC ICO joint letter to Clearview 20 May 2021.pdf](#)
[Clearview - Joint statement of facts.pdf](#)

Dear Jack Mulcaire,

I refer to the joint investigation by the UK Information Commissioner's Office and the Office of the Australian Information Commissioner into the acts or practices of Clearview AI Inc.

Please find attached a letter regarding the matter.

Yours sincerely,



Sophie Higgins | Director
Dispute Resolution Branch
Office of the Australian Information Commissioner
GPO Box 5218 Sydney NSW 2001 | oaic.gov.au
02 9284 9775 | sophie.higgins@oaic.gov.au



[Subscribe to Information Matters](#)



Justin Lodge | A/g Director
Dispute Resolution Branch
Office of the Australian Information Commissioner
GPO Box 5218 Sydney NSW 2001 | oaic.gov.au
+61 2 8231 4203 | Justin.Lodge@oaic.gov.au



[Subscribe to OAICnet newsletter](#)

David Reynolds
Lead Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

s 47F F. 01625 524510 ico.org.uk twitter.com/iconews

Please consider the environment before printing this email

For information about what to do with personal data see our [privacy notice](#)

Joint statement of facts

1. Clearview AI (the respondent) provides a facial recognition search tool (the **Facial Recognition Tool**) for registered users. This is available through a mobile application and a website.
2. The Facial Recognition Tool allows clients to upload a digital image of an individual's face and run a search against it. The Tool then applies its algorithm to the digital image and runs the result against the respondent's database, which contains more than 3 billion images¹, to identify and display likely matches and associated source information.
3. To populate its database, the Facial Recognition 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 URL of the webpage from which the Scraped Image was sourced,² and any associated metadata that was not stripped by the source website³ (including the webpage title).⁴ These are all collected by automated means. As the images are scraped from the internet, the respondent submits that it cannot determine the nationality of individuals depicted in the images.
4. The Facial Recognition Tool then generates a mathematical representation of the Scraped Image (**Scraped Image Vector**) using a machine-learning algorithm⁵ to measure certain characteristics of an individual's face.⁶ Scraped Image Vectors are stored along with Scraped Images (and URLs and metadata), in the respondent's database.
5. When a registered user wishes to identify an individual using the Facial Recognition Tool, they upload that individual's image through the app or website (the **Probe Image**). The Facial Recognition Tool then analyses the image and generates a mathematical representation of the Probe Image (the **Probe Image Vector**). The Probe Image Vector is compared against all of the Scraped Image Vectors stored in its database, which in turn are linked back to any Scraped Images that appear to show the same individual.
6. Once sufficiently similar Scraped Images are identified, these **Matched Images** are displayed alongside the Probe Image on the user's screen as 'search results.'⁷ The images are displayed in the form of a thumbnail image/s and a link or links to the URL location where that image appears online. 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.
7. The respondent submits that it currently offers its service to law enforcement only. It markets its product as helping law enforcement agencies 'identify perpetrators and victims of crime'.⁸ Notwithstanding this, in its US patent application filed on 7 August 2020, the respondent describes ways to apply its facial recognition software to the private sector as well as to law enforcement and social work, where it says it could be used to possibly identify people who use

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

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 Letter from the respondent to the ICO dated 4 August 2020 (**respondent's response dated 4 August 2020**), p 3.

⁵ Respondent's response dated 4 August 2020, p 2.

⁶ Letter from the respondent to the ICO and OAIC dated 25 September 2020 (**respondent's response of 25 September 2020**).

⁷ Respondent's response dated 25 September 2020.

⁸ Respondent's website: <https://clearview.ai/>

drugs or people experiencing homelessness.⁹ The respondent has also filed an international patent application that contains the same title and description. Both the US and international patent applications follow on from a provisional patent application filed on 9 August 2019.¹⁰

8. From October 2019 to March 2020, the respondent offered free trials to four Australian police services. Members from each of these Police services used the Facial Recognition Tool on a free trial basis.¹¹ This involved police members uploading 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.

9. s 33

10. From 29 January 2020, the respondent began to offer Australian and UK residents an online form to opt out of the respondent's search results. To make such a request, individuals must submit a valid email address and a facial image, and the respondent then generates a mathematical representation of the submitted image (the **Opt-out Image Vector**). The Opt-out Image Vector is retained permanently.¹²

11. The respondent searches for the Opt-out Image Vector against the Scraped Image Vectors, to identify any sufficiently similar Scraped Images. The respondent will block images of that individual from appearing in future search results, and will prevent further collection of Scraped Images of that individual.

12. As at the date of this letter, the online form for opt-out described above does not appear to be available. There does not appear to be another opt-out mechanism available to Australian or UK residents.

13. s 47E(d)

14. The respondent submitted that by the end of March 2020, it had terminated all of its trial users in Australia and the UK and had instituted a policy of refusing all requests for accounts from those countries.¹⁵ The respondent also submitted that in September 2020, it blocked access to its website and mobile application for Australian and UK IP addresses.¹⁶

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.

¹⁰ World Intellectual 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>

¹¹ Respondent's response dated 25 February 2020; Respondent's response dated 19 August 2020, p 2.

¹² Respondent's response dated 25 September 2020, pp 9-10.

¹³ Respondent's website, De Index request: <https://clearview.ai/privacy/deindex>

¹⁴ Ibid.

¹⁵ Letter from the respondent to the ICO and OAIC dated 2 November 2020 (**respondent's response dated 2 November 2020**).

¹⁶ Respondent's response dated 2 November 2020.

15. However, as at the date of this letter, the respondent's website, its form for requesting access to the Facial Recognition Tool and its 'Sign In' form remain accessible to Australian and UK IP addresses. The respondent has not taken any steps (other than the opt-out mechanism), to stop collecting Scraped Images of Australians or UK residents, generating facial vectors from those images, and disclosing any Australians and UK residents in Matched Images to its registered users.

From: [Justin Lodge](#)
To: [Sophie Higgins](#); [Wendy Tian](#); [Emi Christensen](#)
Subject: FW: Correspondence from the UK ICO and OAIC [SEC=OFFICIAL]
Date: Friday, 21 May 2021 2:59:01 PM
Attachments: [image001.jpg](#)
[image002.png](#)
[image003.png](#)
[image004.png](#)
[image005.png](#)
s 47G, s47E(d), s 47B

fyi

From: Justin Lodge
Sent: Friday, 21 May 2021 2:58 PM
To: Jack M [s 47G](#)
Subject: FW: Correspondence from the UK ICO and OAIC [SEC=OFFICIAL]

Dear Jack Mulcaire,

I refer to the letter dated 20 May 2021 regarding the joint investigation by the UK Information Commissioner's Office and the Office of the Australian Information Commissioner (OAIC) into the acts or practices of Clearview AI Inc.

That letter noted that the OAIC will contact you separately regarding next steps in its investigation. Please find attached a letter from the OAIC about next steps in the investigation, as well as the OAIC's preliminary view, and attachments.

If you have any questions, please feel free to contact us.

Yours sincerely,



Justin Lodge | Assistant Director
Dispute Resolution Branch
Office of the Australian Information Commissioner
GPO Box 5218 Sydney NSW 2001 | oaic.gov.au
+61 2 8231 4203 | Justin.Lodge@oaic.gov.au

| | | [Subscribe to OAICnet newsletter](#)

From: Sophie Higgins <sophie.higgins@oaic.gov.au>
Sent: Thursday, 20 May 2021 12:27 PM
To: [s 47G](#)
Cc: Justin Lodge <justin.lodge@oaic.gov.au>; David Reynolds <[s 47F](#)>
Subject: Correspondence from the UK ICO and OAIC [SEC=OFFICIAL]

Dear Jack Mulcaire,

I refer to the joint investigation by the UK Information Commissioner's Office and the Office of the Australian Information Commissioner into the acts or practices of Clearview AI Inc.

Please find attached a letter regarding the matter.

Yours sincerely,



Sophie Higgins | Director
Dispute Resolution Branch
Office of the Australian Information Commissioner
GPO Box 5218 Sydney NSW 2001 | oaic.gov.au
02 9284 9775 | sophie.higgins@oaic.gov.au



 [Subscribe to Information Matters](#)



Justin Lodge | A/g Director
Dispute Resolution Branch
Office of the Australian Information Commissioner
GPO Box 5218 Sydney NSW 2001 | oaic.gov.au
+61 2 8231 4203 | Justin.Lodge@oaic.gov.au



 [Subscribe to OAICnet newsletter](#)

David Reynolds
Lead Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

T. **s 47F** | F. 01625 524510 | ico.org.uk | twitter.com/iconews

Please consider the environment before printing this email

For information about what to do with personal data see our [privacy notice](#)



Our reference: CII20/00006

Clearview AI Inc.
214 W 29th St, 2nd floor
New York City, NY, 10001

By email: **s47G**

Commissioner Initiated Investigation into Clearview AI Inc

Dear Jack Mulcaire,

I refer to the investigation opened by the Australian Information Commissioner on 4 March 2020 under s 40(2) of the *Privacy Act 1988* (Cth) into the acts and practices of Clearview AI Inc (the Investigation). I also refer to the correspondence from the UK Information Commissioner's Office (ICO) and the Office of the Australian Information Commissioner (OAIC) dated 7 July 2020 informing you that the investigation would be undertaken jointly.

As stated in the joint correspondence from the UK ICO and the OAIC dated 20 May 2021, the joint evidence gathering is now concluded, and the OAIC and ICO will correspond with you separately.

Based on the information received to date in connection with the Investigation, I am minded to recommend that the Commissioner make a determination in this matter.

The Commissioner may make a determination under s 52(1A) of the Privacy Act, that includes one or more of a number of prescribed matters, including:

- a. a declaration that the relevant act or practice is an interference with the privacy of one or more individuals and that the relevant entity must not repeat or continue the act or practice; and
- b. a declaration that the relevant entity must take specified steps within a specified period to ensure that the act or practice is not repeated or continued.

The Commissioner will decide whether it is appropriate to make a determination on completion of the Investigation, having regard to the Privacy Act and both the OAIC's Guide to Privacy Regulatory Action (available here: <https://oaic.gov.au/assets/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action.pdf>) and the OAIC's

Privacy Regulatory Action Policy (available here: <https://oaic.gov.au/assets/about-us/our-regulatory-approach/privacy-regulatory-action-policy.pdf>).

If the Commissioner does make a determination in relation to this matter, the determination will be published on the OAIC's website and on the AustLII website.

Under s 55A of the Privacy Act, the Commissioner may commence proceedings in the Federal Court of Australia or the Federal Circuit Court of Australia for an order to enforce any determination that she makes on completion of the Investigation.

Preliminary view

Please find enclosed, at **Attachment A**, my preliminary view in this Investigation. A preliminary view sets out my preliminary findings and reasons, and the recommendations I intend to make to the Commissioner. It is not a final decision and may change upon consideration of submissions and additional information.

Clearview is invited to provide any comments on the preliminary view by **11 June 2021**. Any such comments will be considered in finalising the Investigation.

In addition, if Clearview intends to claim that any information in the preliminary view and/or Clearview's response to the preliminary view is confidential, please provide the following information by **11 June 2021**:

- identify the claimed confidential information with specificity (including the relevant paragraph, information asserted to be confidential, and title of the source document, if applicable); and
- explain why the information specified is confidential.

Information provided by third parties

It is the OAIC's usual practice to invite comments from respondents on all information that is credible, relevant, adverse and significant to their case.

Accordingly, I enclose and invite any comments on the following information gathered from third parties in this Investigation:

- Letter from the AFP to the OAIC dated 21 April 2020 (redacted version)
- Letter from the AFP to the OAIC dated 22 May 2020
- Letter from the AFP to the OAIC dated 19 March 2021

- Letter from the Queensland Police Service to the OAIC dated 7 August 2020 (redacted version)
- Letter from Queensland Police Service to the OAIC dated 26 February 2021
- Email from Victoria Police to the OAIC, 29 June 2020, Attachment titled “1. Combined”
- Victoria Police Issue Cover Sheet on the use of Clearview (undated) (redacted version)
- Letter from South Australia Police to the OAIC dated 14 July 2020
- Letter from Twitter to the OAIC dated 9 November 2020 (redacted version)
- Letter from LinkedIn to the ICO and OAIC dated 6 November (redacted version)

Please also provide any comments on the above documents by **11 June 2021**.

Please contact Sophie Higgins on (02) 9284 9775 or sophie.higgins@oaic.gov.au should you wish to discuss.

Yours sincerely



Elizabeth Hampton
Deputy Commissioner

21 May 2021



Commissioner initiated investigation into Clearview AI - CII20/00006

Preliminary view

21 May 2021

1. This is a preliminary view in relation to the Commissioner initiated investigation into Clearview AI Inc (the **respondent**), commenced under s 40(2) of the *Privacy Act 1988* (Cth) (the **Privacy Act**).
2. I intend to recommend that the Australian Information Commissioner (the **Commissioner**) make a declaration that the Respondent has:
 - a. failed to comply with the requirement in Australian Privacy Principle (**APP**) 1.2 in Schedule 1 of the *Privacy Act*, to take reasonable steps to implement practices, procedures and systems relating to the entity's functions or activities, to ensure compliance with the APPs.
 - b. interfered with the privacy of individuals by failing to comply with the requirement:
 - i. to collect sensitive information about an individual only where the individual consents to the collection (and the information is reasonably necessary for one or more of the entity's functions or activities), or an exception applies (APP 3.3)
 - ii. to collect personal information only by lawful and fair means (APP 3.5)
 - iii. to take such steps (if any) as are reasonable in the circumstances to notify individuals of the collection of personal information (APP 5)
 - iv. to 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 (APP 10.2).
3. The reasons for my preliminary view are outlined below.
4. The respondent now has an opportunity to comment on my preliminary view before the Commissioner considers this matter.

Background

5. The respondent provides a facial recognition search tool (the **Facial Recognition Tool**) for registered users. This is available through a mobile application and a website.
6. The Facial Recognition Tool allows clients to upload a digital image of an individual's face and run a search against it. The Tool then applies its algorithm to the digital image and runs the result against the respondent's database, which contains more than 3 billion images,¹ to identify and display likely matches and associated source information.
7. To populate its database, the Facial Recognition 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 URL of the webpage from which the Scraped Image was sourced,² and any associated metadata that was not stripped by the source website³ (including the webpage title).⁴ These are all collected by automated means. As the images are scraped from the internet, the respondent submits that it cannot determine the nationality of individuals depicted in the images.
8. The Facial Recognition Tool then generates a mathematical representation of the Scraped Image (**Scraped Image Vector**) using a machine-learning algorithm⁵ to measure certain characteristics of an individual's face.⁶ Scraped Image Vectors are stored, along with Scraped Images (and URLs and metadata), in the respondent's database.
9. When a registered user wishes to identify an individual using the Facial Recognition Tool, they upload that individual's image through the app or website (the **Probe Image**). The Facial Recognition Tool then analyses the image and generates a mathematical representation of the Probe Image (the **Probe Image Vector**). The Probe Image Vector is compared against all of the Scraped Image Vectors stored in the Database, which in turn are linked back to any Scraped Images that appear to show the same individual.
10. Once sufficiently similar Scraped Images are identified, these **Matched Images** are displayed alongside the Probe Image on the user's screen as 'search results'.⁷ Each Matched Images is displayed in the form of a thumbnail image and a link to the URL location where that image appears online. 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.
11. The respondent submits that it currently offers its service to law enforcement only. It markets its product as helping law enforcement agencies to 'quickly, accurately, and efficiently identify suspects, persons of interest and victims of crime'.⁸ Notwithstanding

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

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 Letter from the respondent to the ICO dated 4 August 2020 (**respondent's response dated 4 August 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 of 26 September 2020**).

⁷ Respondent's response dated 26 September 2020 p 4.

⁸ Respondent's website: <https://clearview.ai/>

this, in its US and international patent applications filed on 7 August 2020, the respondent describes ways to apply its facial recognition software to the private sector, including:

- a. to learn more about a person the user has just met, such as through business, dating, or other relationship
 - b. to verify personal identification for the purpose of granting or denying access for a person, a facility, a venue, or a device
 - c. by a public agency to accurately dispense social benefits and reduce fraud.⁹
12. 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. 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
13. From 29 January 2020, the respondent began to offer Australian residents an online form to opt out of the respondent's search results. To make such a request, individuals must submit a valid email address and a facial image, and the respondent then generates a mathematical representation of the submitted image (the **Opt-out Vector**). The Opt-out Vector is retained permanently (see below at paragraph 108).¹²
14. The respondent searches for the Opt-out Vector against the Scraped Image Vectors, to identify any sufficiently similar Scraped Images. The respondent will block images of that individual from appearing in future search results, and will prevent further collection of Scraped Images of that individual.¹³
15. To make such a request, an individual could:
- Click on a hyperlink on the respondent's homepage, 'Privacy Request Forms'
 - Click on a hyperlink, 'Data Deletion Request Form' (under the heading, 'For Residents of the EU, UK, Switzerland, and Australia'). This page is titled 'EU/UK/Switzerland/Australia Opt-Out' and states that it 'is designed to enable members of the public to request to opt-out of Clearview search results'.¹⁴
 - Click 'Start'. When completing the Request Form, individuals must submit a valid email address and a facial image.

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

¹³ Ibid.

¹⁴ <https://clearview.ai/privacy/requests>. Accessed on 1 February 2021.

16. Screenshots of the above process are at **Attachment C**.

17. As at the date of this preliminary view, the online form for Australians to opt-out described in paragraphs 13 to 16 does not appear to be available. There does not appear to be another opt-out mechanism available to Australians.

18. s 47E(d)

19. The respondent submits 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.¹⁶ The respondent also submits that in September 2020, it blocked access to its website and mobile application for Australian IP addresses.¹⁷

20. However, as at the date of this preliminary view, the respondent's website, its form for requesting access to the Facial Recognition Tool and its 'Sign In' form remain accessible to Australian IP addresses. The respondent has not taken any steps (other than the opt-out mechanism which no longer appears to be available to Australians), to stop collecting Scraped Images of Australians, generating facial vectors from those images, and disclosing any Australians in Matched Images to its registered users.

Investigation by the OAIC

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

22. On 4 March 2020, the Commissioner notified Clearview AI that she had commenced an investigation under subsection 40(2) of the Privacy Act.

23. The Commissioner noted she 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.

24. 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 their intention to jointly investigate the respondent's data processing practices.

25. The joint letter set out that:

- It is the Australian Information Commissioner's intention to continue its investigation, commenced on 4 March 2020, through a joint investigation with the ICO.
- 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 jointly with the ICO.¹⁸

¹⁵ Respondent's website, De Index request: <https://clearview.ai/privacy/deindex>.

¹⁶ Letter from the respondent to the ICO and OAIC dated 2 November 2020 (**respondent's response dated 2 November 2020**).

¹⁷ Respondent's response dated 2 November 2020.

¹⁸ 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

- 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.¹⁹
- 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.

The Law

26. All references to provisions in this preliminary view are to those contained in the Privacy Act except where indicated.

27. 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**).

28. 'Personal information' means:

'information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- Whether the information or opinion is true or not; and
- Whether the information or opinion is recorded in a material form or not.²⁰

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

30. The APPs relevant to the Commissioner's investigation are:

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

31. In her letter of 4 March 2020, the Commissioner notified the respondent that she would also be investigating the respondent's compliance with APPs 3.2, 3.6, 6, 8 and 11. At this stage, I have not made preliminary findings in relation to these APPs.

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

the purposes of joint investigations, available at: <https://www.oaic.gov.au/about-us/our-corporate-information/memorandums-of-understanding/mous/mou-with-ico/>.

¹⁹ 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/>

²⁰ s 6(1) of the Privacy Act.

33. 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;
- a declaration that it would be inappropriate for any further action to be taken in the matter.

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

Material considered

35. The relevant documents before me are set out in **Attachment B**.

36. I have also considered the *Australian Privacy Principles Guidelines*, February 2014 issued by the Australian Information Commissioner (**APP Guidelines**)²¹, the OAIC's *Privacy Regulatory Action Policy*²² and the OAIC's *Guide to Privacy Regulatory Action*, July 2020.²³

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

Australian link

Law and policy

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

39. 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'.

40. As the respondent is incorporated in the State of Delaware in the United States,²⁴ for the Respondent to have an "Australian link", the following conditions in s 5B(3) of the Privacy Act must apply:

- the organisation carries on business in Australia

²¹ As at July 2019. Available online at: <https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/>

²² Available online at: <https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/>

²³ Available online at: <https://www.oaic.gov.au/about-us/our-regulatory-approach/guide-to-privacy-regulatory-action/>

²⁴ Respondent's response dated 25 February 2020, p 1.

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

41. The *Explanatory Memorandum for the Privacy Amendment (Enhancing Privacy Protection) Act 2012* (the **Explanatory Memorandum**), which introduced the concept of an “Australian link” in s 5B(3) of the Privacy Act, relevantly states:

The collection of personal information ‘in Australia’ under paragraph 5B(3)(c) includes the collection of personal information from an individual who is physically within the borders of Australia or an external territory, by an overseas entity.

For example, a collection is taken to have occurred ‘in Australia’ where an individual is physically located in Australia or an external Territory, and information is collected from that individual via a website, and the website is hosted outside of Australia, and owned by a foreign company that is based outside of Australia and that is not incorporated in Australia. It is intended that, for the operation of paragraphs 5B(3)(b) and (c) of the Privacy Act, entities such as those described above who have an online presence (but no physical presence in Australia), and collect personal information from people who are physically in Australia, carry on business in Australia.²⁵

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

42. 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

43. 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

44. In *Valve Corporation v Australian Competition and Consumer Commission*,²⁸ the Full Federal Court 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’.²⁹

45. The Full Federal Court stated in *Tiger Yacht Management Ltd v Morris* that the expression ‘carrying on business’ 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.³⁰ 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.³¹

²⁵ Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth), p 218.

²⁶ *Ibid.*

²⁷ APP guidelines [B.13].

²⁸ (2017) 258 FCR 190 (**Valve Corporation**)

²⁹ *Valve Corporation* at [149], after considering the analysis in *Campbell v Gebo Investments (Labuan) Ltd* (2005) 190 FLR 209

³⁰ *Tiger Yacht Management Ltd v Morris* [2019] FCFCA 8 at [50] (**Tiger Yacht**)

³¹ *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.³²
 - A company may be carrying on business in Australia even though it does not have an identifiable place of business within Australia.³³
46. I have taken the above judicial guidance into account. In considering the statutory context, I have also had regard to the objects of the Privacy Act, including:
- a. to promote the protection of the privacy of individuals (s 2A(a))
 - b. to promote responsible and transparent handling of personal information by entities (s 2A(d)).

Paragraph 5B(3)(c): the personal information was collected or held in Australia at the time of the act or practice

47. ‘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.

48. Relevantly, s 6(1) defines ‘record’ to include an electronic or other device.

49. ‘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.

50. 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 from an individual who is physically within the borders of Australia or an external territory, by an overseas entity.³⁴

Consideration

51. The respondent has repeatedly asserted that it is not subject to the Privacy Act.³⁵

52. According to the respondent:

- The respondent was founded in, is based in, and conducts its business in the United States. 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.

³² *Tiger Yacht* at [52]

³³ *Tiger Yacht* at [53]

³⁴ Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth), p 218.

³⁵ 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.

- 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 USA where the respondent conducts its business.³⁶
 - The respondent does ‘not exclude images in bulk based on the apparent location of the individual within the EU or Australia – to the extent that location information is even knowable based on a photo available on the internet.’³⁷
53. The respondent admitted that it provided trials and demonstrations of its products to several Australian police agencies inside of Australia, and did so at the request of personnel in those agencies.³⁸ 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.³⁹

Does the respondent carry on business in Australia?

54. In my preliminary view, the circumstances of this matter clearly demonstrate that the respondent has carried on business in Australia, not only while trial services were provided to Australian police services, but also throughout the entire period the respondent has indiscriminately scraped facial images from the Internet.
55. In the period October 2019 to 12 March 2020 (the **Trial Period**), the respondent provided trials of the Facial Recognition Tool to certain Australian police forces, whose members used the service during the following dates:
- Australian Federal Police: s 47E(d)
 - Queensland Police: s 47E(d)
 - South Australia Police: s 47E(d)
 - Victoria Police: s 47E(d)
56. The fact that none of the Australian police agencies became paying customers is, in my view, 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.
57. In this period, the respondent undertook multiple activities to support its provision of the Facial Recognition Tool to Australian police forces including actively marketing its service for commercial purposes. For example:

³⁶ Respondent’s response dated 19 August 2020 p 4.

³⁷ Respondent’s response dated 26 September 2020 p 6.

³⁸ Respondent’s response dated 19 August 2020 p 3.

³⁹ Respondent’s response dated 19 August 2020 p 3.

⁴⁰ 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”.

- 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.⁴¹
- The respondent emailed some Australian police force 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.⁴²
- The respondent emailed some Australian police forces encouraging them to refer other law enforcement officers to try out the Facial Recognition Tool, stating:

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.⁴³

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.

...⁴⁴

- The respondent submits that "[o]bviously, the purpose of a free trial is to sell the product."⁴⁵

⁴¹ 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)

⁴² Ibid.

⁴³ Queensland Police response dated 7 August 2020, pp 41, 83.

⁴⁴ Queensland Police response dated 7 August 2020, p 56.

⁴⁵ Respondent's response dated 26 September 2020, p 11.

- 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: '[t]hey 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"'.⁴⁶
 - 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)'.⁴⁷
 - A Clearview brochure provided to an Australian police force user included a page headed 'RAPID INTERNATIONAL EXPANSION'. The page included a map of the world with certain countries highlighted and labelled, including Australia.⁴⁸
 - The respondent sent advertising emails to users of Crimedex in Australia.⁴⁹
58. In the Trial Period, the respondent also collected Probe Images in Australia from Australian police force users as part of the trials and collected Scraped Images from the internet for inclusion in its database (see paragraphs 63-66 below).⁵⁰
59. For these reasons, in my preliminary view it is clear that during the period the respondent offered trials to Australian police agencies, it carried on business in Australia within the meaning of s 5B(3)(b).
60. In reaching this view, 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.⁵¹
61. Since the Trial Period, I accept that the respondent has made some changes to its business practices. The respondent no longer undertakes marketing activities in Australia, and s 47E(d) [REDACTED] By the end of March 2020, the respondent had instituted a policy of refusing all requests for accounts from Australia.⁵²
62. Notwithstanding these changes, the respondent admitted that it continues to collect images from the internet without regard to geography or source.⁵³ The exact number of images derived from individuals in Australia is unknown, as, according to the respondent, it 'cannot determine the nationality of the person'.⁵⁴ However, having regard to the indiscriminate nature of the respondent's scraping, and the size of the respondent's database (which contains 3 billion images),⁵⁵ I consider that the respondent has

⁴⁶ Queensland Police response dated 7 August 2020, p 12.

⁴⁷ Ibid.

⁴⁸ AFP response dated 21 April 2020, Annexure C, p 8.

⁴⁹ Respondent's response dated 26 September 2020 p 10.

⁵⁰ 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 Report on the use of Clearview, undated (**Victoria Police Report**) p 1-2.

⁵¹ s 2A of the Privacy Act.

⁵² Respondent's response dated 2 November 2020 p 2.

⁵³ Respondent's response dated 19 August 2020 p 2.

⁵⁴ Respondent's response dated 26 September 2020 p 3.

⁵⁵ Respondent's response dated 25 February 2020 p 2.

collected, and continues to collect Australians' facial images,⁵⁶ and uses them to derive image vectors for its database, including to market to law enforcement agencies.

63. The evidence shows that image scraping from publicly available sources across a global internet, 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.⁵⁷

64. For example, in emails from the respondent to some Australian police force 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)⁵⁸

65. In another email to Australian police force 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.⁵⁹

66. An Australian police force 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 2020.⁶⁰

67. 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.⁶¹ 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.⁶² 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 of Australia.⁶³

⁵⁶ 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/>

⁵⁷ 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."⁵⁸ 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.

⁵⁸ 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.

⁵⁹ 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.

⁶⁰ Queensland Police response dated 7 August 2020, p 12.

⁶¹ Tiger Yacht at [50].

⁶² s 2A of the Privacy Act

⁶³ Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth), p 218.

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

69. For these reasons, it is my preliminary view that the respondent has been carrying on business in Australia since at least October 2019 within the meaning of s 5B(3)(b).

Does the respondent hold personal information in Australia?

70. There is no evidence before me at this stage to contradict the respondent’s submission that it does not store information or images in Australia.⁶⁴

71. 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?

72. The evidence shows that the respondent collected the following personal information in Australia in the Trial Period:

- the name, contact information and employer name, of each member of an Australian Police Force that registered to use the Facial Recognition Tool⁶⁵
- information about the usage activity of its registered Australian users, including IP address, browser information, location data, search history, and login history⁶⁶
- Probe Images uploaded to the Facial Recognition Tool by registered Australian users (including suspects, victims of crime and members of Australian police forces who searched themselves or individuals known to them).⁶⁷

73. I am also satisfied that the respondent has been collecting Scraped Images in Australia at least since October 2019, for the following reasons:

- The respondent submits that it maintains a database of more than 3 billion facial images that it has collected from various publicly available websites.
- The respondent submits that it indexes Scraped Images and URLs from the internet without targeting particular countries, and advised that it is not aware of the nationality of individuals depicted in Scraped Images in its Database, and that it does not exclude images based on the apparent location of those individuals.⁶⁸
- 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 the Australian police force users,

⁶⁴ Respondent’s response dated 19 August 2020, p 3.

⁶⁵ Respondent’s Privacy Policy available at: https://clearview.ai/privacy/privacy_policy.

⁶⁶ Respondent’s Privacy Policy available at: https://clearview.ai/privacy/privacy_policy.

⁶⁷ 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.

⁶⁸ Respondent’s response dated 26 September 2020, p 6.

some of whom used the service to upload images depicting individuals located in Australia to find Matched Images.⁶⁹

- For some Australian police force members that used the respondent's Facial Recognition Tool, the Facial Recognition Tool displayed Matched Images⁷⁰ including Matched Images of unknown persons of interest located in Australia.⁷¹
- Some Australian police force users, who were Australia residents, searched for and identified images of themselves in Clearview's database.⁷²
- The respondent's website contained information directed specifically to individuals in Australia, to provide them with the option to opt-out of the respondent's search results.⁷³
- Information on the respondent's website gives Australians (along with EU, Swiss and UK residents) the option to view search results relevant to themselves.⁷⁴

74. The respondent repeatedly asserted that it does not identify whether images of Australians are included in its Database.⁷⁵ s 47E(d)

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

75. Taking into account the indiscriminate nature of the respondent's scraping (including from social media platforms), and the size of the respondent's database (which contains 3 billion images),⁷⁷ and the fact that Australian police force members have conducted successful searches of the Facial Recognition Tool using facial images of individuals

⁶⁹ 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.

⁷⁰ Victoria Police Report (report stating that trials undertaken by the author and another police member resulted in initial success), p 1.

⁷¹ 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 2021, p 3; AFP response dated 19 March 2021 p 2.

⁷² Queensland Police response dated 26 February 2021 p 1-3; AFP response dated 19 March 2021 p 1-2.

⁷³ Respondent's website, Privacy Request Forms: <https://clearview.ai/privacy/requests> (accessed 17 December 2020)

⁷⁴ Ibid.

⁷⁵ Respondent's response dated 19 August 2020 p 4; Respondent's response dated 26 September 2020 p 3-4; Respondent's response dated 2 November 2020, p 3.

⁷⁶ "Clearview Defendants' Memorandum of Law In Opposition To Plaintiff's Motion For Preliminary Injunction," filed 6 May 2020 US District Court For the Northern District of Illinois, Eastern Division; <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-no-facial-recognition-private-companies>

⁷⁷ Respondent's response dated 25 February 2020 p 2.

located in Australia,⁷⁸ I am satisfied that the respondent's web crawler collected images of many individuals located in Australia for inclusion in its database.

76. Based on the available information, it is my preliminary view that since at least October 2019, the respondent has collected Scraped Images of individuals in Australia within the meaning of s 5B(3)(c).

77. As outlined in paragraph 13 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.

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.⁷⁹

78. In response to questions from the OAIC about the number of opt-out and access requests from Australian residents, the respondent submits that 'Clearview AI 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 s 47E(d) Australia'.⁸⁰

79. It is my preliminary view that the respondent also collects email addresses and images of Australians seeking to make an opt-out request.

APP entity

Law and policy

80. The Privacy Act regulates the acts and practices of 'APP entities'. An 'APP entity' is either an organisation or an 'agency' (s 6).

81. An 'organisation' includes a body corporate that is not a 'small business operator' (s 6C). 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).⁸¹ A 'small business' is a business that has an annual turnover for the previous financial year that is \$AUD3 million or less (s 6D(1)).

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

⁷⁸ Victoria Police Report; 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.

⁷⁹ Respondent's opt-out form: <https://clearviewai.typeform.com/to/zqMFnt>

⁸⁰ Respondent's response dated 26 September 2020 p 8-9.

⁸¹ s 6C of the Privacy Act.

else for a benefit, service or advantage, without the individual's consent or as required or authorised by or under legislation (s6D(4)(c)).

Consideration

83. The respondent submits that:

- It is a small business operator with an annual turnover of less than \$3,000,000.
- It has not had an annual turnover of greater than \$3 million 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.⁸²

84. Despite written requests by the OAIC⁸³, the respondent provided no evidence to support its submission that it has not had an annual turnover of greater than \$3 million in any financial year, and is not related to any business that has had such an annual turnover.⁸⁴

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 in any financial year (and is not related to any business that has had an annual turnover of \$3,000,000 or less), in my view the exception in s 6D(4)(c) applied during the Trial Period and as at the date of this preliminary view.

87. The evidence shows that during the Trial Period the respondent disclosed Scraped Images about Australian individuals (and associated source URLs), to Australian police forces as part of the free trials.⁸⁵ The purpose of those disclosures was part of a deliberate marketing strategy to attract paying customers.⁸⁶

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.⁸⁷ It is reasonable to infer that the

⁸² Respondent's response dated 19 August 2020, p 3-4.

⁸³ Section 44 notice issued to the respondent on 7 July 2020 asked: "Clearview advised the OAIC that it was incorporated on 3 August 2017 and has not had an annual turnover greater than \$3 million since that time. Provide details confirming that this is correct, including a copy of Clearview's tax return for the most recent financial year." (at question 76, p 18).

⁸⁴ Ibid.

⁸⁵ See, for example, Victoria Police Report, which stated that trials undertaken by the author and another officer resulted in initial success. See also Queensland Police responses dated 26 February 2021 and dated 7 August 2020 that show at least 4 Queensland Police Service members conducted successful searches using images of themselves, and successful searches of a number of persons of interest located in Australia. See also the AFP response dated 19 March 2021 that shows 3 AFP members conducted successful searches using images of themselves and of one person of interest located in Australia.

⁸⁶ Respondent's response dated 26 September 2020 p 11: 'Obviously, the purpose of a free trial is to sell the product.'

⁸⁷ <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

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 13 above).

89. The Scraped Images are personal information, collected without consent (see paragraphs 101 and 141 -151 below).
90. For these reasons, in my preliminary view, even if the respondent had an annual turnover of \$3 million 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 (ss 6C(4)(d)).⁸⁸

'Personal information'

Law and policy

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 there is a connection between the information and the individual. This is ultimately a question of fact and will depend on the context and the circumstances of each particular case.⁸⁹
94. Whether a person is 'reasonably identifiable' is an objective test that has practical regard to the context in which the particular information is handled.
95. Generally speaking, an individual is 'identified' when, within a group of persons, that person is 'distinguished' from all other members of a group.⁹⁰ 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 it is possible to identify the individual from available information, including, but not limited to, the information in issue.⁹¹ 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 another audience (or machine) could make that link.
96. 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

⁸⁸ s 6D(7)-(8) of the Privacy Act; <https://www.oaic.gov.au/privacy/privacy-for-organisations/trading-in-personal-information/>.

⁸⁹ 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.

⁹⁰ <https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/>

⁹¹ 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/>.

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.⁹²

Consideration

97. The respondent submits that it does not collect or handle any ‘personal information’. It submits 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 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.⁹³
- Vectors it retains for the purpose of actioning a deletion or opt-out request are not associated with the original image (which is deleted), or any other identifying information.⁹⁴

Scraped Images and Probe Images

98. I first consider whether Scraped Images and Probe Images constitute Personal Information.

s 47E(d)



101. I am satisfied that individuals in Scraped Images and Probe Images are reasonably identifiable. These kinds of facial images contain a multiplicity of data points, from which an individual can be uniquely distinguished from others within the respondent’s database.

102. Moreover, according to the respondent, the purpose of offering the Facial Recognition Tool, is to assist a user to identify an unknown individual, including perpetrators and victims of crime.⁹⁵ The respondent provides registered users with Scraped Images that appear to match the Probe Image, along with associated source URLs and webpage title, so that the registered user can either identify the user from information in that URL and/or webpage title (for example, if the URL or webpage title includes the individual’s name), or by clicking through to another linked webpage to view more information about the individual. In the circumstances, the steps needed to identify an individual can involve a single click on the URL, and are reasonable to achieve.

⁹² 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/>.

⁹³ Respondent’s response dated 19 August 2020, p 2, 4.

⁹⁴ Respondent’s response dated 2 November 2020, p 4.

⁹⁵ Respondent’s response dated 19 August 2020, p 2 states: ‘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.’

103. For the reasons outlined above, I am satisfied that Probe Images and Scraped Images handled by the respondent are information about individuals who are reasonably identifiable. It is therefore my preliminary view that the Scraped Images and Probe Images are 'personal information' as defined in s 6(1) of the Privacy Act.

Image vectors

104. A Probe Image Vector is a mathematical representation of information in a Probe Image (see above at paragraph 8). A Scraped Image Vector is a mathematical representation of information in a Scraped Image (see above at paragraph 7).⁹⁶ As these digital templates are direct representations of a particular individual's facial features, I am satisfied that they are 'about' an individual.

105. I am also satisfied that individuals depicted in these vectors are reasonably identifiable. While the vectors themselves are not disclosed to registered users, collection and use of this information is an inherent feature of the identification process. The respondent's tool generates these vectors from Scraped Images and Probe Images, then when a user conducts a search, the system uses a Probe Image Vector to interrogate its database of image vectors to find Matched Images. This process, which involves routinely linking image vectors with other available information, enables an individual to be identified.

106. On this basis, I am satisfied that Probe Image Vectors and Scraped Image Vectors constitute information about a reasonably identifiable individual, and accordingly, that they are 'personal information' as defined in s 6(1) of the Privacy Act.

Opt-out Vectors

107. The respondent collects a facial image and an email address from individuals that submit a request to opt out of search results (see paragraph 13 above). From this image, the respondent generates a mathematical representation of that person's image. The respondent subsequently deletes the image.⁹⁷

108. However, the respondent retains the Opt-out Vector (and an anonymised hash of the email address) permanently, in order to block the individual requesting opt-out from search results and prevent further collection of any images of that person.⁹ Where there is a match, the respondent omits any images in its database showing the individual depicted in that vector, from future search results.⁹⁸

109. In my view, 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.

110. On that basis, I am satisfied that Opt-out Vectors are about 'reasonably identifiable' individuals. Accordingly, I am satisfied that these Opt-out Vectors are 'personal information' as defined in s 6(1) of the Privacy Act.

⁹⁶ Respondent's response dated 4 August 2020 p 3; Respondent's response date 26 September 2020 p 7.

⁹⁷ Respondent's response dated 2 November 2020 p 5.

⁹⁸ Respondent's response dated 26 September 2020 p 9-10.

Preliminary findings on breach

APP 3.3

Law and policy

111. 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.
112. The requirements in APP 3.3 apply, even if personal information is collected from a publicly available source.

Collects

113. 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.
114. The term 'collection' 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.⁹⁹ This includes collection by 'creation' which may occur when information is created with reference to, or generated from, other information the entity holds.¹⁰⁰

Sensitive information and biometrics

115. The definition of 'sensitive information' extends to two particular kinds of biometric information, 'biometric information collected for use in automated biometric verification and identification systems' and 'biometric template information'.¹⁰¹
116. 'Biometric information', 'biometric systems' and 'biometric templates' are not defined in the Privacy Act.
117. '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).¹⁰² These characteristics cannot normally be changed and are persistent and unique to the individual.

⁹⁹ APP Guidelines [B.23]-[B.28].

¹⁰⁰ <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>

¹⁰¹ s 6(1) of the Privacy Act.

¹⁰² 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*.

118. '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.
119. A 'biometric template' is a digital or mathematical representation of an individual's biometric information that is created and stored when that information is 'enrolled' into a biometric system.¹⁰³ Machine learning algorithms then use the biometric template to match it with other biometric information, for verification, or to search and match against other templates within a database, for identification.

Consent

120. 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, and
- the individual has the capacity to understand and communicate their consent.

121. 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.¹⁰⁴

122. Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity.¹⁰⁵

123. Use of an opt-out mechanism to infer an individual's consent will only be appropriate 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.¹⁰⁶

Exceptions to APP 3.3

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

¹⁰³ 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).

¹⁰⁴ APP Guidelines [B.41].

¹⁰⁵ APP Guidelines [B.37].

¹⁰⁶ APP Guidelines [B.40].

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

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.¹⁰⁷

126. For this exception to apply, there must be a reasonable basis for the belief, and not merely a genuine or subjective belief.¹⁰⁸ 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.¹⁰⁹

Consideration

127. The respondent submits 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).'¹¹⁰ s 47E(d)

On that basis, I am satisfied that the respondent 'collects' the Scraped Images.

128. The respondent's Facial Recognition Tool analyses Scraped Images and Probe Images to produce a vector for each image. As collection under the Privacy Act includes creation of personal information from existing information, this is also considered a 'collection' under the Privacy Act.

129. The respondent submits that it does not seek consent from any individuals shown in Scraped Images to collect their images. It maintained that it does not need to obtain consent as it does not handle personal or sensitive information. In the respondent's submission, this is because all identification processes rely on external information.¹¹²

Does the respondent collect sensitive information?

Scraped and probe images and associated vectors

130. Consistent with the definition of 'biometrics' above, 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 largely 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'.

131. The respondent's Facial Recognition Tool compares an unknown person's biometric characteristic (in the Probe Image and associated vectors), to other characteristics of the

¹⁰⁷ APP 3.4(b), section 16A(1), Item 1.

¹⁰⁸ APP Guidelines, [B.111].

¹⁰⁹ APP Guidelines [C.8].

¹¹⁰ Letter from the respondent to the ICO dated 21 July 2020 (**respondent's response dated 21 July 2020**) p 2.

¹¹¹ Respondent's response dated 26 September 2020 p 7.

¹¹² Respondent's response dated 19 August 2020 p 2.

same type in its Database (Scraped Images and associated vectors). 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, so that the user can identify that person.¹¹³ This is an entirely automated process based on an algorithm developed through machine learning technology.¹¹⁴ 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.¹¹⁵

132. The evidence before me shows that members of Victoria Police, Queensland Police Service and the AFP conducted successful searches of the Facial Recognition Tool using facial images of themselves and persons of interest located in Australia.¹¹⁶
133. On this basis, I am satisfied that Scraped and Probe Images and vectors generated from these are 'biometric information collected for use in automated biometric verification and identification systems'.
134. Furthermore, Scraped and Probe Image Vectors are derived from biometric samples by using an algorithm, which is premised on complex mathematical formulas, to measure certain characteristics of an individual's face.¹¹⁷ That is, the respondent creates representations of individuals' biometric information and stores these in a biometric identification system. On that basis, I am satisfied that these kinds of vectors are 'biometric templates'.

Opt-out vectors

135. As discussed at paragraph 13 – 14, 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.
136. Consistent with the definition and explanations above, I am satisfied that Opt-Out Vectors are 'biometric information collected for use in automated biometric verification and identification systems' and 'biometric templates'.
137. It is therefore my preliminary view 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).

¹¹³ Clearview AI'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.'

¹¹⁴ Respondent's response dated 4 August 2020 p 3.

¹¹⁵ 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.

¹¹⁶ 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.

¹¹⁷ Respondent's response dated 26 September 2020 p 7.

Did individuals consent to the collection of their sensitive information?

138. 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 obtains express consent to collect Probe Images of a witness, suspect or victim, or to collect any image vectors.

139. While entities should generally not rely on implied consent when collecting sensitive information,¹¹⁸ I have considered whether individuals impliedly consent to the collection of their personal information by the Respondent.

Probe Images and Probe Image Vectors

140. 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.

Scraped Images and Scraped Image Vectors

141. 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 submits that it did 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'.¹¹⁹
- The respondent provides some information in its Privacy Policy (available on its website), about its collection of public images. In particular:
 - Clearview's Privacy Policy dated 29 January 2020 to 19 March 2021 (the **29 January 2020 Privacy Policy**) 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.'
 - Clearview's Privacy Policy dated 20 March 2021 to the present (the **20 March 2021 Privacy Policy**) states:
 - 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

¹¹⁸ APP Guidelines [B.41].

¹¹⁹ Respondent's response dated 21 July 2020 p 2; Respondent's response dated 4 August 2020 p 3, 5.

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.’
142. For the reasons set out below, I am not satisfied that consent can be implied in these circumstances, as any such consent would not meet the requirements discussed in paragraphs 120 to 123 above.
143. Consent may not be implied if an individual’s intent is ambiguous or there is reasonable doubt about the individual’s intention.¹²⁰ In my view, 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.¹²¹ 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.
144. Consent also cannot be implied if individuals are not adequately informed about of 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.¹²² The respondent’s publicly accessible policy documents do not refer to the creation and handling of image vectors. Although the 20 March 2021 Privacy Policy contains a reference to extracting ‘measurements of facial features for individuals’, this is insufficient to enable individuals to understand that image vectors are being collected and how they are handled by Clearview. Thus, any consent provided through these policy documents would not be adequately informed.
145. Even if these documents did refer to the creation of image vectors, an APP entity cannot infer consent simply because it has published a policy about its personal information handling practices.¹²³ Any such consent would not be current and specific to the context in which that information is being collected.
146. Consent cannot be implied from the fact that individuals did not make a request to opt out (see paragraphs 14 to 16). The opt-out mechanism is 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 to 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 at paragraph 159).

¹²⁰ APP Guidelines [B.39].

¹²¹ 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>.

¹²² APP Guidelines [B.47].

¹²³ *Flight Centre Travel Group (Privacy)* [2020] AICmr 57 (25 November 2020), [53].

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

Opt-Out Vectors

148. I have also considered whether individuals consented to the collection of their Opt-out Vectors.

149. 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.

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

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

Exceptions to APP 3.3

152. I have considered whether the exceptions in APP 3.4 apply.

153. In respect of the Serious Threat to Life, Health or Safety exception,¹²⁴ I have considered whether 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'.

154. In my view, there is no reasonable basis to support such a belief.

155. As the respondent's database includes over 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 would be 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.

156. On that basis, I am not satisfied that there is a reasonable basis for any belief that collection of Australian individuals' sensitive information is 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 s 16A(1), Item 1 does not apply.

157. None of the other exceptions in subclause 3.4 apply.

Preliminary finding

158. It is my preliminary view that, by collecting sensitive information without consent, the respondent has interfered with the privacy of the following groups of Australian individuals in breach of APP 3.3:

- a. individuals whose Scraped Images and derived vectors have been collected by the respondent in Australia

¹²⁴ APP 3.4(b), s 16A, item 1.

- b. individuals such as witnesses, victims and suspects, whose Probe Images have been collected by the respondent in Australia
- c. individuals whose Opt-out Image Vectors have been collected by the respondent for the purpose of actioning a deletion or opt-out request.

APP 3.5

159. 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.¹²⁵ Collection may also be unfair where an entity misrepresents the purpose or effect of collection.¹²⁶
160. When assessing whether a collection is ‘unfair’ for the purposes of APP 3.5, all the circumstances must be considered.¹²⁷ For example, it would usually be unfair to collect 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

161. The respondent submits 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).¹²⁸ The respondent admitted that it does not notify individuals depicted in the images of the collection of their images.¹²⁹

Collection of Scraped Images and Scraped Image Vectors

162. In my view, the vast majority of individuals would not be aware or have any reasonable expectation¹³⁰ that their personal information has 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.¹³¹
 - 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.¹³² 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 143 above) and a number of social media companies have sent the respondent cease and desist letters in relation to alleged scraping from their sites.¹³³

¹²⁵ Explanatory Memorandum, *Privacy Amendment (Enhancing Privacy Protection) Bill 2012* (Cth), p 77.

¹²⁶ APP Guidelines [3.63].

¹²⁷ *‘LP’ and The Westin Sydney (Privacy)* [2017] AICmr 53 (7 June 2017) [33].

¹²⁸ Respondent’s response dated 21 July 2020 p 2.

¹²⁹ Respondent’s response dated 19 August 2020 p 2.

¹³⁰ *‘LP’ and The Westin Sydney (Privacy)* [2017] AICmr 53 (7 June 2017).

¹³¹ Respondent’s response dated 19 August 2020, p 2.

¹³² Respondent’s response dated 25 February 2020 p 2-3.

¹³³ Correspondence to the OAIC from online platforms, including Twitter and LinkedIn.

- The respondent’s publicly available Terms of Service and Privacy Policies provide limited information about its information handling practices. For example, they do not explain:
 - that the respondent collects facial images
 - how the respondent collects Scraped Images or the particular sites they are gathered from¹³⁴
 - 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
 - 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;
 - that third parties may search the system for unrestricted trial purposes (rather than just law enforcement purposes).
163. In my view, the absence of specific and timely information about the respondent’s collection practices, particularly in circumstances where scraping is inconsistent with the policies of certain social media companies from which the information is scraped, constitutes covert collection.
164. 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.
165. 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.¹³⁵
166. More broadly, the respondent’s collection of biometric information in such circumstances may cause individuals to perceive that they are under constant surveillance by a private company, which would likely have ensuing impacts on their exercise of personal freedoms such as freedom of expression (in relation to, for instance, sharing on social media), association and movement.
167. 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

¹³⁴ 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’

¹³⁵ US Patent and Trademark Office, *United States Patent Application*, 20210042527, Thon-That, Cam-Hoan, filing date 7 August 2020, publication date 11 February 2021.

enforcement objectives, must be subject to a careful and critical assessment of its necessity, legitimacy and proportionality.¹³⁶

168. In this case, I do not accept that the impact on individuals' privacy are 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 cannot be reissued or cancelled like other forms of compromised identification information. It can also be replicated for identity theft purposes.
- The respondent collects the personal information of millions of individuals, only a fraction of whom would ever be connected with law enforcement investigations. The evidence suggests that this includes the information of vulnerable individuals, including victims of crime and minors.¹³⁷
- The information is collected for commercial purposes even though it is currently offered to law enforcement. These purposes include training and improving the respondent's algorithm and monetizing the respondent's technology and data holdings through contractual arrangements.

169. Having regard to the kind of information collected and handled by the respondent, the respondent's commercial purposes of offering its service, and the covert and indiscriminate method of collection, I consider that the covert collection of these kinds of information, is unreasonably intrusive.

Preliminary findings

170. It is my preliminary view that the respondent interfered with the privacy of individuals by collecting Scraped Images (and URLs and metadata) of Australians, as well as vectors derived from these images, by unfair means in breach of APP 3.5.

APP 5

171. 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 ('**APP 5 matters**') or to otherwise ensure that the individual is aware of any such matters.

172. 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.

173. The APP 5 matters 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 collection¹³⁸

¹³⁶ 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>>

¹³⁷ See Victoria Police Report, p 1, that states cropped images depicting faces of unknown child victims were uploaded.

¹³⁸ APP 5.2(b)(ii).

- The purposes for which the APP entity collects personal information¹³⁹
 - 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.¹⁴⁰
174. 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.¹⁴¹

Consideration

175. The respondent submits 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.¹⁴²
176. The Respondent also submits that from 29 January 2020, it began to offer Australian residents an online form to 'opt-out' from its search results (see paragraphs 13 to 16). Screenshots of the process are at Attachment C.
177. The respondent submits that it provides a Privacy Policy to the general public.¹⁴³ I have had regard to the 29 January 2021 Privacy Policy and 20 March 2021 Privacy Policy.¹⁴⁴
178. The respondent also has a Data Policy that it submits was accessible when Australian residents made a request through the publicly available data subject portal (which no longer appears to be available on the respondent's website). The respondent submits that the response individuals were sent contained a link to the respondent's Data Policy.¹⁴⁵

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

179. The respondent's Data Policy, Privacy Policies and notices do not address all the matters in APP 5.2.
180. In particular, for Scraped Images, they do not explain that the respondent collects personal information in Scraped Images (and associated Scraped URLs and Metadata), and they do not provide adequate detail about where this personal information is collected from (APP 5.2(b)).¹⁴⁶
181. For vectors generated from Scraped Images, they generally do not explain that biometric templates are generated from algorithmic analysis of an individual's facial image, and that they are collected and retained each time the Respondent collects a Scraped Image (APP 5.2(b)). The only reference to collection of such information appears

¹³⁹ APP 5.2(d)

¹⁴⁰ APP 5.2(f)

¹⁴¹ APP Guidelines [5.4].

¹⁴² Respondent's response dated 19 August 2020 p 2.

¹⁴³ Respondent's response dated 21 July 2020 p 3.

¹⁴⁴ https://clearview.ai/privacy/privacy_policy.

¹⁴⁵ Respondent's response dated 26 September 2020 p 6.

¹⁴⁶ The 29 January 2020 Privacy Policy stated: 'Publicly available images: Clearview uses proprietary methods to collect publicly available images from various sources on the Internet', available at <https://clearview.ai/>

in the 20 March 2021 Privacy Policy, which states, ‘Clearview may extract information from those photos [that are publicly available on the Internet] including geolocation and measurements of facial features for individuals in the photos.’

182. Moreover, they do not explain the respondent’s purpose of collection. While the 29 January 2020 Privacy Policy explains the purpose that the respondent’s users use the collected Scraped Images for, it does not explain the respondent’s own purpose of collecting Scraped Images (and associated Scraped URLs and Metadata) and Scraped Image Vectors (APP 5.2(d)).
183. In respect of Opt-Out images, the respondent does not provide any information to individuals about the collection, through creation from opt-out image, of biometric templates.
184. In addition, while it appears from the link referred to at paragraph 174(b) above that individuals can request data deletion, this is not the case. As noted above, the effect of making a deletion/ opt-out request, is that the respondent will block images of that individual from appearing in future search results, and will prevent further collection of Scraped Images of that individual. The respondent does not delete these images from its database.
185. There is no evidence that the respondent provides any other information to individuals depicted in Scraped Images or to individuals submitting an opt-out request about the APP 5 matters.

Are the steps Clearview takes to notify individuals of APP 5 matters reasonable in the circumstances?

186. 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 nor obtaining consent.
187. In my view, even if the respondent’s Privacy Policy and/or Data Policy had included all of the information listed at APP 5.2 (and I do not consider that they do), this would not constitute 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 be aware of the respondent’s Privacy Policy or would seek it out, as most of these individuals would have had no direct dealings with the respondent.
 - The Data Policy is not easily accessible, as it is only provided when an individual makes an access request.
 - Some individuals whose information the respondent collects may have particular needs, such as children or individuals from a non-English speaking background.
 - 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 is required to take more rigorous steps to ensure individuals are notified under APP 5.
188. Accordingly, I am not satisfied that the respondent takes reasonable steps in the circumstances to notify individuals depicted in biometric templates derived from Scraped Images, Scraped Images, biometric templates derived from opt-out request images, and

facial images submitted with an opt-out request, at or before the time their images are scraped, of the APP 5 matters.

Preliminary finding

189. It is my preliminary view that the respondent interfered with the privacy of individuals by failing to take reasonable steps to:

- notify individuals about the fact and circumstances of collecting each of the following:
 - Scraped Images
 - biometric templates derived from those images
 - biometric templates derived from opt-out request images under APP 5.2(b).
- notify individuals about the purpose of collecting each of the following:
 - Scraped Images
 - biometric templates derived from those images
 - facial images submitted as part of the opt-out process
 - biometric templates derived from those images under APP 5.2(d).

APP 10

190. 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**).

191. Personal information is inaccurate if it contains an error or defect as well as if it is misleading.¹⁴⁷

192. Where there is evidence that an APP entity has disclosed personal information that does not meet one or more of the quality factors, this may suggest that the APP entity has breached APP 10.2, though it is not determinative.

193. Similarly, merely because 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.

194. Reasonable steps that an entity should take will 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.¹⁴⁸

195. 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:¹⁴⁹

¹⁴⁷ APP guidelines [10.12].

¹⁴⁸ APP guidelines [10.6].

¹⁴⁹ 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

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 compelling risks of harm to individuals, particularly when facial recognition is used in the context of law enforcement.¹⁵⁰

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.¹⁵¹ 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.¹⁵² Harms resulting from such misidentification can range from individuals being excluded from opportunities, to individuals being investigated and detained based on incorrect information.

Consideration

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

196. The respondent has made the following representations about accuracy of the Facial Recognition Tool:

- As at the date of this preliminary view, the respondent’s Code of Conduct states: ‘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.’¹⁵³ The

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>

¹⁵⁰ Angwin, J. et al. “Machine Bias,” *ProPublica*, May 23, 2016.

¹⁵¹ 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.

¹⁵² “Face Recognition Vendor Test, Part 3: Demographic Effects,” *National Institute of Standards and Technology* (NIST), December 2019.

¹⁵³ 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.

corollary is that the purpose of disclosing Matched Images through the Facial Recognition Tool, is to provide a source for establishing the identity of an individual.

- As at the date of this preliminary view, the respondent’s website states:
 - ‘Clearview AI’s technology empowers agencies to quickly, accurately, and efficiently identify suspects, persons of interests and victims of crime.’¹⁵⁴
 - ‘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.’¹⁵⁵
 - ‘Independently Assessed For Accuracy An independent panel of experts assessed the accuracy of Clearview AI’s search results and found no errors.’¹⁵⁶
- 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)¹⁵⁷

197. s 47E(d)

198. It 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.’¹⁵⁹

199. The respondent submits that it ‘has conducted multiple tests of the accuracy of our image search algorithm, including a test performed by a panel of independent experts’.¹⁶⁰ In support of this assertion, 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**).¹⁶¹

200. 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).

201. For each individual in the test, the two top-ranked matches returned from the respondent’s Database were compared with the submitted image.

202. 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’.¹⁶²

¹⁵⁴ <https://clearview.ai/>

¹⁵⁵ <https://clearview.ai/overview>

¹⁵⁶ <https://clearview.ai/legal>

¹⁵⁷ Queensland Police response dated 7 August 2020 p 32, 38, 58, 63, 73, 81.

¹⁵⁸ Respondent’s response dated 4 August 2020 p 3.

¹⁵⁹ Respondent’s response dated 4 August 2020 p 3.

¹⁶⁰ Respondent’s response dated 21 July 2020 p 3.

¹⁶¹ Respondent’s response dated 26 September 2020 Attachment B.

¹⁶² Respondent’s response dated 26 September 2020 response p 16.

203. An extract of the Accuracy Report, including a summary of the methodology, conclusion and descriptions of the panel members, was sent to the AFP.¹⁶³
204. 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 2020.¹⁶⁴

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

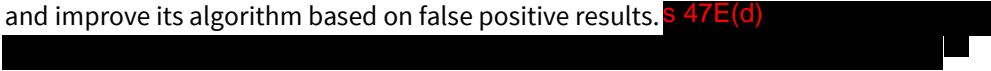
205. The respondent's business offers a facial recognition service to law enforcement for profit. As part of this service, the respondent handles a substantial and rapidly expanding volume of personal information, from which serious decisions may be made by its law enforcement clients. In circumstances 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 195), the steps needed to ensure accuracy should be robust, demonstrable, independently verified and audited.
206. While the respondent claims it does not guarantee accuracy, I give little weight to this evidence. The statements on its website and to prospective clients outlined in paragraph 196 above clearly indicate that the purpose of disclosing a Matched Image/s to a user, is to match the image/s with a Probe Image, for the purposes of identifying the individual in the Probe Image. Having regard to this purpose, reasonable steps must be taken to ensure the match/es are accurate.
207. I am not satisfied that the steps the respondent takes to ensure the accuracy of Matched Images are reasonable in the circumstances.
208. The respondent's submissions only provide evidence of a single accuracy test – the October 2019 test (even though in its submissions to the OAIC, the respondent has vaguely referred to conducting 'multiple' tests).
209. According to the respondent, this test was based on a test conducted by the American Civil Liberties Union (ACLU) in July 2018.¹⁶⁵ 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, of which false matches were disproportionately people of colour.¹⁶⁶
210. 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 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.
211. In my view, this led to limitations in the testing methodology, including, for example:

¹⁶³ AFP response dated 21 April 2020, Annexures Part 1, Annexure C, p 15.

¹⁶⁴ OAIC s 44 notice dated 7 July 2020, questions 57 and 58, p 15.

¹⁶⁵ Respondent's response dated 26 September 2020 p 16.

¹⁶⁶ <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>.

- 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 Database are displayed to the user as search results.
 - Given that the respondent populates its database using an automated web crawler, the more public photos of an individual there are on the internet, the more successful the Facial Recognition Tool is likely to be. 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 impact on accuracy.
 - Based on the biographies included in the Accuracy Report,¹⁶⁷ it is unclear that the panel members that participated in the October 2019 test had expertise or qualifications in facial recognition. While it is not necessarily a prerequisite to have particular expertise or qualifications, if the panel members were being presented by the respondent as ‘a panel of independent experts’¹⁶⁸ 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.
212. There is no evidence that the respondent engaged independent experts to conduct subsequent accuracy tests.
213. There is also no evidence that the respondent implemented mechanisms to train and improve its algorithm based on false positive results. s 47E(d) 
214. Having regard to the sensitivity of the data, the risk of harms 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 images displayed to users.

Preliminary finding

215. It is my preliminary view that the respondent interfered with the privacy of individuals whose Matched Images it discloses to its clients, by not taking reasonable steps to ensure that the personal information it disclosed is accurate, having regard to the purpose of disclosure, in breach of APP 10.2.

APP 1.2

216. 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.
217. 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

¹⁶⁷ Respondent’s response dated 26 September 2020 p 19-20.

¹⁶⁸ Respondent’s response dated 21 July 2020 p 3.

¹⁶⁹ Respondent’s response dated 4 August 2020 p 3.

APP 1.2, to demonstrate that personal information is managed in an open and transparent way.¹⁷⁰

218. The reasonable steps that an APP entity should take will depend upon 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.¹⁷¹
219. 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
 - 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. 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 1.2.¹⁷²

Consideration

Procedures for de-identification/ destruction of personal information

220. 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.
221. The respondent 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.¹⁷³ 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.¹⁷⁴

¹⁷⁰ APP Guidelines [1.5].

¹⁷¹ APP Guidelines [1.6].

¹⁷² APP Guidelines [1.7].

¹⁷³ 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).

¹⁷⁴ 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).

222. Based on the respondent's policy documents and responses to supplementary OAI/ICO questions, the steps taken to implement these kinds of practices, procedures and systems are:

- The respondent offers a tool to remove links from its search results that are already taken down from the web (see paragraph 18).
- The respondent does not have a formal retention schedule.¹⁷⁵
- The respondent has not conducted a formal Data Protection Impact Assessment in relation to the Facial Recognition Tool.¹⁷⁶

223. 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.

224. s 47E(d)



225. It is the responsibility of an APP entity to be able to justify that reasonable steps were taken. There is no evidence of other relevant measures implemented by the respondent.

226. As I have discussed in paragraphs 162-170 above, in my preliminary view, the respondent collected Australian's 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.

227. Even if the respondent were permitted to use and disclose the information under the Privacy Act, at a minimum, additional steps that must be taken in the circumstances include implementing a data retention policy, that:

- enables the respondent to proactively identify personal information that must be destroyed or de-identified under APP 11.2
- ensures that such information is destroyed, or de-identified as required
- documents how the policy will 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

228. The respondent submits that it has not conducted a formal Data Protection Impact Assessment in relation to any of the processing it carries out.¹⁷⁷ There is no evidence that the respondent otherwise conducted a systematic assessment of measures and controls

¹⁷⁵ Respondent's response dated 21 July 2020, p 3.

¹⁷⁶ Respondent's response dated 21 July 2020 p 3.

¹⁷⁷ Respondent's response dated 21 July 2020 p 3.

that should be implemented to identify and mitigate the risks associated with the Facial Recognition Tool.

229. While the Privacy Act does not include a separate obligation to undertake a PIA, for many new projects or updated projects involving personal information, this will be a reasonable step under APP 1.2.¹⁷⁸
230. 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.
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:¹⁷⁹
- 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 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 164).
 - Noting the above factors, 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.
232. Having regard to the above factors, I consider that conducting a PIA before allowing user access to the Facial Recognition Tool, would have been a reasonable step under APP 1.2.

Preliminary findings

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 61 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, it is my preliminary view that the respondent does not take reasonable steps to implement practices, procedures and systems relating to the entity's functions or activities that would ensure that it complies with the APPs.

¹⁷⁸ 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/>

¹⁷⁹ <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/>, under 'Assessing the project's scope'.

Preliminary findings

235. I intend to recommend that the Commissioner make a declaration that the Respondent has:
- a. failed to comply with the requirement in APP 1.2 to take reasonable steps to implement practices, procedures and systems relating to the entity's functions or activities, to ensure compliance with the APPs
 - b. interfered with the privacy of individuals by failing to comply with the requirements in:
 - i. APP 3.3 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 an exception applies
 - ii. APP 3.5 to collect personal information only by lawful and fair means
 - iii. APP 5 for entities to take such steps as are reasonable in the circumstances to notify individuals of the collection of personal information
 - iv. APP 10.2 for entities to 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.

Preliminary recommendations

236. I intend to recommend that the Commissioner make the following declarations:
- a. Under s 52(1A)(a)(ii) – the respondent must not repeat or continue the acts and practices that, in my preliminary view, are an interference with the privacy of one or more individuals. In particular:
 - i. The respondent must cease to offer the Facial Recognition Tool that has been the subject of this investigation to users in Australia.
 - ii. The respondent must cease to collect Scraped Images, Probe Images, Scraped Image Vectors, Probe Image Vectors, Opt-out Image Vectors and associated Scraped URLs and Metadata from individuals in Australia in breach of APPs 3.3, 3.5 and 5.
 - b. Under s 52(1A)(b) – within 90 days of a determination made by the Commissioner, the respondent must destroy all Scraped Images, Probe Images, Scraped Image Vectors, Probe Image Vectors, Opt-out Image Vectors and associated Scraped URLs and Metadata it has collected from individuals in Australia.

Next steps

237. The respondent is invited to provide submissions and additional information in response to this preliminary view.

A handwritten signature in black ink, appearing to read "Elizabeth Hampton", with a long horizontal flourish extending to the right.

Elizabeth Hampton
Deputy Commissioner
21 May 2021

Attachment A

APP 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 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.

APP 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.

APP 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.

APP 3.5

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

APP 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.

APP 5.2

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

- a. the identity and contact details of the APP entity;
- b. if:
 - i. the APP entity collects the personal information from someone other than the individual; or
 - ii. the individual may not be aware that the APP entity has collected the personal information;
the fact that the entity so collects, or has collected, the information and the circumstances of that collection;
- c. if the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorises the collection);
- d. the purposes for which the APP entity collects the personal information;
- e. the main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;
- f. any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity;
- g. that the APP privacy policy of the APP entity contains information about how the individual may access the personal information about the individual that is held by the entity and seek the correction of such information;
- h. that the APP privacy policy of the APP entity contains information about how the individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;
- i. whether the APP entity is likely to disclose the personal information to overseas recipients;

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

Attachment B

Relevant material before the OAIC

In reaching the conclusions set out in this preliminary view, I have considered and had regard to the following:

1. Documents provided by the respondent

- a. Letter from the respondent to the OAIC dated 25 February 2020
- b. Letter from the respondent to the OAIC dated 6 March 2020
- c. Letter from the respondent to the ICO dated 21 July 2020
- d. Letter from the respondent to the ICO dated 4 August 2020
- e. Letter from the respondent to the OAIC dated 19 August 2020
- f. Letter from the respondent to the OAIC and ICO dated 26 September 2020
- g. Letter from the respondent to the OAIC and ICO dated 2 November 2020

2. Documents provided by the Australian police

- a. Letter from the AFP to the OAIC dated 21 April 2020 [redacted version]
- b. Letter from the AFP to the OAIC dated 22 May 2020
- c. Letter from the AFP to the OAIC dated 19 March 2021
- d. Letter from the Queensland Police Service (QPS) to the OAIC dated 7 August 2020 [redacted version]
- e. Letter from QPS to the OAIC dated 26 February 2021
- f. Email from Victoria Police to the OAIC, 29 June 2020, Attachment titled “1. Combined”.
- g. Victoria Police Issue Cover Sheet on the use of Clearview (undated) [redacted version]
- h. Letter from South Australia Police to the OAIC dated 14 July 2020

3. Correspondence from social media companies

- a. Letter from Twitter to the OAIC dated 9 November 2020
- b. Letter from LinkedIn to the ICO and OAIC dated 6 November 2020 [redacted version]

Attachment C



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:

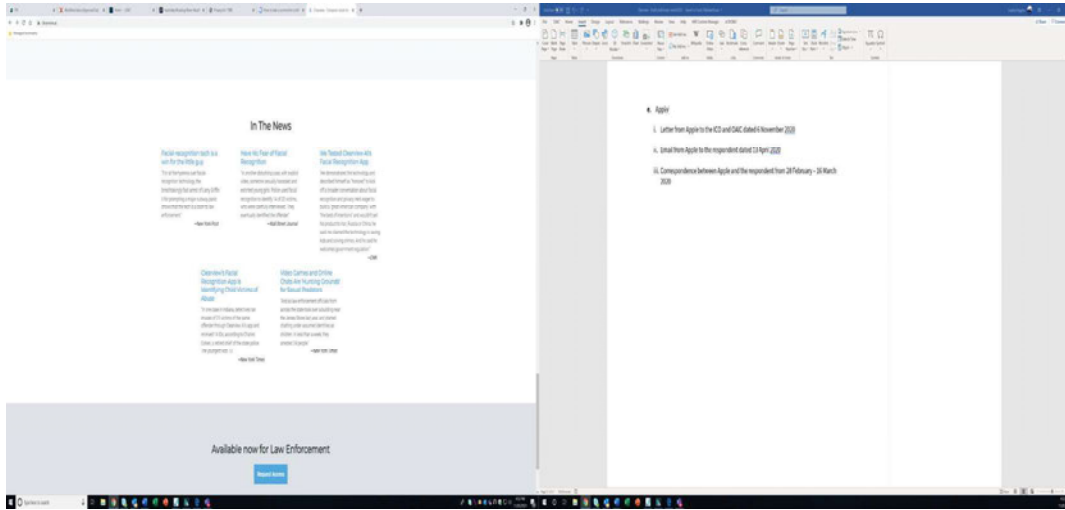
- [Illinois Opt-Out Request Form](#)

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](#)



s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 27 November 2019 2:35 PM
To: s 37
Subject: Please activate your Clearview account

Hi Senior Intelligence Analyst s 37

You have been invited to Clearview! **To activate your account please click the button below:**



It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 27 November 2019 2:39 PM
To: s 37
Subject: How to use Clearview

Hi Senior Intelligence Analyst s 37

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

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.
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.
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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER

Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.

Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.

Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.

Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.



s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 27 November 2019 2:39 PM
To: s 37
Subject: Verify your email for Clearview

Hi Senior Intelligence Analyst s 37

Welcome to Clearview, please click the link below to verify your email:

https://app.clearview.ai/confirm_email/InRheWxhaC5iYWtlckBwb2xpY2UudmljLmdvdi5hdSI.EL-BWA.lqKVs2JaFM0UJFarrzUXrH_jW28

Thanks,
Team Clearview

PS. If you have any issues or questions, just reply to this email



s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Thursday, 12 March 2020 11:10 AM
To: s 37
Subject: Login to Clearview


Hi there!

Click the button below to log in to Clearview:



Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview 

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Thursday, 12 March 2020 11:11 AM
To: s 37
Subject: Someone just logged into your Clearview account


Hi Senior Intelligence Analyst s 37

Someone logged into your account from the following device:

IP Address: s 37
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko
Browser: IE 11.0
OS: Windows 10
Device: None None

If this wasn't you, please e-mail help@clearview.ai immediately with the subject "Unauthorized Login".

Best regards,

—Team Clearview 

s 37

From: s 37
Sent: Thursday, 12 March 2020 11:35 AM
To: 'Jack M'
Subject: RE: Password change

OFFICIAL: Sensitive

Hi Jack,

I was alerted by my IT security team.
There are also lots of articles online. An example is below.
<https://www.thedailybeast.com/clearview-ai-facial-recognition-company-that-works-with-law-enforcement-says-entire-client-list-was-stolen>

I've just found how to change it. All sorted.

Thankyou.

Kind Regards,

s 37

Senior Intelligence Analyst
Joint Anti Child Exploitation Team (JACET) | Crime Command | Victoria Police
Level 6 313 Spencer St Docklands VIC 3008
P: s 37 E: s 37

From: Jack M <s 47G>
Sent: Thursday, 12 March 2020 11:30 AM
To: s 37 s 37
Subject: Re: Password change

Hello Taylah,

We'll get you a password change in a minute. First, can you tell me a little more about the security breach in question? I need more information to assess our response. How did you find out about it? Are you unable to access your account?

Regards,
Jack Mulcaire
Clearview AI

s 47G

On Wed, Mar 11, 2020 at 8:24 PM s 37 <s 37> wrote:

OFFICIAL: Sensitive

Hi,

I have been alerted to a security breach and need to change my password.

I am unable to find where to change my password.

Can you please advise where I can do this?

Thank you.

Kind Regards,

s 37

Senior Intelligence Analyst

Joint Anti Child Exploitation Team (JACET) | Crime Command | Victoria Police

Level 6 313 Spencer St Docklands VIC 3008

P: s 37 E: s 37

OFFICIAL: Sensitive

=====

EMAIL DISCLAIMER

This email and any attachments are the property of Victoria Police and should not be disclosed. They may also be subject to copyright.

If you are not an intended recipient of this email please immediately contact us by replying to this email and then delete this email. You must not read, use, copy, retain, forward or disclose this email or any attachment.

We do not accept any liability arising from or in connection with unauthorised use or disclosure of the information contained in this email or any attachment.

We make reasonable efforts to protect against computer viruses but we do not accept liability for any liability, loss or damage caused by any computer virus contained in this email.

OFFICIAL: Sensitive

s 37

From: privacy@clearview.ai
Sent: Friday, 13 March 2020 3:06 PM
To: s 37
Subject: Re: Password change

Hello Ms s 37

We apologize for the delay in response. If you still need to change your password, please email s 47G

Regards,
Clearview AI Privacy Team

—
OFFICIAL DISCLAIMER

Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.

Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.

Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.

Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.



On March 11, 2020, 7:23 PM CDT s 37 wrote:

OFFICIAL: Sensitive

Hi,

I have been alerted to a security breach and need to change my password.

I am unable to find where to change my password.

Can you please advise where I can do this?

Thank you.

Kind Regards,

s 37

Senior Intelligence Analyst

Joint Anti Child Exploitation Team (JACET) | Crime Command | Victoria Police

Level 6 313 Spencer St Docklands VIC 3008

P: s 37 E: s 37

OFFICIAL: Sensitive

=====
EMAIL DISCLAIMER

FOIREQ23/00215 -185-

This email and any attachments are the property of Victoria Police and should not be disclosed. They may also be subject to copyright.

If you are not an intended recipient of this email please immediately contact us by replying to this email and then delete this email. You must not read, use, copy, retain, forward or disclose this email or any attachment.

We do not accept any liability arising from or in connection with unauthorised use or disclosure of the information contained in this email or any attachment.

We make reasonable efforts to protect against computer viruses but we do not accept liability for any liability, loss or damage caused by any computer virus contained in this email.

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Sunday, 1 December 2019 1:44 AM
To: s 37
Subject: Your Clearview account is waiting

Hi Intelligence Analyst s 37

You have been invited to Clearview! To activate your account please click the button below:

Activate Account

<http://email.mg.clearview.ai/c/eJxVjkEOwiAURE_TLgmfj7QsWGAA49Ir0PKpmApYa6u3t4krk8nkZRYv4wOGjgB1NIKDBkAOUqLkDji16ogKwXatbdtGV5LfrZzM5OY10sZcrK_GoQqqJy3woCFwHhRRo4UKreyVA11P5ros5VmhrcRpjyvlz_Gb9o5pjQvtcOG398effZcBt0dq6tksNLrEQvaU9hclT3EgtsaBjXII7vUFVXk7tw>

It only takes one minute to install and start searching.

Remember: your password must be 8 characters and contain a number.

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 largest proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or fe

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Thursday, 5 December 2019 11:07 AM
To: s 37
Subject: How to use Clearview

Hi Intelligence Analyst s 37

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

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.
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.
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,

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Thursday, 5 December 2019 11:07 AM
To: s 37
Subject: Verify your email for Clearview

Hi Intelligence Analyst s37,

Welcome to Clearview, please click the link below to verify your email:

https://app.clearview.ai/confirm_email/lnRIZ2FuLmZvZGVuQHBvbGljZS52aWMuZ292LmF1lg.EMnbsw.ppJjvFBUoVqDHmdJnjqReYesXs

Thanks,
Team Clearview

PS. If you have any issues or questions, just reply to this email



s 37

s 22

From: help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai> on behalf of Team Clearview <help@clearview.ai>
Sent: 27 November 2019 11:19 AM
To: s 37
Subject: Verify your email for Clearview

Hi Sergeant s 37

Welcome to Clearview, please click the link below to verify your email:

https://app.clearview.ai/confirm_email/InNpbW9uLmZvZ2FydHlAcG9saWNlLnZpYy5nb3YuYXUi.EL9SjQ.uXOLvwP09-PrqF8sw2KZRZENknI

Thanks,
Team Clearview

PS. If you have any issues or questions, just reply to this email
<http://email.mg.clearview.ai/o/eJwNzEEOWiAQAMDXyHGzu0ApBy4m9h9bCkjSikHF-Ht7mttsQWfURKoGRvJE7PCULRAg3tzir8bNhnmx9mLwKBD3JH3U9AWp6h7WJCJstjhznierR13b1PCWMMevss-rhVY_2gNyK9PfvTJ5trzHBqBFKGyCfP0NzJyI>

OFFICIAL: Sensitive

s 37

s 22

From: help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai> on behalf of Team Clearview <help@clearview.ai>
Sent: 27 November 2019 11:19 AM
To: s47F, s33
Subject: How to use Clearview

Hi Sergeant s47F, s33

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

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.
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.
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

OFFICIAL: Sensitive

s 37

s 22

From: help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai> on behalf of Team Clearview <help@clearview.ai>
Sent: 28 November 2019 1:36 AM
To: Fogarty, s 37
Subject: Take a selfie with Clearview

Hi Sergeant s 37

Have you tried taking a selfie with Clearview yet? See what comes up! It's the best way to quickly see the power of Clearview in real time. Try your friends or family. Or a celebrity like Joe Montana or George Clooney.

Your Clearview account has unlimited searches. So feel free to run wild with your searches. Test Clearview to the limit and see what it can do. The photos you search with Clearview are always private and never stored in our proprietary database, which is totally separate from the photos you search.

You can get Clearview on your iPhone or Android cell phone by clicking "Get Mobile App" on the left-hand side of the screen when you're logged in to Clearview on desktop.

To log in to Clearview on desktop just click the button below:

<http://email.mg.clearview.ai/c/eJxVjcEOgyAQBb9GjhuWBcQDB9LE_wBFJMFC1Nr072vSU5OXOcxh3m xp4YTIshUcB0TRoySNBhCcE1o_pBZyRNdz10m-JZhK9PuV4xt8ZqtFPpthDlpGRSh7qTSSCYarhYZAKrBi1_NsR0euE-M939pf46dulpryk-32yFt9wIKT>

OFFICIAL: Sensitive

s 37

s 22

From: help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai> on behalf of Team Clearview <help@clearview.ai>
Sent: 29 November 2019 1:38 AM
To: s 37
Subject: Can you get to 100 searches with Clearview?

Hi Sergeant s 37

Your Clearview account has unlimited searches. Don't stop at one search. Or ten. Try to reach 100 searches with Clearview.

Investigators who do 100+ Clearview searches have the best chances of successfully solving crimes with Clearview in our experience. It's the best way to thoroughly test the technology. You never know when a search will turn up a match. It only takes 1-5 seconds to find out with Clearview, unlike other facial identification systems.

The more searches, the more matches. It's a numbers game. The investigators who search the most are the investigators who solve the most cases. Our proprietary database is the biggest in the world and gets bigger every day. Every new day means more potential results from Clearview.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview <<http://email.mg.clearview.ai/o/eJwNzE0OwiAQQOHTyHLCQP>>

OFFICIAL: Sensitive

s 37

s 22

From: help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai> on behalf of Team Clearview <help@clearview.ai>
Sent: 01 December 2019 1:42 AM
To: s 37
Subject: Refer your colleagues to Clearview

Hi Sergeant s 37

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
<http://email.mg.clearview.ai/c/eJxVzU0OgyAQQOHT6HLCzDCKCxb9ifdAQCWxxaiV9PZ12-Stvxcsj4oR62RJYyfICrUmUYAgHWrp_n_Tghu_SdpVWrwn8Et12pljApXq2EsT7wESGWPTYUGNi1K2XYIbBRF8vdj6Oda_4VIF_VUr5Nza7p1d-w5gntx3f67LmJfkIZ_Iw5RPc5we80zHs> 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.

Feel free to reach out to if you have any questions, comments, or feedback. J

OFFICIAL: Sensitive

s 47F, s 37

s 22

From: help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai> on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 27 November 2019 2:33 PM
To: s 37
Subject: Please activate your Clearview account

Hi Detective Senior Constable s 37

You have been invited to Clearview! To activate your account please click the button below:

Activate Account

<http://email.mg.clearview.ai/c/eJxVjk0LwjAQRH9NewzZbmg2hxyK4kUoeFK8LUNaBvtFbePfN-BJGIbHb7jLXYSAcpoKwkGoNISESUIEKjwbExjTK2q5kR1oeTUCzcG3lIMH8GxHCxRrQ37QAp8R0ykSGMI ndYEPngoRzvs-_ousCmqSw6v65_jN-WOc4p7yPA63F3frsOjVU_Pn7bc7LTM0bEYlp7nfGNdxuiCSNGJfkmCjy-i8DxY>

It only takes one minute to install and start searching.

Remember: your password must be 8 characters and contain a number.

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.

Feel free to reach out to if you have any questions, commen

OFFICIAL: Sensitive

s 47F, s 37

s 22

From: help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai> on behalf of Team Clearview <help@clearview.ai>
Sent: Sunday, 1 December 2019 1:43 AM
To: s 37
Subject: Your Clearview account is waiting

Hi Detective Senior Constable s37

You have been invited to Clearview! To activate your account please click the button below:



It only takes one minute to install and start searching.

Remember: your password must be 8 characters and contain a number.

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 largest proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

OFFICIAL: Sensitive

OFFICIAL: Sensitive

s 37

s 22

From: help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai> on behalf of Team Clearview <help@clearview.ai>

Sent: Monday, 2 December 2019 7:17 AM

To: s 37

Subject: How to use Clearview

Hi Detective Senior Constable s 37

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

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.
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.
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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER

Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.

Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.

Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.

Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.

OFFICIAL: Sensitive

OFFICIAL: Sensitive

s 37

s 22

From: help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai> on behalf of Team Clearview <help@clearview.ai>

Sent: Monday, 2 December 2019 7:17 AM

To: s 37

Subject: Verify your email for Clearview

Hi Detective Senior Constable s 37

Welcome to Clearview, please click the link below to verify your email:

https://app.clearview.ai/confirm_email/lm1vbmIjYS5ob2dhbkBwb2xpY2UudmljLmdvdi5hdSI.EMWxUA.2hTcGE-YYnACgA8eFBcqQEoQXjs

Thanks,
Team Clearview

PS. If you have any issues or questions, just reply to this email

OFFICIAL: Sensitive

OFFICIAL: Sensitive

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Friday, 29 November 2019 12:22 PM
To: s 37
Subject: Please activate your Clearview account

Hi None,

You have been invited to Clearview! **To activate your account please click the button below:**



It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.


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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview 

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Saturday, 30 November 2019 2:54 AM
To: s 37
Subject: Please activate your Clearview account

Hi Detective s 37

You have been invited to Clearview! **To activate your account please click the button below:**



It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.


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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview 

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Tuesday, 3 December 2019 1:46 AM
To: s 37
Subject: Your Clearview account is waiting

Hi None,

You have been invited to Clearview! **To activate your account please click the button below:**



It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

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 largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview 

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Friday, 6 December 2019 1:51 AM
To: s 37
Subject: Your Clearview account is still waiting

Hi None,

You have been invited to Clearview! **To activate your account please click the button below:**



It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

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 largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Friday, 29 November 2019 12:22 PM
To: s 37
Subject: Please activate your Clearview account

Hi None,

You have been invited to Clearview! **To activate your account please click the button below:**



It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Friday, 29 November 2019 2:46 PM
To: s 37
Subject: Verify your email for Clearview

Hi s 37

Welcome to Clearview, please click the link below to verify your email:

https://app.clearview.ai/confirm_email/lm5pY29sZS5wb3ludG9uQHBvbGljZS52aWMuZ292LmF1lg.EMlI8Q.FnBoJqjaSlbnv6zSteMIQ2gZhvQ

Thanks,
Team Clearview

PS. If you have any issues or questions, just reply to this email



s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Friday, 29 November 2019 2:46 PM
To: s 37
Subject: How to use Clearview

Hi s 37

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

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.
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.
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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER

Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.

Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.

Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.

Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.



s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Saturday, 30 November 2019 1:41 AM
To: s 37
Subject: Take a selfie with Clearview

Hi s37,

Have you tried taking a selfie with Clearview yet? See what comes up! It's the best way to quickly see the power of Clearview in real time. Try your friends or family. Or a celebrity like Joe Montana or George Clooney.

Your Clearview account has **unlimited** searches. So feel free to run wild with your searches. Test Clearview to the limit and see what it can do. The photos you search with Clearview are **always** private and **never** stored in our proprietary database, which is totally separate from the photos you search.

You can get Clearview on your iPhone or Android cell phone by clicking "Get Mobile App" on the left-hand side of the screen when you're logged in to Clearview on desktop.

To log in to Clearview on desktop just click the button below:



You can also upload a photo of yourself to Clearview on your desktop computer.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview 

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Sunday, 1 December 2019 1:43 AM
To: s 37
Subject: Can you get to 100 searches with Clearview?

Hi s 37

Your Clearview account has **unlimited** searches. Don't stop at one search. Or ten. **Try to reach 100 searches with Clearview.**

Investigators who do 100+ Clearview searches have the best chances of **successfully solving crimes** with Clearview in our experience. It's the best way to thoroughly test the technology. You never know when a search will turn up a match. It only takes 1-5 seconds to find out with Clearview, unlike other facial identification systems.

The more searches, the more matches. It's a numbers game. The investigators who search the most are the investigators who solve the most cases. Our proprietary database is the biggest in the world and gets bigger every day. Every new day means more potential results from Clearview.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview 

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Tuesday, 3 December 2019 1:46 AM
To: s 37
Subject: Refer your colleagues to Clearview

Hi s 37

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview 

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 4 March 2020 9:56 AM
To: s 37
Subject: Login to Clearview

Hi there!

Click the button below to log in to Clearview:



Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 4 March 2020 9:57 AM
To: s 37
Subject: Someone just logged into your Clearview account

Hi s37,

Someone logged into your account from the following device:

s 37

User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko

Browser: IE 11.0
OS: Windows 7
Device: None None

If this wasn't you, please e-mail help@clearview.ai immediately with the subject "Unauthorized Login".

Best regards,

—Team Clearview 

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 27 November 2019 2:35 PM
To: s 37
Subject: Please activate your Clearview account

Hi Leading Senior Constable s37,

You have been invited to Clearview! **To activate your account please click the button below:**



It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Thursday, 28 November 2019 5:19 PM
To: s 37
Subject: Verify your email for Clearview

Hi Leading Senior Constable s 37

Welcome to Clearview, please click the link below to verify your email:

https://app.clearview.ai/confirm_email/ImJlbmphbWluLnJ1dGhlcmZvcmlRACG9saWNlLnZpYy5nb3YuYXUi.EMD4SQ.9zF_x9JkpJTl4133gNYonlk9XRI

Thanks,
Team Clearview

PS. If you have any issues or questions, just reply to this email



s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Thursday, 28 November 2019 5:19 PM
To: s 37
Subject: How to use Clearview

Follow Up Flag: Follow up
Flag Status: Flagged

Hi Leading Senior Constable s 37

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

- 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.
- 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.
- 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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER

Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.

Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.

Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.

Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.



s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Thursday, 12 March 2020 11:07 AM
To: s 37
Subject: Login to Clearview


Hi there!

Click the button below to log in to Clearview:



Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview 

s47F, s33

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Saturday, 14 December 2019 01:05
To: [REDACTED]
Subject: Can you get to 100 searches with Clearview?

Hi [REDACTED]

Your Clearview account has **unlimited** searches. Don't stop at one search. Or ten. **Try to reach 100 searches with Clearview.**

Investigators who do 100+ Clearview searches have the best chances of **successfully solving crimes** with Clearview in our experience. It's the best way to thoroughly test the technology. You never know when a search will turn up a match. It only takes 1-5 seconds to find out with Clearview, unlike other facial identification systems.

The more searches, the more matches. It's a numbers game. The investigators who search the most are the investigators who solve the most cases. Our proprietary database is the biggest in the world and gets bigger every day. Every new day means more potential results from Clearview.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview



s47F, s33

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Tuesday, 11 February 2020 14:11
To: [REDACTED]
Subject: Login to Clearview

Hi there!

Click the button below to log in to Clearview:



Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,
—Team Clearview

s47F, s33

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Saturday, 14 December 2019 01:05
To: [REDACTED]
Subject: Can you get to 100 searches with Clearview?

Hi [REDACTED]

Your Clearview account has **unlimited** searches. Don't stop at one search. Or ten. **Try to reach 100 searches with Clearview.**

Investigators who do 100+ Clearview searches have the best chances of **successfully solving crimes** with Clearview in our experience. It's the best way to thoroughly test the technology. You never know when a search will turn up a match. It only takes 1-5 seconds to find out with Clearview, unlike other facial identification systems.

The more searches, the more matches. It's a numbers game. The investigators who search the most are the investigators who solve the most cases. Our proprietary database is the biggest in the world and gets bigger every day. Every new day means more potential results from Clearview.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview 

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Tuesday, 11 February 2020 14:11
To: [REDACTED]
Subject: Login to Clearview

Hi there!

Click the button below to log in to Clearview:



Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,
—Team Clearview

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Friday, 13 December 2019 01:02
To: [REDACTED]
Subject: Take a selfie with Clearview

Hi [REDACTED]

Have you tried taking a selfie with Clearview yet? See what comes up! It's the best way to quickly see the power of Clearview in real time. Try your friends or family. Or a celebrity like Joe Montana or George Clooney.

Your Clearview account has **unlimited** searches. So feel free to run wild with your searches. Test Clearview to the limit and see what it can do. The photos you search with Clearview are **always** private and **never** stored in our proprietary database, which is totally separate from the photos you search.

You can get Clearview on your iPhone or Android cell phone by clicking "Get Mobile App" on the left-hand side of the screen when you're logged in to Clearview on desktop.

To log in to Clearview on desktop just click the button below:



You can also upload a photo of yourself to Clearview on your desktop computer.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Wednesday, 11 December 2019 21:00
To: [REDACTED]
Subject: You have been invited to Clearview

Hi [REDACTED]

s 37 [REDACTED] invited you to Clearview!

To try it out for free please click the button below:




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 largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview 

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Thursday, 12 December 2019 08:29
To: [REDACTED]
Subject: How to use Clearview

Hi [REDACTED]

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

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.
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.
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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER

Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.

Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.

Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.

Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.



s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Thursday, 12 December 2019 08:21
To: [REDACTED]
Subject: Please activate your Clearview account

Hi [REDACTED]

You have been invited to Clearview! **To activate your account please click the button below:**



It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,
—Team Clearview

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Monday, 16 December 2019 01:10
To: [REDACTED]
Subject: Refer your colleagues to Clearview

Hi [REDACTED]

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview 

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Thursday, 12 December 2019 08:29
To: [REDACTED]
Subject: Verify your email for Clearview

Hi [REDACTED]

Welcome to Clearview, please click the link below to verify your email:

https://app.clearview.ai/confirm_email/InNvZm9jbGVvdXMuc2FtcEBwb2xpY2UucWxkLmdvdi5hdSI.ENL_SA.JuzrVGgEEI91iFrXwFRXgLA5yo0

Thanks,
Team Clearview

PS. If you have any issues or questions, just reply to this email



s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Saturday, 14 December 2019 01:05
To: [REDACTED]
Subject: Can you get to 100 searches with Clearview?

Hi [REDACTED]

Your Clearview account has **unlimited** searches. Don't stop at one search. Or ten. **Try to reach 100 searches with Clearview.**

Investigators who do 100+ Clearview searches have the best chances of **successfully solving crimes** with Clearview in our experience. It's the best way to thoroughly test the technology. You never know when a search will turn up a match. It only takes 1-5 seconds to find out with Clearview, unlike other facial identification systems.

The more searches, the more matches. It's a numbers game. The investigators who search the most are the investigators who solve the most cases. Our proprietary database is the biggest in the world and gets bigger every day. Every new day means more potential results from Clearview.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview



s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Thursday, 12 December 2019 08:29
To: [REDACTED]
Subject: How to use Clearview

Hi [REDACTED]

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

- 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.
- 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.
- 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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER

Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.

Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.

Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.

Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.



s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Tuesday, 11 February 2020 14:11
To: [REDACTED]
Subject: Login to Clearview

Hi there!

Click the button below to log in to Clearview:



Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,
—Team Clearview

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Thursday, 12 December 2019 08:21
To: [REDACTED]
Subject: Please activate your Clearview account

Hi [REDACTED]

You have been invited to Clearview! **To activate your account please click the button below:**



It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,
—Team Clearview

s 37

From: help@clearview.ai
Sent: Friday, 20 March 2020 09:12
To: [REDACTED]
Subject: Re: Account disabled

H [REDACTED]

We are working on bringing this back to Australian customers soon. Happy to talk on the phone.

OFFICIAL DISCLAIMER

Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.

Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.

Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.

Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.



On March 15, 2020, 11:30 PM EDT [REDACTED] wrote:

Afternoon,

I can log in successfully but when I attempt to conduct a search it says that my account is disabled.

Regards,



[REDACTED]

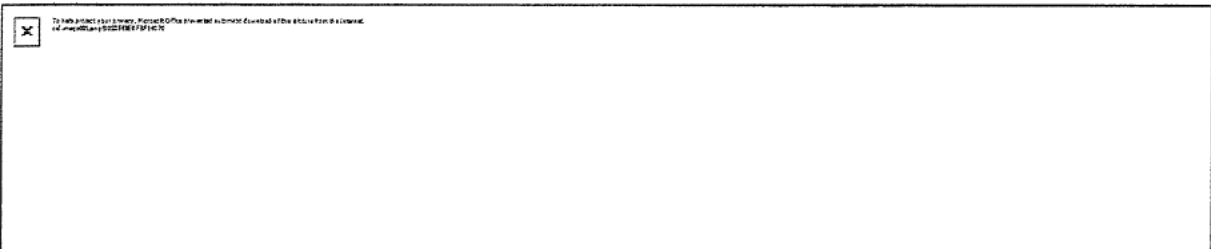
s 37

s 37

Queensland Police Service

11 Civic Parade, Logan Central Qld 4114

Phone: s 37



CONFIDENTIALITY: The information contained in this electronic mail message and any electronic files attached to it may be confidential information, and may also be the subject of legal professional privilege and/or public interest immunity. If you are not the intended recipient you are required to delete it. Any use, disclosure or copying of this message and any attachments is unauthorised. If you have received this electronic message in error, please inform the sender or contact 1300ITPSBA@psba.qld.gov.au. This footnote also confirms that this email message has been checked for the presence of computer viruses.

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Monday, 16 December 2019 01:10
To: [REDACTED]
Subject: Refer your colleagues to Clearview

Hi [REDACTED]

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview



s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Friday, 13 December 2019 01:02
To: [REDACTED]
Subject: Take a selfie with Clearview

Hi [REDACTED]

Have you tried taking a selfie with Clearview yet? See what comes up! It's the best way to quickly see the power of Clearview in real time. Try your friends or family. Or a celebrity like Joe Montana or George Clooney.

Your Clearview account has **unlimited** searches. So feel free to run wild with your searches. Test Clearview to the limit and see what it can do. The photos you search with Clearview are **always** private and **never** stored in our proprietary database, which is totally separate from the photos you search.

You can get Clearview on your iPhone or Android cell phone by clicking "Get Mobile App" on the left-hand side of the screen when you're logged in to Clearview on desktop.

To log in to Clearview on desktop just click the button below:



You can also upload a photo of yourself to Clearview on your desktop computer.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview



s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Thursday, 12 December 2019 08:29
To: [REDACTED]
Subject: Verify your email for Clearview

Hi [REDACTED]

Welcome to Clearview, please click the link below to verify your email:

https://app.clearview.ai/confirm_email/InNvZm9jbGVvdXMuc2FtcEBwb2xpY2UucWxkLmdvdi5hdSI.ENL_SA.JuzrVGgEEI91iFrXwFRXgLA5yo0

Thanks,
Team Clearview

PS. If you have any issues or questions, just reply to this email



s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Wednesday, 11 December 2019 21:00
To: [REDACTED]
Subject: You have been invited to Clearview

Hi [REDACTED]

s 37 [REDACTED] invited you to Clearview!

To try it out for free please click the button below:



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 largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview 

S 47B

S 47B

JIR/23/266

S 47B

JIR/23/267

S 47B

JIR/23/268

S 47B

JIR/23/269

S 47B

DIP/23/271

S 47B

JIR/23/272

6/25/2020

Verify your email for Clearview

help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai>

on behalf of

Team Clearview <help@clearview.ai>

Tue 12/11/2019 11:59 AM

To:

s37

Hi

s37

Welcome to Clearview, please click the link below to verify your email:

https://app.clearview.ai/confirm_email/1mRlc2lycy5hZGVsZUBwb2xpY2UucWxkLmdvdidi5hdSI.EKuivQ.Xzbh8hic9KOIWJem_EJlkdyrhUo

Thanks,

Team Clearview

PS. If you have any issues or questions, just reply to this email

6/25/2020

How to use Clearview

help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai>

on behalf of

Team Clearview <help@clearview.ai>

Tue 12/11/2019 12:01 PM

To:

s37

Hi s37

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

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.

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.

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

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER

Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.

Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.

Clearview AI is neither designed nor intended to be used as a single-source system for establishing the

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Monday, 6 January 2020 14:18
To: [REDACTED] s37
Subject: You have been invited to Clearview

[REDACTED] s37

I invited you to Clearview!

To try it out for free please click the button below:



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 largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview 

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Tuesday, 7 January 2020 00:27
To:
Subject: Please activate your Clearview account

Hi **s37**

You have been invited to Clearview! **To activate your account please click the button below:**

Activate Account

It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,
—Team Clearview

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Thursday, 9 January 2020 01:57
To:
Subject: Refer your colleagues to Clearview

Hi!

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview



Hello Han,

I am just following up on your email. Would you still like to have a discussion?

s37

Queensland Police Headquarters, 200 Roma Street, Brisbane Qld 4000 |
GPO Box 1440 Brisbane Qld 4001 Australia

From: s37
Sent: Friday, 8 November 2019 7:47 AM
To: Han T s 47G
Subject: Re: Clearview app

Hello Han,

Are you still available for a conversation today?

s37

Queensland Police Headquarters, 200 Roma Street, Brisbane Qld 4000 |
GPO Box 1440 Brisbane Qld 4001 Australia

From: s37
Sent: Thursday, 7 November 2019 3:03 PM
To: Han T s 47G
Subject: Re: Clearview app

EST huh. So it's midnight there now? You are a hard worker.

Maybe we can do 8 AM so you're not working too late.

We look for victims all over the world so all geographical locations would be useful for us, we are not just limited to Australia. Do you scrape anything in Australia?

s37

Queensland Police Headquarters, 200 Roma Street, Brisbane Qld 4000 |
GPO Box 1440 Brisbane Qld 4001 Australia

Login to Clearview

help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai>

on behalf of

Team Clearview <help@clearview.ai>

Tue 12/11/2019 11:31 AM

To: [REDACTED] s37

Hi there!

Click the button below to log in to Clearview:

 [Log in](#)

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

From: Han T s 47G
Sent: Thursday, 7 November 2019 3:00 PM
To: s37
Subject: Re: Clearview app

I'm in EST. It's a little later here. Yes, we are always adding to the database, are there any geographic locations you're looking for in particular?

Hope everything's good down under!

Best
Han

> On Nov 6, 2019, at 11:59 PM, s37 wrote:

>

> Hello Han,

>

> I would be more than happy to talk with you. I discovered your product a few weeks ago while working on a Task Force to help identify victims of child sexual abuse.

>

> I am currently trialling it to see how useful the product is to our group. The hit rate is pretty low at the moment. I see a lot of results from instagram and VK but not a lot from Facebook. Are you able to scrape Facebook or is there a limitation there? With the exception of Russia, Facebook is usually the most useful when we are looking for children worldwide.

>

> What time zone are you in? I am in UTC +10. Are you available for a talk tomorrow, Friday November 8, at about 10 AM my time?

>

> Regards

s37

> Queensland Police Headquarters, 200 Roma Street, Brisbane Qld 4000 |

> GPO Box 1440 Brisbane Qld 4001 Australia

>

>

> From: Han T s 47G

> Sent: Wednesday, 6 November 2019 11:50 PM

> To: s37

> Subject: Clearview app

>

> Hi s37

>

> I'm one of the founders of Clearview and I'm reaching out to see how your app has been going so far

>

> I grew up in Australia and you guys are our first Australian users. Let me know if you have time for a quick 5 minute call.

Please activate your Clearview account

help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai>

on behalf of

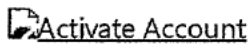
Team Clearview <help@clearview.ai>

Sat 19/10/2019 2:19 AM

To: [REDACTED] s37

H [REDACTED] s37

You have been invited to Clearview! **To activate your account please click the button below:**

 [Activate Account](#)

It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,
—Team Clearview

Your Clearview account is waiting

help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai>

on behalf of

Team Clearview <help@clearview.ai>


Tue 22/10/2019 12:09 AM

To:

Hi



You have been invited to Clearview! **To activate your account please click the button below:**

 [Activate Account](#)

It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

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 largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

How has Clearview been treating you so far?

help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai>

on behalf of

Team Clearview <help@clearview.ai>

Fri 8/11/2019 3:29 PM

To: s37

Hi s37

How has Clearview been treating you so far? Take our quick 5-minute survey to let us know! Just click the link below to begin:

<https://clearview.typeform.com/to/TdtBRX?>

name=s37 &phone=
ser_id=2f8a1065-6c1d-493a-af46-51ebab2f09a5

Your feedback will help us understand how investigators are using Clearview in the field and how we can improve Clearview so that it works even better for you.

Best,

Team Clearview

PS: If you have any issues or questions, just reply to this email or email help@clearview.ai

How to use Clearview

help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai>

on behalf of

Team Clearview <help@clearview.ai>

Tue 22/10/2019 9:49 PM

To:

Hi ^{s37}

s37

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

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.

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.

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER

Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.

Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.

Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.

Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.

Verify your email for Clearview

help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai>

on behalf of

Team Clearview <help@clearview.ai>

Tue 22/10/2019 9:49 PM

To: s37

Hi

Welcome to Clearview, please click the link below to verify your email:

https://app.clearview.ai/confirm_email/lmFuZGVyc29uLnNjb3R0QHBvbGljZS5xbGQuZ292LmF1lg.EJB-VQ.WzzCg7FZToengwC5CSkhMNtbMWQ

Thanks,

Team Clearview

PS. If you have any issues or questions, just reply to this email

Can you get to 100 searches with Clearview?

help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai>

on behalf of

Team Clearview <help@clearview.ai>

Fri 25/10/2019 12:11 AM

To:

Hi

s37

Your Clearview account has **unlimited** searches. Don't stop at one search. Or ten. **Try to reach 100 searches with Clearview.**

Investigators who do 100+ Clearview searches have the best chances of **successfully solving crimes** with Clearview in our experience. It's the best way to thoroughly test the technology. You never know when a search will turn up a match. It only takes 1-5 seconds to find out with Clearview, unlike other facial identification systems.

The more searches, the more matches. It's a numbers game. The investigators who search the most are the investigators who solve the most cases. Our proprietary database is the biggest in the world and gets bigger every day. Every new day means more potential results from Clearview.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

Take a selfie with Clearview

help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai>

on behalf of

Team Clearview <help@clearview.ai>

Thu 24/10/2019 12:10 AM

To:

Hi

s37

Have you tried taking a selfie with Clearview yet? See what comes up! It's the best way to quickly see the power of Clearview in real time. Try your friends or family. Or a celebrity like Joe Montana or George Clooney.

Your Clearview account has **unlimited** searches. So feel free to run wild with your searches. Test Clearview to the limit and see what it can do. The photos you search with Clearview are **always** private and **never** stored in our proprietary database, which is totally separate from the photos you search.

You can get Clearview on your iPhone or Android cell phone by clicking "Get Mobile App" on the left-hand side of the screen when you're logged in to Clearview on desktop.

To log in to Clearview on desktop just click the button below:

You can also upload a photo of yourself to Clearview on your desktop computer.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

Refer your colleagues to Clearview

help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai>

on behalf of

Team Clearview <help@clearview.ai>

Sat 26/10/2019 12:12 AM

To: s37

Hi

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

6/25/2020

Can you get to 100 searches with Clearview?

help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai>

on behalf of

Team Clearview <help@clearview.ai>

Thu 28/11/2019 12:36 AM

s37


Your Clearview account has **unlimited** searches. Don't stop at one search. Or ten. **Try to reach 100 searches with Clearview.**

Investigators who do 100+ Clearview searches have the best chances of **successfully solving crimes** with Clearview in our experience. It's the best way to thoroughly test the technology. You never know when a search will turn up a match. It only takes 1-5 seconds to find out with Clearview, unlike other facial identification systems.

The more searches, the more matches. It's a numbers game. The investigators who search the most are the investigators who solve the most cases. Our proprietary database is the biggest in the world and gets bigger every day. Every new day means more potential results from Clearview.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

6/25/2020

Mail

s37

Rate your Clearview experience here

help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai>

on behalf of

Team Clearview <help@clearview.ai>

Tue 21/01/2020 7:58 AM

To: s37

Hi s37

How likely are you to recommend Clearview on a scale of 1-10? Please click the link below to let us know:

[https://clearview.typeform.com/to/Pd1eoy?](https://clearview.typeform.com/to/Pd1eoy?name=/&user_id=B61403695883)

name=/&user_id=B61403695883
f5e9041-c4c7-4aa8-a35b-ff1e2b77aaf9

.B61403695883&user_id=7

Your feedback will help us understand how investigators are using Clearview in the field and how we can improve Clearview so that it works even better for you.

Thank you for using Clearview!

Best,
Team Clearview

PS: If you have any issues or questions, just reply to this email or email help@clearview.ai

6/25/2020

s 37

Please activate your Clearview account

help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai>


on behalf of

Team Clearview <help@clearview.ai>

Tue 12/11/2019 11:51 AM

s37

You have been invited to Clearview! **To activate your account please click the button below:**

 [Activate Account](#)

It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,
—Team Clearview

6/25/2020

Ma

How has Clearview been treating you so far?

help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai>

on behalf of

Team Clearview <help@clearview.ai>

Mon 9/12/2019 12:38 PM

To:

Hi .

How has Clearview been treating you so far? Take our quick 5-minute survey to let us know! Just click the link below to begin:

<https://clearview.typeform.com/to/TdtBRX?>

f5e9041-c4c7-4aa8-a35b-ff1e2b77aaf9

.695883&user_id=7

Your feedback will help us understand how investigators are using Clearview in the field and how we can improve Clearview so that it works even better for you.

Best,
Team Clearview

PS: If you have any issues or questions, just reply to this email or email help@clearview.ai

6/25/2020

Refer your colleagues to Clearview

help=clearview.ai@mg.clearview.ai <help=clearview.ai@mg.clearview.ai>

on behalf of

Team Clearview <help@clearview.ai>

Mon 18/11/2019 12:20 AM

s37

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s 37

From: [REDACTED] s 37
Sent: Friday, 10 January 2020 10:07
To: State Intelligence CPOR; State Intelligence Child Safety
Subject: Clearview facial recognition software

Follow Up Flag: Follow up
Flag Status: Flagged

Hi everyone,

<https://clearview.ai/i/FQW3>

This is a free open source tool based in the US for law enforcement only. s 47B

It says it is for a trial period but at the moment there isn't a listed end date.

Anyone hope this helps everyone.

Kind regards,

s 37

State Intelligence Group | Intelligence and Covert Services Command
200 Roma Street, Brisbane Queensland 4000
Phone: s 37
Email: [REDACTED]@police.qld.gov.au

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Sunday, 19 January 2020 17:10
To: s 37
Subject: How to use Clearview

Hi

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

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.
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.
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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER

Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.

Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.

Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.

Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.



s37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Sunday, 19 January 2020 00:14
To: [REDACTED]
Subject: Please activate your Clearview account

Follow Up Flag: Follow up
Flag Status: Flagged

Hi [REDACTED]

You have been invited to Clearview! **To activate your account please click the button below:**



It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.


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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview 

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Thursday, 23 January 2020 02:36
To: [REDACTED]
Subject: Refer your colleagues to Clearview

Hi [REDACTED]

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview 

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Wednesday, 4 March 2020 21:25
To: [REDACTED]
Subject: Someone just logged into your Clearview account

Hi [REDACTED]

Someone logged into your account from the following device:

IP Address: s 37 [REDACTED]
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko

Browser: IE 11.0
OS: Windows 10
Device: None None

If this wasn't you, please e-mail help@clearview.ai immediately with the subject "Unauthorized Login".

Best regards,

—Team Clearview



s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Sunday, 19 January 2020 17:10
To: [REDACTED]
Subject: Verify your email for Clearview

Hi [REDACTED]

Welcome to Clearview, please click the link below to verify your email:

https://app.clearview.ai/confirm_email/lmpHa292aWNraXMucGV0ZXJtQHbvbGljZS5xbGQuZ292LmF1lg.EQWSNg.YMo9fMqW0bT11EL5rW71q7CYFRc

Thanks,
Team Clearview

PS. If you have any issues or questions, just reply to this email



S 47B

DIP/23/307

S 47B

JIR/23/308

S 47B

[REDACTED] [ICSC]

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Tuesday, 14 January 2020 10:40
To: [REDACTED] s 37
Subject: Please activate your Clearview account

Hi [REDACTED]

You have been invited to Clearview! **To activate your account please click the button below:**



It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.


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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview 

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Tuesday, 14 January 2020 10:51
To: s 37
Subject: How to use Clearview

Hi [REDACTED]

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

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.
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.
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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER

Search results established through Clearview AI and its related systems and technologies are indicative and not definitive. Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system. Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.

Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.



s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Tuesday, 14 January 2020 10:51
To: s 37
Subject: Verify your email for Clearview

Hi

Welcome to Clearview, please click the link below to verify your email:

https://app.clearview.ai/confirm_email/InNwaW5rcy5zaGFubm9uQHBvbGljZS5xbGQuZ292LmF1lg.EP6h4A.Wb0hNCI2QkG0kcoLq9pPc9H4TCc

Thanks,
Team Clearview

PS. If you have any issues or questions, just reply to this email



s 37

From: [REDACTED] s 37
Sent: Tuesday, 14 January 2020 14:10
To: [REDACTED] [CSC]
Subject: <https://app.clearview.ai/app/face-search>



s 37

State Intelligence Group | Intelligence and Covert Services Command
200 Roma Street, Brisbane Queensland 4000

Phone: s 37
Email: [REDACTED]@police.qld.gov.au

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Wednesday, 15 January 2020 02:12
To: s 37
Subject: Take a selfie with Clearview

Hi [REDACTED]

Have you tried taking a selfie with Clearview yet? See what comes up! It's the best way to quickly see the power of Clearview in real time. Try your friends or family. Or a celebrity like Joe Montana or George Clooney.

Your Clearview account has **unlimited** searches. So feel free to run wild with your searches. Test Clearview to the limit and see what it can do. The photos you search with Clearview are **always** private and **never** stored in our proprietary database, which is totally separate from the photos you search.

You can get Clearview on your iPhone or Android cell phone by clicking "Get Mobile App" on the left-hand side of the screen when you're logged in to Clearview on desktop.


To log in to Clearview on desktop just click the button below:



You can also upload a photo of yourself to Clearview on your desktop computer.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview 

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Friday, 17 January 2020 02:17
To: [REDACTED] s 37
Subject: Can you get to 100 searches with Clearview?

Hi [REDACTED]

Your Clearview account has **unlimited** searches. Don't stop at one search. Or ten. **Try to reach 100 searches with Clearview.**

Investigators who do 100+ Clearview searches have the best chances of **successfully solving crimes** with Clearview in our experience. It's the best way to thoroughly test the technology. You never know when a search will turn up a match. It only takes 1-5 seconds to find out with Clearview, unlike other facial identification systems.

The more searches, the more matches. It's a numbers game. The investigators who search the most are the investigators who solve the most cases. Our proprietary database is the biggest in the world and gets bigger every day. Every new day means more potential results from Clearview.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview



[REDACTED] s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Sunday, 19 January 2020 02:24
To: [REDACTED] s 37
Subject: Refer your colleagues to Clearview

Hi [REDACTED]

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

--Team Clearview 

s 37

From: [REDACTED] s 37
Sent: Monday, 24 February 2020 15:15
To: State Intelligence Child Safety; State Intelligence CPOR
Subject: Technology & Innovation Conference - Info for you

Hey Guys,

I was lucky enough to get to go along to this today and I just wanted to pass on some of the info that I learned/picked up

[REDACTED]

[REDACTED]

[REDACTED]

s 37 [REDACTED] (Homicide) & s 37 [REDACTED] (Homicide) spoke about new Cellebrite features and facial recognition

Facial Recognition

- Nexis hub is to be accessed through the Homicide Investigators.
- QFace is the QPS Facial recognition initiative.
- Clearview is being used/trialled by a couple of areas however please use with caution. (I'm being advised that some areas are being told to cease using it until legal process has been completed – where data etc is held)

[REDACTED]

Regards



s 37

State Intelligence Child Safety | Intelligence and Covert Services Command

Address: Queensland Police Headquarters, 200 Roma Street, Brisbane

Phone: s 37

Email: [redacted]@police.qld.gov.au



AFP
AUSTRALIAN FEDERAL POLICE

Our ref: LEX20938
Your ref: CII20/00006

March 2021

Mr David Stevens
Assistant Commissioner
Office of the Australian Information Commissioner
Level 3, 175 Pitt Street
SYDNEY NSW 2000
By email: carla.wolnizer@oaic.gov.au

Dear Mr Stevens

Notice to produce information and documents in relation to Clearview AI – further response

I refer to the Notice to Give Information and/or Produce Documents dated 3 March 2020 and the AFP's previous responses dated 20 March 2020, 21 April 2020 and 22 May 2020 in relation to the Information Commissioner's investigation into the acts and practices of Clearview AI.

On 5 February 2021, the OAIC requested the AFP provide further information relating to its 21 April 2020 response. Thank you for providing further time for the AFP to respond to 22 March 2021.

Further response

The AFP has conducted further enquiries in relation to the matters raised by the OAIC. As a result of these additional enquiries and searches, the AFP provides the following further information.

Q1 **s 37**: December 2019: Searched on images of herself and another AFP member, with the consent of the other AFP member to use their image for this search. Information on the results is still to be advised."

- a. Please confirm if the search results for **s 37** and the other AFP member displayed accurate matches.
- b. If known, how many matches (including any accurate matches) resulted from these searches?

The searches displayed one accurate match for each AFP member.

Q2. s 37 Date not known s 37

s 37

Q3. s 37 December 2019: s 37

s 37

Q4. Question 4(vii) of the OAIC's notice sought 'a description of whether or not the searches involved the uploading of images of individuals located in Australia by particular staff members and/or contractors of the AFP.' The answer for s 37 stated "Yes: images of herself and s 37

- a. Please confirm if any of the search results for s 37's images displayed accurate matches.
- b. If known, how many matches (including any accurate matches) resulted from these searches?

The search displayed an accurate match for the AFP member and one of the POIs (located in Australia).

AFP responses should not be shared

The OAIC also indicated its intention to share the AFP's responses dated 21 April 2020, 22 May 2020 and this response dated 22 March 2021 (including all annexures). The AFP objects to sensitive operational information being shared. This information was provided to assist the OAIC's enquiries and not for further dissemination. The disclosure of this information could impact ongoing investigations and reveal police methodology. A redacted copy of the AFP's response dated 21 April 2020 with this information removed is attached.

Should you wish to discuss this response, please do not hesitate to contact me.

Yours sincerely

s 47E(c)

Deputy General Counsel
Information Law



AFP
AUSTRALIAN FEDERAL POLICE

Our ref: LEX20938

Your ref: CII20/00006

21 April 2020

Ms Elizabeth Hampton
Office of the Australian Information Commissioner
Level 3, 175 Pitt Street
SYDNEY NSW 2000
By email: justin.lodge@oaic.gov.au

Dear Ms Hampton

Notice to produce information and documents in relation to Clearview AI

I refer to the Notice to Give Information and/or Produce Documents dated 3 March 2020 in relation to the Information Commissioner's investigation into the acts and practices of Clearview AI. Thank you for the extension of time to respond to 17 April 2020.

Background

The Australian Centre to Counter Child Exploitation (**ACCCE**) used the Clearview AI application (the **Application**) to undertake a limited trial to ascertain its suitability for ACCCE operations.

The ACCCE is AFP-led and supports the existing efforts to counter child exploitation. The ACCCE brings together resources from government, law enforcement agencies, non-government organisations and other partners. The ACCCE drives a collaborative national response to prevent and disrupt exploitation of children, and particularly, organised child sexual exploitation networks operating in the online environment.

Offenders are often sophisticated and evolve their operating methods to avoid detection. To meet these challenges, investigators use a range of methods and tools to counter child exploitation. The effectiveness of these methods and tools is critical to modern policing. As technology advances, the ACCCE is committed to exploring new and innovative solutions to disrupt this activity, including capabilities for identifying potential offenders and victims.

The ACCCE was aware another law enforcement agency was undertaking a trial of the Application, which had led to the successful identification of a number of individuals. On that basis, the ACCCE also decided to undertake a trial of the Application to ascertain the accuracy

and effectiveness of the facial recognition algorithm. In particular, the ability of the algorithm to match side profile photographs with front facing photographs, which is a necessary function when dealing with child abuse material.

The trial was restricted to a group of investigators within the ACCCE. s 37 members created an account for the purposes of undertaking the trial, but not all accounts conducted searches and one account was not activated. It appears the vast majority of the use by AFP members concerned open source images or images of AFP members provided with their consent, for the purposes of testing the Application. Other use by AFP members for the purpose of investigating serious child exploitation offences was confined. Any searches for investigative purposes were only undertaken in the interests of protecting children (including likely imminent harm in at least one case).

This limited trial by the ACCCE is the extent of the AFP's use of the Application. The more detailed responses to the notice set out below all relate to the use of the Application by ACCCE.

The AFP is also undertaking additional enquiries to ensure it has provided all available information to the Information Commissioner, and will provide a supplementary response on or before **6 May 2020**.

The AFP is also separately reviewing the ACCCE's use of the Application in relation to the AFP's obligations under the *Privacy Act 1988* and internal governance processes.

Response to the notice

Further to the information provided by email on 20 March 2020, the AFP provides the following additional information and relevant documents.

Q1. Confirm whether the AFP have entered into a Commonwealth contract with Clearview. If so, provide a copy of the contract.

The AFP has not entered into a contract to adopt Clearview AI as an enterprise product. However, as previously advised, the Application was used by AFP members on a limited trial basis.

Q2. Confirm whether any staff member and/or contactor of the AFP has received a demonstration of the Clearview application. If so, provide the names of the staff members and/or contractors who attended or participated in the demonstration, and a description of what occurred during the demonstration, including (but not limited to) details of any searches of the Clearview application that involved the uploading of images of individuals located in Australia.

No AFP member or contractor received a demonstration of the Application.

Q3. Confirm whether any staff member and/or contactor of the AFP has received a free trial of the Clearview application.

The following s 37 AFP members received a free trial of the Application:

s 37

s 37

in the absence of the Information Commissioner accepting information on a confidential basis, the AFP has provided the unique AFP identification number for each member. This approach has also been reflected in the annexures.

Q3 cont... If so, provide any relevant documents, including (but not limited to) the terms and conditions of the free trial.

The AFP understands the trial was accessible by invitation which was sent by automated email from 'help@clearview.ai' via another law enforcement officer using the Application. This email provides a link to register a trial account (see **Annexure A**).

The AFP is undertaking enquiries to identify applicable terms and conditions of the free trial (if any) and will provide a supplementary response on or before 6 May 2020.

Q4. Provide the following information about the use of the Clearview application by staff members and/or contractors of the AFP:

i. the names and job titles of the staff members and/or contractors of the AFP that conducted searches on the Clearview application

Searches were conducted by the following AFP members:

s 37

in the absence of the Information Commissioner accepting information on a confidential basis, the AFP has provided the unique AFP identification number for each member. This approach has also been reflected in the annexures.

ii. the date/s on which staff members and/or contractors of the AFP requested access via the Clearview website

AFP members registered for a trial account by responding to an email invitation (rather than independently requesting access via the Clearview website) on the following dates:

s 37

s 37

In

the absence of the Information Commissioner accepting information on a confidential basis, the AFP has provided the unique AFP identification number for each member. This approach has also been reflected in the annexures.

iii. details of the process by which staff members and/or contractors of the AFP accessed and/or downloaded the Clearview application

The email invitation sent to AFP members contained an account creation link. Each member created their own account and then accessed the Application on the web-based interface using their own details.

iv. the date/s on which the staff members and/or contractors of the AFP used Clearview's application to search its database of images

The specific dates of searches conducted by AFP members is not known at this time.

The AFP is undertaking additional ICT searches to identify whether the AFP is able to obtain this information, and will provide a supplementary response on or before 6 May 2020. However, as previously advised, the AFP used the Application in a limited capacity between 2 December 2019 and 22 January 2020.

Further detail in relation to the use of the application is provided in response to **Q4 vi** below.

v. the number of searches of Clearview's database of images undertaken by staff members and/or contractors of the AFP

The specific number of searches conducted by AFP members is not known at this time. However, information about the nature of searches conducted is provided in response to **Q4 vi** to **viii** below.

The AFP is undertaking additional ICT searches to identify whether the AFP is able to obtain this information, and will provide a supplementary response on or before 6 May 2020.

vi. a description of the purposes for which each staff member and/or contractor of the AFP used Clearview's application

s 37

-

AFP Information

-

s 37

-

AFP Information

s 37

- December 2019: Searched on images of herself and another AFP member, with the consent of the other AFP member to use their image for this search. Information on the results obtained is still to be advised.

s 37

- December 2019: Searched on images of herself and AFP Information

s 37

- AFP Information

s 37

- Date not known: Searched on images of herself and in relation to a Nil results were obtained.

s 37

- December 2019: Searched on images of AFP Information in

There was no use of the Application by s 37.

s 37

In the absence of the Information Commissioner accepting information on a confidential basis, the AFP has provided the unique AFP identification number for each member. This approach has also been reflected in the annexures.

vii. a description of whether or not the searches involved the uploading of images of individuals located in Australia by particular staff members and/or contractors of the AFP

s 37

s 37

In the absence of the Information Commissioner accepting information on a confidential

basis, the AFP has provided the unique AFP identification number for each member. This approach has also been reflected in the annexures.

viii. if the searches did involve the uploading of images of individuals located in Australia by particular staff members and/or contractors of the AFP, provide details

As provided above at **Q4 vi**, images of AFP members were provided by the individual members themselves. [redacted] AFP Information [redacted]

These images were uploaded to match [redacted] with publicly available images in an attempt to identify the individuals. The identification of victims to prevent further victimisation and ongoing sexual abuse is the highest priority for ACCCE.

The AFP is undertaking additional ICT searches and enquiries to identify any additional details about the images uploaded to the Application, and will provide a supplementary response on or before 6 May 2020.

Q5. Provide a copy of all correspondence and/or documents that staff members and/or contractors of the AFP, sent to Clearview, or received from Clearview, including (but not limited to) email communications, marketing materials, pricing agreements, quotes, and/or invoices.

As above, a copy of the email from Clearview providing a link to register a trial account is provided at **Annexure A**. The following correspondence is also provided:

- email correspondence between **s 37** and Clearview ('Han T' and 'Hoan T') at **Annexure B**; and
- email correspondence from Clearview to **s 37** and **s 37** as well as email correspondence and documents from Clearview to **s 37** at **Annexure C**.

s 37. In the absence of the Information Commissioner accepting information on a confidential basis, the AFP has provided the unique AFP identification number for each member. This approach has also been reflected in the annexures.

Q6. Provide a copy of all file notes or other documents generated by staff members and/or contractors of the AFP, recording the results of searches made using the Clearview application.

A copy of the following documents generated by AFP members is provided:

- email correspondence between **s 37** at **Annexure D**; and
- the relevant parts of AFP case note entries generated by **s 37** at **Annexure E**.

These documents contain operational material relevant to ongoing and/or sensitive investigations and that material has been redacted. The AFP considers disclosure of this information would reveal material obtained in confidence and/or prejudice the resolution of these investigations. Accordingly, if the AFP is required to produce an unredacted copy of these documents, the AFP will arrange for safe hand delivery and requests access is confined to the Information Commissioner only, as other entries relating to this investigation are considered particularly sensitive.

Q7. Provide a copy of any electronic logs that show access and/or use of the Clearview application by staff members and/or contractors of the AFP.

The AFP does not hold any logs recording details of access and/or use of the Application by AFP members.

The AFP is undertaking additional ICT searches to identify whether the AFP holds this information and will provide a supplementary response on or before 6 May 2020.

Should you wish to discuss this response, please do not hesitate to contact me.

Yours sincerely

s 47E(d)

A/Deputy General Counsel
Information Law
Chief Counsel Portfolio

Annexure A



help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
You have been invited to Clearview

s 37

This item is expired.

Hi

s 37

Scott Anderson invited you to Clearview!

To try it out for free please click the button below:

[Try it out for free](#)

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 largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

Annexure B



Han T s 47G | s 37
Re: Connecting re: Clearview [SEC=UNOFFICIAL]

i This item is expired.
We removed extra line breaks from this message.

Great chatting s 37

Just let me know the names/emails of any colleague you want to give the app too

Let's stay in touch!

> On Dec 2, 2019, at 11:18 PM, s 37 <@afp.gov.au> wrote:
>
> UNOFFICIAL
> Hi Han,
>
> Thanks for reaching out. We've only just started using it and so far it has been valuable.
>
> I'm available anytime.
>
> Rgds
>

s 37

> COVERT ONLINE ENGAGEMENT
> AUSTRALIAN CENTRE TO COUNTER CHILD EXPLOITATION AUSTRALIAN FEDERAL
> POLICE
>
> Tel: s 37 <www.afp.gov.au>
> UNOFFICIAL
>

> -----Original Message-----
> From: Hoan T s 47G
> Sent: Tuesday, 3 December 2019 2:13 PM
> To: s 37 <@afp.gov.au>
> Subject: Connecting re: Clearview
>

> Hi Detective s 37
>
> I'm one of the founders of Clearview - and also incidentally from
> Australia, but now living in the USA
>
> How have you found the app so far? I would love to connect and learn more about how it can be used for the AFP.
>
> Let me know what time is good to chat!
>
> Best Regards
> Han
>

> *****
> WARNING
>

> This email message and any attached files may contain information that
> is confidential and subject of legal privilege intended only for
> use by the individual or entity to whom they are addressed. If you
> are not the intended recipient or the person responsible for
> delivering the message to the intended recipient be advised that you
> have received this message in error and that any use, copying,
> circulation, forwarding, printing or publication of this message or
> attached files is strictly forbidden, as is the disclosure of the
> information contained therein. If you have received this message in
> error, please notify the sender immediately and delete it from your
> inbox.
>
> AFP Web site: <http://www.afp.gov.au>
> *****

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Wednesday, 4 December 2019 11:52 AM
To: s 37
Subject: How to use Clearview

Hi s 37

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

- 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.
- 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.
- 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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER

Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.

Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.

Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.

Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Thursday, 5 December 2019 12:27 AM
To: s 37
Subject: Please activate your Clearview account

Hi s 37

You have been invited to Clearview! **To activate your account please click the button below:**

Activate Account

It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,
—Team Clearview

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Wednesday, 4 December 2019 11:55 AM
To: s 37
Subject: You have been invited to Clearview

Hi s 37

s 37 invited you to Clearview!

To try it out for free please click the button below:

Try it out for free

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 largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview <help@clearview.ai>
Sent: Wednesday, 18 December 2019 1:14 AM
To: [REDACTED]
Subject: Take a selfie with Clearview

Hi [REDACTED]

Have you tried taking a selfie with Clearview yet? See what comes up! It's the best way to quickly see the power of Clearview in real time. Try your friends or family. Or a celebrity like Joe Montana or George Clooney.

Your Clearview account has **unlimited** searches. So feel free to run wild with your searches. Test Clearview to the limit and see what it can do. The photos you search with Clearview are **always** private and **never** stored in our proprietary database, which is totally separate from the photos you search.

You can get Clearview on your iPhone or Android cell phone by clicking "Get Mobile App" on the left-hand side of the screen when you're logged in to Clearview on desktop.

To log in to Clearview on desktop just click the button below:



You can also upload a photo of yourself to Clearview on your desktop computer.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

[Redacted] s 37

From: Jessica G [Redacted] s 47G
Sent: Thursday, 19 December 2019 1:07 PM
To: [Redacted] s 37
Subject: cv
Attachments: Clearview_Search_Tips.pdf; Success Stories.pdf

Good evening. You should have an email from Team Clearview with your account activation link. I encourage you to test the tech on computer/laptop (log in thru <https://app.clearview.ai/app/login>) and the mobile app. Also attached is general info and sample success stories and a doc with some tips on how to best use photos. If you would find a video demo call helpful just let me know. Finally – if there are any other officers/agents that would like an account just send me names and emails.

Please do not hesitate to contact me with any questions.

- Jess

Jessica Medeiros Garrison
205.568.4371

[Redacted] s 47G

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Monday, 9 December 2019 11:02 AM
To: s 37
Subject: Verify your email for Clearview

Hi s 37

Welcome to Clearview, please click the link below to verify your email:

https://app.clearview.ai/confirm_email/Im5pY29sZS53YXRraW5zQGFmcC5nb3YuYXUi.EM8ujw.cGPF5ahClGV-W-chZrhuPWcdNPs

Thanks,
Team Clearview

PS. If you have any issues or questions, just reply to this email

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Monday, 9 December 2019 11:02 AM
To: s 37
Subject: How to use Clearview

Hi s 37

You should have a setup email in your inbox shortly. It only takes one minute to install and start searching.

Here are three important tips for using Clearview:

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.
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.
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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Finally, please note the disclaimer at the bottom.

Best regards,

— Team Clearview

OFFICIAL DISCLAIMER

Search results established through Clearview AI and its related systems and technologies are indicative and not definitive.

Clearview AI, Inc. makes no guarantees as to the accuracy of its search-identification software. Law enforcement professionals MUST conduct further research in order to verify identities or other data generated by the Clearview AI system.

Clearview AI is neither designed nor intended to be used as a single-source system for establishing the identity of an individual.

Furthermore, Clearview AI is neither designed nor intended to be used as evidence in a court of law.

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Monday, 9 December 2019 10:36 AM
To: s 37
Subject: Please activate your Clearview account

Hi s 37

You have been invited to Clearview! **To activate your account please click the button below:**

Activate Account

It only takes **one minute** to install and start searching.

Remember: your password must be 8 characters and contain a number.

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.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,
—Team Clearview

s 37

From: help=clearview.ai@mg.clearview.ai on behalf of Team Clearview
<help@clearview.ai>
Sent: Monday, 9 December 2019 9:01 AM
To: s 37
Subject: You have been invited to Clearview

Hi s 37

s 37 invited you to Clearview!

To try it out for free please click the button below:



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 largest** proprietary database of facial images to help you find the suspects you're looking for.

Feel free to reach out to if you have any questions, comments, or feedback. Just reply to this e-mail or contact help@clearview.ai

Best regards,

—Team Clearview

What is Clearview? Clearview's mission is to drastically reduce crime, fraud and risk in order to make communities safer and commerce secure.

Clearview provides law enforcement a revolutionary facial search engine. From a single image it can instantly and accurately return photos matching that face from the Internet and other publicly available sources.




Paul Clement Legal Implications Briefing Counsel to Clearview

KIRKLAND & ELLIS LLP

MEMORANDUM

TO: Clearview AI, Inc.

FROM: Paul D. Clement Esq. 

DATE: August 14, 2019

RE: Legal Implications of Clearview Technology

Clearview is an investigative application that uses state-of-the-art facial-recognition technology to match the face in a user-uploaded image to faces in publicly available images. It is designed to be used in ways that ultimately reduce crime, fraud, and risk in order to make communities safer. This memorandum analyzes the potential legal implications of Clearview's use by public entities as an investigative tool. We conclude, based on our understanding of the product, that law enforcement agencies do not violate the federal Constitution or relevant existing state biometric and privacy laws when using Clearview for its intended purpose. Moreover, when employed as intended, Clearview's effective and evenhanded facial-recognition technology promotes constitutional values in a manner superior to many traditional identification techniques and competing technologies.

**Entire Memo - Attachment "A"*

(Pew, 9/19)

Trust in the Law...

Percentage of Americans who say they trust these groups to use facial recognition technology responsibly

A great deal
 Somewhat
 Not too much
 Not at all

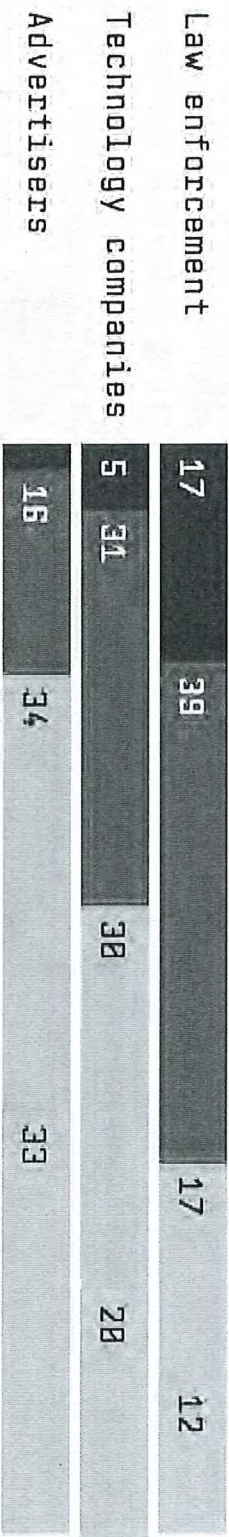
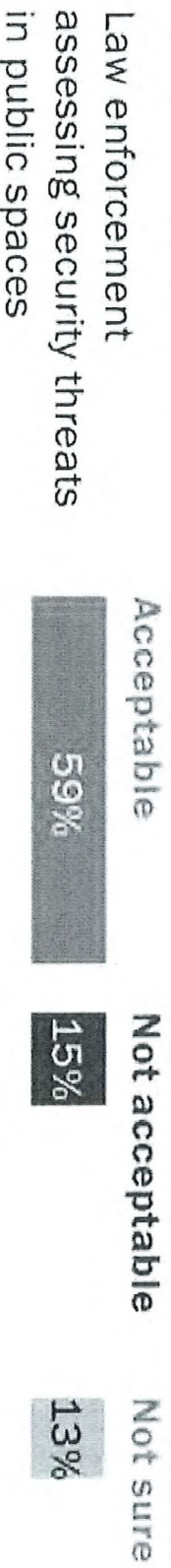


CHART: VIDEO - SOURCE: PEW RESEARCH CENTER

Majority of Americans find it acceptable for law enforcement to use facial recognition to assess threats in public spaces

% of U.S. adults who say the use of facial recognition technology in the following situations is ...



Accuracy Test Report

In October 2019, the undersigned Panel conducted an independent accuracy test of Clearview AI.. For the purposes of this analysis, the Panel used the same basic methodology used by the American Civil Liberties Union (ACLU) in its July 2018 accuracy test of Amazon's Rekognition technology.

The ACLU's approach entailed comparing photographs of all 535 members of the U.S. House of Representatives and Senate against a database of 25,000 arrest photos. The test resulted in 28 members of Congress being incorrectly matched to arrestees from the photo database.

With those important concerns in mind, the Panel conducted the same test of Clearview. **Along with analyzing all 535 members of Congress, the Panel also analyzed all 119 members of the California State Legislature and 180 members of the Texas State Legislature, for good measure.**

The test compared the headshots from all three legislative bodies against Clearview's proprietary database of 2.8 billion images (112,000 times the size of the database used by the ACLU). The Panel determined that Clearview rated 100% accurate, producing instant and accurate matches for every one of the 834 federal and state legislators in the test cohort.

Conducted Independently By:



Hon. Jonathan Lippman

Nicholas Cassimatis, PhD

Aaron M. Renn

- Judge Lippman served as Chief Judge of the State of New York from 2009 to 2015....
- Nicholas Cassimatis is former Chief of Samsung's North American AI Research
- Aaron Renn is a Senior Fellow at the Manhattan Institute

In late 2018, the Clearview team began testing its technology's capability to solve crimes by scanning images pulled from news reports about persons of interest.

On September 24, 2018, **The Gothamist** published a photo of a man who assaulted two individuals outside a bar in Brooklyn, NY.

Two Men Assaulted After Leaving Williamsburg Gay Bar
BY BEN CHING | 9:45 AM, SEP 24, 2018 | 10/10/18



Using Clearview, we instantly identified the assailant and sent the tip to the police, who confirmed his identity.



Clearview begins to launch pilot programs with law enforcement.

Detectives begin breaking unsolved cases involving pedophiles, credit-card fraud, sexual harassment, ATM theft and hate-crimes.

Here are some of their stories...

S 47F

NEW YORK (AP) — Three abandoned devices that looked like pressure cookers caused an evacuation of a major New York City subway station and closed off an intersection in another part of town Friday morning before police determined the objects were not explosives.

Police were looking to talk to a man seen on surveillance video taking two of the objects — one out of a shopping cart and placing them in a subway lower Manhattan. In photos released by authorities, the young man is seen standing by a pressure cooker and then lugging a cooker in.

But police stressed that so far, it wasn't clear whether he was trying to frighten people by throwing the objects away.

"I would stop very short of calling him a suspect," said John Miller, the New York Police Department's top counterterrorism official. "It is possible that somebody put out a bunch of items in the cash today and this guy plucked them up and then discarded them, or it's possible that this was an intentional act."

Earlier, Gov. Andrew Cuomo had said authorities suspected the items were placed in the subway

S 47F

S 47F

NOTE ON BOMB SCARES

Van loaded with 1,000 gallons of gas forces Baltimore evacuation

Panic erupts at Newark City pressure cooker scare

Larry Griffin II, 26, was charged with making a \$200,000 bond following his arraignment on Sunday.

Fulton Street subway station Friday was ordered panic by scattering a pair of rice cooker bombs in subway held on

S 47F

NYC Bomb Scare

<https://www.youtube.com/watch?v=JqA9cPJU04> Click here to see News Coverage

Police seek to question man in NYC rice cooker bomb scare

JENNIFER PELTZ August 16, 2019

West Virginia Man Sought by NYPD After 3 Hours of Manhattan Spark Rush-Hour Scare

Jonathan Blum

A report of the first two items at the Fulton Street subway station Friday was ordered panic by scattering a pair of rice cooker bombs in subway held on

NEW YORK

Home News Weather Investigations Entertainment

www.nbcnewyork.com

Man accused of placing fake rice cooker bombs in subway held on

AP

S 47F

Financial Fraud

Vineland Police: Fraud suspect pretended to be car salesman

VINELAND – Police announced the arrest of a man who allegedly committed fraud by selling rented cars as his own. [REDACTED] was arrested on Nov. 15. At the time of his arrest, according to reports, he was found in possession of numerous documents that lead investigators to believe there are additional victims in the South Jersey area...Mero would rent vehicles from a local car rental agency and attempt to sell them to residents, accepting down payments and deposits from the victims. [REDACTED] Also allegedly took potential victims to car dealerships after hours on Sundays, claiming to be a salesperson.

s 37

[REDACTED] was identified using Clearview when a BOLO was disseminated using a pnuu from one of the victims. [REDACTED] had been released from federal prison in November 2018, serving time for fraud, and made his way to Raleigh. Total Loss Exposure was \$191,536.46 with 15 known victims. On June 3, 2019, US Marshal TFO [REDACTED] and the US Marshals located and arrested [REDACTED] in Henderson, NC. Mero was wanted on an outstanding federal probation warrant and several financial crimes warrants. The interview with Mero also elicited incriminating statements as well as his consent to examine his cell phone. Initial review of the cell phone found not only incriminating information to his fraudulent activity but child pornography.

- False Pretense
- Credit Card Theft
- Identity Theft
- Second Degree Sex
- Exploitation of Minor x 12

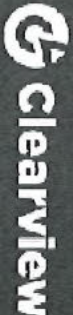
Mailbox Theft

Mail theft is a big problem in the Atlanta area. Detective [REDACTED] identifying a mailbox theft suspect. One potential victim, in a heavily run area, installed a camera in his mailbox. When the suspect opened the mailbox, he did not get out of the car to retrieve the mail but just leaned into the mailbox. This allowed the camera to capture a full frontal facial image. The detective ran the image through Clearview. This produced positive identification based on definitive tattoos on the suspect's shoulder. Clearview returned a 10 year old mugshot and social media photos that corroborated the other evidence on file.

S 47F

S 47F

S 47F



Crimes Against Children

S 47F

Las Vegas, Nevada – A federal Child Exploitation Investigations Unit had been investigating a major child pornography/exploitation case in Las Vegas. They were reviewing a series of 14 photographs. Two photos included the image of a John Doe in the background. Agents searched the face against available criminal databases and found nothing. A subsequent search of the image through Clearview enabled the investigators to quickly identify the man. This was a major break in this case.

S 47F

Crimes Against Children

Birmingham, Alabama – the images below were used in identifying a John Doe suspect in a child enticement case.

S 47F

Grand Theft / Forgery

S 47F

This female suspect alluded law enforcement for several years and was wanted for 17 counts of forgery. Using Clearview, the Sergeant received intelligence that led to her identification and the fact that she was returning from a trip to the Bahamas courtesy of the return ticket she had posted in a photo. The investigator notified TSA, customs and the airline. The suspect was arrested at the gate. Criminal prosecution is pending.

S 47F

^{s 47F} unit assists multiple departments with identifying suspects of crimes ranging from drugs, prostitution and theft. In his words, "Great product! Every investigator should have this as a tool". - Sergeant Juan Balceiro, Crime Suppression Unit, Miami Beach Police Department

S 47F

Pedophile

- Law enforcement was unable to identify this suspect in a NY child pedophile investigation.
- Using Clearview, they matched the facial image to a tax professional through a public website.
- After follow-up investigation, he was arrested six days later.

S 47F

Deceased John Doe

This John Doe victim was found shot on a sidewalk. The officer used the Clearview app to receive information leading immediately to his identity.

S 47F

Jacks Fast Food Robbed by masked gunman. When the suspect was arrested, he was still in possession of the Regions Bank bag the money was placed in during the robbery.

Robbery

S 47F

S 47F

RAPID INTERNATIONAL EXPANSION





Clearview AI

Stop Searching. Start Solving.



Clearview Search Tips

Potential Causes of Reduced Accuracy for Clearview Facial Recognition Technology

Clearview is an investigative software application that uses state-of-the-art facial- recognition technology to match a face in a user-uploaded image to a face in publicly available images. It is designed to be used in ways that ultimately reduce crime, fraud, and risk in order to make communities safer. Clearview's technology is designed with the utmost attention to accurate and unbiased match-generation.

The following factors can inhibit facial recognition technology from making accurate facial matches. All of these factors concern characteristics of the image that is input by the user (the "probe image") and in some way obscure or disrupt algorithmic analysis of the features of the person the user is attempting to identify (the "search subject"). Searches which are affected by one or more of these factors are more likely to result in search results which do not facilitate accurate identification of image subjects, although accurate results are still sometimes possible when searching images that are affected by these factors. The human operators of Clearview's search technology must follow Clearview's user guidelines and use their law enforcement training to determine the accuracy of all search results.

The most common confounding factors include:

1) Low-Resolution Probe Images

Probe images must have sufficiently high resolution in the facial area of the search subject to allow the facial recognition algorithm to identify and match specific features. Low resolution images, with high pixelation in the face region of the subject, cannot consistently support accurate facial matching. Low resolution probe images may result from the inherent limitations on the resolution of the

camera which took the source image, motion blur, or may result from other conditions such as the distance between the search subject and the camera which took the probe image.

2) Image and Video “Noise” in Probe Image

Just as inherent low resolution can prevent inaccurate matches, “noisy” imagery containing motion blurs and atmospheric interference will result in pixelated and/or blurred facial features for the search subject which frustrates the operation of the facial feature identification and matching algorithm.

3) Poor Lighting Conditions in Probe Images

The facial area of the search subject must be sufficiently well-lit in the probe image to allow the facial recognition algorithm to identify and match specific features. Probe images which do not contain a sufficiently well-lit facial area will not produce accurate search results because the facial features are not sufficiently visible for algorithmic identification.

4) High Camera Pitch Angle Probe Images

Many cameras, such as roof and ceiling-mounted security cameras, and cameras on airborne platforms, produce images which look down on the search subject from a high “pitch”, or transverse, angle. When used as a probe images, cameras that are at a high pitch/transverse angle to the search subject’s face will produce accurate matches at significantly lower rates, because many facial features are not visible from a high transverse angle, and because transposing features to match them with photos taken at a low transverse angle is difficult to accomplish algorithmically.

5) Monitor Screen Artifacts in Probe Images

Some users display an image of the search subject on an LCD monitor and then take a photo of that image with their mobile device, using this photo as the probe image in a search in the mobile app version of Clearview. This often results in artifacts, including visible resolution cells, in the probe image, which prevents accurate algorithmic detection and matching of facial features. To prevent this problem, users should not resort to the “photo of a screen” technique, and should

instead directly upload images from their computers to the web browser version of Clearview.

6) Ancillary/Background Features in Probe Image

Probe images that contain conspicuous background objects and patterns that overlap with the facial area of the search subject can result in inaccuracies in the search results returned by Clearview. This problem can be mitigated in some cases by cropping background objects out of the image.

7) Hats, Glasses and Other Face-Covering Objects

Objects, most commonly items of clothing like hats or sunglasses, which partially or totally obscure the face of the search subject will reduce the likelihood of an accurate match.

Users searching images that are affected by one or more of these factors should exercise additional scrutiny and caution when analyzing the search results, and should expect lower rates of successful identification when using probe images that are characterized by one or more of these factors.

ISSUE COVER SHEET

File No:

Issue:

Update regarding JACET use of Clearview AI online facial recognition tool and identified security breach of Clearview servers.

Background:

In November 2019 I delivered training at the Covert Online Investigation Course facilitated by The European Union Agency for Law Enforcement Training (CEPOL) in Hungary. There were other presenters from Europe, The USA and Canada. Topics delivered covered all aspects of covert online Investigations including open source searching and online tools. The presenters all work in the child exploitation field and are considered experts in their jurisdictions.

During one of the presentations from the Toronto Police Service, a demonstration was given of an online service called Clearview AI. Clearview AI is a tool that provides facial recognition capabilities and searches open source images scraped from social networking sites such as Facebook, Instagram and Google etc, and compares these images against an image uploaded by the user. The hope is to get a matching or similar image to provide information regarding the source of the image or name of the profile the image was located at. The images contained in Clearview are all sourced from publicly available images and none of the images are sourced from private social networking accounts. This tool is not dissimilar to other applications such as Google reverse image searches that are regularly used by LEA. Toronto Police and other LEA's have successfully used this application to identify and rescue children from child sexual abuse.

It was explained during the demonstration that the Clearview AI server is split into two areas. The first area is where the scraped data is stored for searching against. The second area is an encrypted area that houses your image upload to compare against the database. It was further explained that this data cannot be seen by Clearview AI and is deleted from the secure server once you log off. The demonstration included a visual display of the searching capabilities of the tool. Discussion was had at this point as to how beneficial this tool could be to assist in the identification of unidentified child victims.

Upon returning to the JACET, in my role as the research and training sergeant, I provided an overview to members from the Intelligence Team, Victim Identification Team and the Proactive Engagement Team who all saw benefit in its use. To access the tool the user must first register using their LEA email address. The use of Clearview AI by JACET members was only for intelligence purposes and would in no way form part of a prosecution. The software was to assist in the identification of unknown children by locating social networking profiles that may have links to their real identities. It is imperative the JACET conduct research and training into tools such as this to establish possibilities and opportunities to enhance our capabilities and identify unknown children at risk of sexual abuse.

Trials undertaken by _____ and me resulted in initial success, however subsequent searches by _____ during investigations were unsuccessful and the application therefore was not used any further. During the use of the application there were both open source images uploaded and there was also cropped images depicting the faces of unknown child victims. At no stage was any child abuse material uploaded to the service.

On 12-Mar-2020 I received an email from I.T. Security Team, Security and Management Services advising that there had been a Clearview AI data breach. The advice given at that time was to:

- Change your passwords wherever this password or a combination based on this password is currently being used.
- You must refrain from using this password or a combination based on this password in the future.

At no point were we told not to further use this application. I have subsequently conducted an audit of the use of Clearview AI and given instructions via email for JACET members to stop using the application pending further advice from VicPol command and the I.T Security Team.

It has been identified that the following seven members from JACET created accounts and conducted the following activities:

NAME:	ACCOUNT CREATION DATE:	SEARCHES:	SEARCH PRE / POST BREACH:
	27-Nov-2019	2 test searches using open source images	Pre
	02/12/2019	Nil	N/A
	05-DEC-2019	Nil	N/A
	27-Nov-2019	Nil	N/A
	29-Nov-2019	Nil	N/A
	29-Nov-2019	10 approximately to test software capability	Pre
	27-Nov-2019	Nil	N/A

JACET have commenced an audit of all software used in the covert environment to identify any possible risks in the use of these applications.

Comment:

For information of JACET management regarding use of Clearview AI and for clarification of use of this application in future investigations.

Recommendation:

Date:

1.

<Date>

From: [Sophie Higgins](#)
To: [Wendy Tian](#); [Justin Lodge](#)
Cc: [Emi Christensen](#); [Karin Van Eeden](#)
Subject: Fwd: Correspondence from the UK ICO and OAIC [SEC=OFFICIAL]
Date: Monday, 24 May 2021 8:50:31 AM
Attachments: [image001.jpg](#)
[image002.png](#)
[image003.png](#)
[image004.png](#)
[image005.png](#)

Get [Outlook for iOS](#)

From: Jack Mulcaire <[s 47G](#)>
Sent: Friday, May 21, 2021 11:48:37 PM
To: Sophie Higgins <sophie.higgins@oaic.gov.au>
Subject: Re: Correspondence from the UK ICO and OAIC [SEC=OFFICIAL]

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Dear Sophie,

Thank you for your letter, we will review and respond appropriately with a submission by June 3rd.

Regards

Jack Mulcaire

Counsel, Clearview AI

[s 47G](#)

On Wed, May 19, 2021 at 10:26 PM Sophie Higgins <sophie.higgins@oaic.gov.au> wrote:

Dear Jack Mulcaire,

I refer to the joint investigation by the UK Information Commissioner's Office and the Office of the Australian Information Commissioner into the acts or practices of Clearview AI Inc.

Please find attached a letter regarding the matter.

Yours sincerely,



Sophie Higgins | Director

Dispute Resolution Branch

Office of the Australian Information Commissioner

GPO Box 5218 Sydney NSW 2001 | oaic.gov.au

02 9284 9775 | sophie.higgins@oaic.gov.au



 [Subscribe to Information Matters](#)



Justin Lodge | A/g Director

Dispute Resolution Branch

Office of the Australian Information Commissioner

GPO Box 5218 Sydney NSW 2001 | oaic.gov.au

+61 2 8231 4203 | Justin.Lodge@oaic.gov.au



 [Subscribe to OAICnet newsletter](#)

David Reynolds

Lead Case Officer

Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

T. s 47F F. 01625 524510 ico.org.uk twitter.com/iconews

Please consider the environment before printing this email

For information about what to do with personal data see our [privacy notice](#)

WARNING: The information contained in this email may be confidential.
If you are not the intended recipient, any use or copying of any part
of this information is unauthorised. If you have received this email in
error, we apologise for any inconvenience and request that you notify
the sender immediately and delete all copies of this email, together
with any attachments.

FOIREQ23/00215 -374-

From: [Sophie Higgins](#)
To: [Wendy Tian](#); [Justin Lodge](#); [Emi Christensen](#)
Subject: FW: Investigation under s40(2) of the Privacy Act 1988 (Cth) [BAL-M.CLEA0009.200240] [SEC=OFFICIAL]
Date: Thursday, 10 June 2021 10:26:32 AM
Attachments: [image001.png](#)
[Letter to OAIC.pdf](#)
[image002.jpg](#)
[image003.png](#)
[image004.png](#)
[image005.png](#)
[image006.png](#)



Sophie Higgins | Director
Dispute Resolution Branch
Office of the Australian Information Commissioner
GPO Box 5218 Sydney NSW 2001 | oaic.gov.au
02 9284 9775 | sophie.higgins@oaic.gov.au



[Subscribe to Information Matters](#)

From: Colletta Nyamambi <Colletta.Nyamambi@ballawyers.com.au>
Sent: Thursday, 10 June 2021 10:25 AM
To: Sophie Higgins <sophie.higgins@oaic.gov.au>
Subject: Investigation under s40(2) of the Privacy Act 1988 (Cth) [BAL-M.CLEA0009.200240]

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Dear Sophie,

Matter reference: 200240

Please find **attached** our letter to you of even date.

Kind regards,

COLLETTA NYAMAMBI
EXECUTIVE ASSISTANT
BUSINESS & CORPORATE

[P02 6274 0921](tel:0262740921)



Level 9 Canberra House, 40 Marcus Clarke St. Canberra ACT 2601
GPO Box 240 Canberra ACT 2601 | DX 5626 Canberra

BALLAWYERS.COM.AU | [LINKED IN](#) | [TWITTER](#)

NOTICE: Please notify us on 02 6274 0999 if his communication has been sent to you by mistake.
If it has been, Client Legal Privilege is not waived or lost and you are not entitled to use it in any way.
Please consider the environment before printing this email.

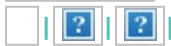
FOIREQ23/00215 -375-


From: [Sophie Higgins](#)
To: [Wendy Tian](#)
Subject: FW: Investigation under s40(2) of the Privacy Act 1988 (Cth) [SEC=OFFICIAL]
Date: Thursday, 17 June 2021 5:01:16 PM
Attachments: [image001.png](#)
[image002.jpg](#)
[image003.png](#)
[image004.png](#)
[image005.png](#)
[image006.png](#)
[2021-06 Letter to Clearview.pdf](#)

Could you please save to the files when you have a sec?



Sophie Higgins | Director
Dispute Resolution Branch
Office of the Australian Information Commissioner
GPO Box 5218 Sydney NSW 2001 | oaic.gov.au
02 9284 9775 | sophie.higgins@oaic.gov.au



 [Subscribe to Information Matters](#)

From: Sophie Higgins
Sent: Thursday, 17 June 2021 5:01 PM
To: Mark Love <Mark.Love@ballawyers.com.au>
Cc: Wendy Tian <wendy.tian@oaic.gov.au>; Justin Lodge <justin.lodge@oaic.gov.au>
Subject: Investigation under s40(2) of the Privacy Act 1988 (Cth) [SEC=OFFICIAL]

Dear Mr Love

OAIC reference: CI120/00006

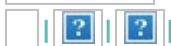
Please find attached a letter from the OAIC Assistant Commissioner dated 17 June 2021.


Kind regards

Sophie



Sophie Higgins | Director
Dispute Resolution Branch
Office of the Australian Information Commissioner
GPO Box 5218 Sydney NSW 2001 | oaic.gov.au
02 9284 9775 | sophie.higgins@oaic.gov.au



 [Subscribe to Information Matters](#)

From: Colletta Nyamambi <Colletta.Nyamambi@ballawyers.com.au>
Sent: Thursday, 10 June 2021 10:25 AM
To: Sophie Higgins <sophie.higgins@oaic.gov.au>

Subject: Investigation under s40(2) of the Privacy Act 1988 (Cth) [BAL-M.CLEA0009.200240]

CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Dear Sophie,

Matter reference: 200240

Please find ***attached*** our letter to you of even date.

Kind regards,

COLLETTA NYAMAMBI
EXECUTIVE ASSISTANT
BUSINESS & CORPORATE

P [02 6274 0921](tel:0262740921)



Level 9 Canberra House, 40 Marcus Clarke St. Canberra ACT 2601
GPO Box 240 Canberra ACT 2601 | DX 5626 Canberra

BALLAWYERS.COM.AU | [LINKED IN](#) | [TWITTER](#)

NOTICE: Please notify us on 02 6274 0999 if his communication has been sent to you by mistake.
If it has been, Client Legal Privilege is not waived or lost and you are not entitled to use it in any way.
Please consider the environment before printing this email.

FOIREQ23/00215 -377-

From: [Wendy Tian](#)
To: mark.love@ballawyers.com.au
Cc: s 47G [Sophie Higgins](#)
Subject: CII20/00006: Commissioner initiated investigation into Clearview AI, Inc. [SEC=OFFICIAL]
Date: Thursday, 14 October 2021 3:55:00 PM
Attachments: [2021-10 Letter to BAL Lawyers re Clearview determination.pdf](#)
[Commissioner initiated investigation into Clearview AI, Inc. \(Privacy\) \[2021\] AICmr 54 \(14 October 2021\).pdf](#)
[image001.jpg](#)
[image002.png](#)
[image003.png](#)
[image004.png](#)
[image005.png](#)

Dear Mr Love

I refer to the Commissioner initiated investigation into Clearview AI, Inc. Please see the attached letter and determination, dated today.

I would be grateful if you could confirm receipt of this email and the attachments.

Kind regards



Wendy Tian | Assistant Director
Dispute Resolution Branch
Office of the Australian Information Commissioner
GPO Box 5218 Sydney NSW 2001 | oaic.gov.au
+61 2 8231 4213 | wendy.tian@oaic.gov.au



[Subscribe to Information Matters](#)



Australian Government
Office of the Australian Information Commissioner



Our reference: CII20/00006

Clearview AI, Inc.
By its Proper Officer
c/o Mark Love, Legal Director, BAL Lawyers

By email: mark.love@ballawyers.com.au

cc: **s 47G**

■

Commissioner Initiated Investigation into Clearview AI, Inc.

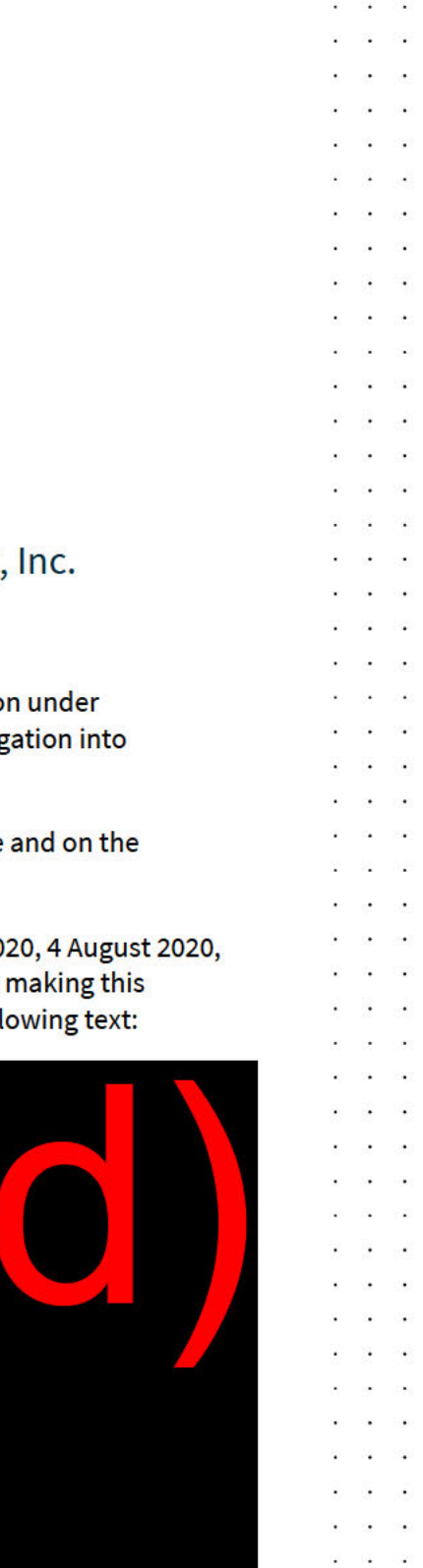
Dear Mr Love,

I am writing to advise you that the Commissioner has made a determination under [s 52\(1A\)](#) of the *Privacy Act 1988* (Cth), following the Commissioner’s investigation into Clearview AI, Inc. under [s 40\(2\)](#) of the Act. The determination is attached.

As previously advised, determinations are published on the OAIC’s website and on the AustLII website. The attached determination will be published online.

The confidentiality claims in your client’s correspondence dated 21 July 2020, 4 August 2020, 26 September 2020, 2 November 2020 and 3 June 2021 were considered in making this determination. Before publishing the determination, we will redact the following text:

s 47E(d)



S 47E(d)

If you have concerns regarding the inclusion of any personal information in the determination, or there are any legal requirements that you need to comply with before publication, please contact us immediately and, at the latest, by Tuesday, 19 October at 5pm (Australian Eastern Daylight Time). Please note that we intend to publish the determination on our website, not before **Wednesday, 20 October 2021**.

Your review rights are outlined on the determination. This matter is now closed.

Yours sincerely



Sophie Higgins
Principal Director
Dispute Resolution

14 October 2021



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 — <i>Privacy Act 1988</i> (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 website³ (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 algorithm⁵ 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. **s 47E(d)**
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 OAIIC 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 OAIIC dated 7 August 2020 (**Queensland Police response dated 7 August 2020**) p 1-5; Email from Victoria Police to the OAIIC, 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 OAIIC 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*

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/>

Protection Act 2018. Those provided to the OAIC will be considered in the context of the respondent's compliance with the Privacy Act.

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

²¹ s 6(1) of the Privacy Act.

- 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
- 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 Policy²³ 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

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.

(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

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:

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

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**).

- In order to be carrying on business, the activities must form a commercial enterprise.³⁴
- 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

³⁴ *Tiger Yacht* at [51]

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)

information 'in Australia' under s 5B(3)(c) includes the collection of personal information 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

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.

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. 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]
[REDACTED]
[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

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/>

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. 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

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

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

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 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).

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

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.

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:

- 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 Images⁸⁰ 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

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.

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 2021, 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.

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 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?

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

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>

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

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

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.

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

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.
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'.

⁹⁷ Respondent's response dated 19 August 2020 p 3-4.

⁹⁸ Ibid.

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/>.

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 "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

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/>.

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:

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

■ s 47E(d)

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:

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

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.

- 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 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

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 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).

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 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

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

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.

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 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

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

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>

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 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:

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*.

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].

- 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:

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 s 47E(d)

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).

¹³¹ APP Guidelines [B.40].

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.

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 s 47E(d)¹³⁹ from Scraped and Probe Images by measuring certain characteristics of an individual's face.¹⁴⁰
- 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

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.

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.'

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 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.

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.

¹⁴⁸ APP Guidelines [B.41].

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:
 - 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.

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

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 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).

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].

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].

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.

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.

¹⁵⁵ APP 3.4(b), s 16A, item 1.

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 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 expectation¹⁶¹ 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

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].

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.

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 from¹⁶⁵
 - 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
 - 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.

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'

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.

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 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:

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.

- 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
 - 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,¹⁷³ 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.

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.

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

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.

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.¹⁷⁴

¹⁷⁴ APP guidelines [B.64]

194. Personal information is inaccurate if it contains an error or defect as well as if it is misleading.¹⁷⁵
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.¹⁷⁶
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 compelling risks of harm to individuals, particularly when facial recognition is used in the context of law enforcement.¹⁷⁷

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.¹⁷⁸ 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.¹⁷⁹ Harms resulting from such misidentification can range from

¹⁷⁵ APP guidelines [10.12].

¹⁷⁶ APP guidelines [10.6].

¹⁷⁷ Angwin, J. *et al.*. "Machine Bias," *ProPublica*, May 23, 2016.

¹⁷⁸ 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.

¹⁷⁹ "Face Recognition Vendor Test, Part 3: Demographic Effects," *National Institute of Standards and Technology* (NIST), December 2019.

individuals being excluded from opportunities, to individuals being investigated and detained based on incorrect information.¹⁸⁰

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.’¹⁸¹
- 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.’¹⁸²
 - ‘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.’¹⁸³
 - ‘Independently Assessed For Accuracy An independent panel of experts assessed the accuracy of Clearview AI’s search results and found no errors.’¹⁸⁴
- 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)¹⁸⁵

199. s 47E(d)

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

¹⁸⁰ 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>

¹⁸¹ 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.

¹⁸² <https://clearview.ai/>

¹⁸³ <https://clearview.ai/overview>

¹⁸⁴ <https://clearview.ai/legal>

¹⁸⁵ Queensland Police response dated 7 August 2020 p 32, 38, 58, 63, 73, 81.

¹⁸⁶ Respondent’s response dated 4 August 2020 p 3.

investigative lead obtained through a Clearview search result. Clearview instructs its users to not rely solely on the search results they receive.¹⁸⁷

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**).¹⁸⁸
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'.¹⁸⁹
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.¹⁹⁰
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 2020.¹⁹¹

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 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.

¹⁸⁷ Respondent's response dated 4 August 2020 p 3.

¹⁸⁸ Respondent's response dated 26 September 2020 Attachment B.

¹⁸⁹ Respondent's response dated 26 September 2020 response p 16.

¹⁹⁰ AFP response dated 21 April 2020, Annexures Part 1, Annexure C, p 15.

¹⁹¹ OAIC s 44 notice dated 7 July 2020, questions 57 and 58, p 15.

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 2018.¹⁹² 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.¹⁹³
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,¹⁹⁴ 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 presented by the respondent as an 'independent panel of experts'¹⁹⁵ 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. s 47E(d)

¹⁹² Respondent's response dated 26 September 2020 p 16.

¹⁹³ <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>.

¹⁹⁴ Respondent's response dated 26 September 2020 p 19-20.

¹⁹⁵ Respondent's response dated 26 September 2020 p 10, 15-20;
<https://www.clearview.ai/legal>

¹⁹⁶ Respondent's response dated 4 August 2020 p 3.

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.¹⁹⁷

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.¹⁹⁸

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
- 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

¹⁹⁷ APP Guidelines [1.5].

¹⁹⁸ APP Guidelines [1.6].

- regular staff training and information bulletins on how the APPs apply to the entity, and its practices, procedures and systems developed under APP 1.2.¹⁹⁹

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] 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.²⁰¹ 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.²⁰²

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.

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

¹⁹⁹ APP Guidelines [1.7].

²⁰⁰ Respondent's response dated 21 July 2020 p 3.

²⁰¹ 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).

²⁰² 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).

- 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 1.2.²⁰³ 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.²⁰⁴

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.

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

²⁰³ 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/>

²⁰⁴ <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/>

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 Policy²⁰⁵ and the OAIC's Guide to Privacy Regulatory Action.²⁰⁶ 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.

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.

²⁰⁵ Privacy Regulatory Action Policy [38].

²⁰⁶ Guide to Privacy Regulatory Action [4.9].

239. I accept that the respondent has instituted a policy of refusing all requests for user accounts from Australia²⁰⁷ 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, s 47E(d), and has redesigned its website to no longer provide an access or opt-out mechanism to Australian residents.²⁰⁸
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

14 October 2021

Review rights

A party may apply under s 96 of the *Privacy Act 1988* (Cth) to have a decision under s 52(1) or (1A) to make a determination reviewed by the Administrative Appeals Tribunal (AAT). The AAT provides independent merits review of administrative decisions and has power to set aside, vary, or affirm a privacy determination. An application to the AAT must be made within 28 days after the day on which the person is given the privacy determination (s 29(2) of the Administrative Appeals Tribunal Act

²⁰⁷ Respondent's response dated 2 November 2020 p 2.

²⁰⁸ Respondent's response dated 3 June 2021 p 2.

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



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](#)