A Clearer View on Privacy, Australian Links and Biometric Data

Authors: Hamish Fraser (Partner) and **Belyndy Rowe** (Senior Associate), Bird & Bird

In November 2021 the Australian privacy regulator (**OAIC**) found that US based company Clearview AI, Inc. (**Clearview**) illegally collected the data of Australian citizens by web scraping it and disclosing it through its facial recognition tool. The OAIC ordered Clearview to cease collecting facial images and biometric templates from individuals in Australia, and to destroy existing images and templates created.

Clearview and its technology has attracted attention as a controversial organisation since it was written up in the New York Times as the 'secretive company' that could 'end privacy as we know it'.[1] Clearview's technology is a facial recognition app provided as a service to law enforcement agencies that assist them to identify and locate individuals in criminal investigations. The tool relies on a database of billions of images that Clearview has scraped from the internet including social media networks. Law enforcement can upload a picture of an individual and receive matched images from Clearview's databases at a scale not available before, along with the metadata and links to where those photos appeared on the internet.

The OAIC's 2021 decision found Clearview failed to implement practices, procedures and systems to ensure compliance with the *Privacy Act 1988* (Cth) (**Privacy Act**). It interfered with Australians' privacy by collecting sensitive information without consent, by failing to collect information lawfully and fairly, by failing to notify individuals that it had collected their data, and by taking insufficient steps to ensure information it used or disclosed via its service was accurate, up to date, complete and relevant.

The consideration of Clearview's offending behaviour is made complicated by amendments to the territorial application of the Privacy Act in December 2022. The Privacy Act requires organisations outside Australia to determine if they have an 'Australian link' and are therefore subject to the Privacy Act including the APPs.

The 2022 changes to section 5B of the Privacy Act lowered the threshold of who the Privacy Act applies to. Prior to the amendment of the Act, the relevant questions for an overseas company were whether it:

- carries on business in Australia; and
- collects the personal information of individuals in Australia?

In December 2022 the second of these two limbs (section 5B(3)(c)) was repealed, so that from this point forward, to establish an Australian link the only question became: *did the entity carry on business in Australia?*

AAT Ruling

To manage this complication the Administrative Appeals Tribunal (**AAT**) considered Clearview's behaviour in distinct periods:

- From December 2022: the Privacy Act was amended to lower the threshold of what counts as an 'Australian link'. Clearview no longer needed to collect or hold information in Australia to have an 'Australian link'.
- March 2022 to December 2022: Clearview ceased providing trials in Australia but continued to web scrape Australian data.
- October 2019 to March 2022: Clearview marketed and provided trials of its facial recognition tool to Australian law enforcement agencies.

In the period following December 2022, the AAT found that Clearview did carry on a business in Australia and was therefore subject to the Privacy Act. However, Clearview's collection of images posted online by Australians, or from .au domain names, did not count as carrying on business in Australia unless it was also hosted in Australia. But the collection of images from servers located in Australia was enough to constitute carrying on business in Australia.

The AAT cited recent Australian case law including OAIC enforcements as evidence that the interpretation of 'carrying on a business' had shifted to a 'modernised analysis' of how businesses are currently conducted, and to acknowledge that overseas businesses are 'extracting value' from information they collect about people.

The test used by the AAT made it clear that the drafting of the relevant section includes the words 'in Australia', and that this drafting sets the limits the reach of the Privacy Act (rather than a broader concept such as the 'information of Australian individuals'). Therefore, what happens 'in' Australia remains relevant. When Clearview obtains information from a server located in Australia there is a clear geographical connection. The AAT was satisfied that Clearview's collection of images is essential to its business, and that the interaction between the servers located in Australia, and the Clearview web crawler technology, are transactions which happen in Australia and make up and support the Clearview business.

In the pre-December 2022 period, the AAT recognised that the OAIC now also needed to establish the (subsequently repealed) requirement for companies to hold or collect data 'in Australia'. The AAT considered whether the necessary collection of Personal Information in Australia occurred was the same collection of Personal Information that was alleged to constitute a breach of the Privacy Act. The AAT

1 https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

undertook a detailed consideration of the web crawlers used and found they were communicating with, and receiving data from, servers in Australia and therefore concluded that the technical way in which Clearview collected Australians' data counted as collection 'in Australia'.

Clearview also argued was that even if it does have the required 'Australian link' it is a small business, so it would be exempt from the application of the APPs. The AAT rejected this argument as 'unconvincing' finding Clearview's revenue to be above the required threshold.

Breaches of the Privacy Act

Once an Australian link has been established, the Privacy Act will extend to an act done or practice engaged in outside Australia by an organisation. The OAIC's 2021 decision found that Clearview has failed to comply with several APPs in its collection and disclosure of the images.

The AAT agreed with the OAIC that Clearview had collected sensitive data without consent. Namely, Clearview had collected photos of individuals' faces (that is, biometric data).

However the AAT did not support the OAIC's other APP breach determinations. The AAT did not support the OAIC's view that Clearview had collected the information unlawfully, primarily because the data was collected from public sources. Therefore, there was no requirement to inform the relevant individuals.

The AAT held it was difficult to judge if the collection was fair, as the data was collected from websites with no access restrictions, although the AAT notes there could be a breach of terms where website terms of use prohibited web scraping. The OAIC had argued that LinkedIn and Twitter's terms of service restrict the use of bots to access those services, establishing that data collection was contrary to users' privacy. The AAT declined to judge whether the interactions between Clearview's web crawler and these sites amount to breaches of conditions of access.

The Privacy Act requires that data collectors "take such steps (if any) as are reasonable in the circumstances" to notify individuals when they collect their data. The AAT said it is difficult to establish what steps are "reasonable in the circumstances" during mass collection scenarios, noting Clearview would not be able to notify all affected individuals.

The AAPs require disclosed data to be accurate and up to date. The AAT was not satisfied that any further steps were required by Clearview to ensure that information that was disclosed via its tool was accurate, noting that Clearview's facial recognition system was providing accurate results and useful investigative leads for law enforcement.

Application to other web scraping businesses

This AAT determination confirms that an organisation may be subject to the Privacy Act despite having no presence in Australia. Web scraping images from Australian servers, even if the processing occurs overseas, may therefore equate to doing business in Australia and attract the application of the Privacy Act.

The AAT commented that the application of "carrying on business in Australia" in the age of the internet is difficult, despite the test being a common formulation appearing not just in the Privacy Act but also in the *Corporations Act* and the *Competition and Consumer Act*. The Court's consideration of the expression in various contexts has demonstrated the Courts are more conscious that the internet has changed the nature of business and are interpreting this requirement accordingly.

The AAT supported the OAIC's view that the collection of images of faces is a collection of sensitive information, and that Clearview collected this sensitive data without consent in breach of the APPs. 'Sensitive information' is defined in section 6 of the Privacy Act to include information or an opinion about an individual's biometric information that is to be used for the purpose of automated biometric verification or biometric identification, or biometric templates.

In accepting the OAIC's conclusion that the information collected by Clearview is biometric data, the AAT commented that the concept of biometric data is a developing one, stating that for most of human history it may not have been appropriate to describe a person's face as biometric information, however this has changed because of the development of powerful computers. The images of faces that have been collected by Clearview become sensitive data when the information is used for biometric identification.