

Clearview AI stops offering its facial recognition technology in Canada¹

Clearview AI, the American facial recognition start-up that has been embraced by police forces world-wide, announced earlier this month that it was ceasing offering its app product to Canadian law enforcement authorities.

Earlier this year, the federal Office of the Privacy Commissioner (OPC), together with the Commissioners in Quebec, Alberta and BC, [announced an investigation](#) into Clearview’s data collection practices – which involve “scraping” photographs of individuals off the internet and providing them, together with other identifiable data, to police forces to aid in their investigations.

However Clearview did not say it would stop collecting images of Canadians on the internet, nor did it undertake to delete the records that it currently holds.

Clearview has stated that it has amassed a database of more than three billion photos across the internet. This database of photos enables users of the Clearview app to match a person to their online photos and link back to the webpages where the photos were found. More precisely, for law enforcement, it means increasing the likelihood of identification of suspects in connection with a criminal investigation for whom only a photograph or video image exists.

Legality of scraping the internet

Under Canada’s privacy laws, the legality of collecting such photographic data from the internet, even if posted ostensibly “publicly”, is clear – it is not permitted unless the individual whose image is involved has consented to the collection. Limited exceptions apply such as when the intended uses are journalistic, literary or artistic. A “public” posting such as on the internet does not exempt the collection from compliance requirements under the privacy laws. Those laws do contain a very limited category of personal information that is exempted as “publicly available” – comprising essentially telephone and professional directory information. However, outside of these categories, personal information made available in a public context such as the Internet, or even on signs posted on public streets, may only be collected by consent of the individual involved.

There certainly are many circumstances when it can be concluded that personal information available online has been posted for purposes of sharing with and use by others, with the consent of the persons involved. “Public” Friends postings on Facebook are an example. However, any “consent” of a user of a Friends list likely does not extend to having their information collected and made use of for commercial – or law enforcement – purposes.

¹ A version of this article was originally published by The Lawyer’s Daily (www.thelawyersdaily.ca), part of LexisNexis Canada Inc.

So scraping the internet for photographic and other personal data by a private company such as Clearview AI is likely illegal in Canada, as well as in other jurisdictions with comprehensive privacy laws such as the European Union, the UK and Australia. Privacy regulators in some of these jurisdictions [have commenced investigations](#). However it is not per se illegal in the US, which has no comprehensive privacy law, and where police forces have embraced the technology. Consequently, challenges to Clearview in that country have focused on breach of civil liberties and unauthorized law enforcement surveillance.

Use by law enforcement

The collection and use of Clearview's facial recognition information by law enforcement in Canada is another aspect of the Canadian Commissioners' investigations. Under our public sector privacy laws, the collection of personal information by any public body, including law enforcement, while not requiring consent, is only permitted if there is clear statutory authorization. Generally, law enforcement authorities require a warrant or court order to obtain such data. However, in urgent circumstances where the data is critical to an investigation, they may collect it without warrant or court order.

Such collection of facial data likely is not authorized under any Canadian police legislation nor is it understood that any warrant or court order has been obtained for such collection. The OPC [has announced](#) a separate investigation into the RCMP's use of the Clearview app.

Opt-out for Canadians

Prior to withdrawing its app product from Canada, Clearview announced that it would enable Canadians to "opt out" of being included in its search results. Apparently, to execute the opt-out, Clearview requires an individual to submit their photo to the company, not simply their name. Furthermore, Clearview will retain that photo in its files. What's more, as noted, Clearview has not committed to deleting existing facial data files of Canadian residents, nor to stop collecting such data. So Canadians' facial data, including any photos submitted to opt out of search results, will remain part of Clearview's database.

The Commissioners' investigations should, among other conclusions, determine that the facial data of Canadian residents held by Clearview was collected improperly and must be deleted, and that such data collection going forward must cease. However, the ability of our regulators to enforce such requirements against Clearview, as a foreign company, is another question. Unfortunately, the international perception of our privacy laws appears to pale – in contrast, Clearview has agreed to allow residents of the EU, the UK and California (which has just enacted a strong consumer privacy law) to have their information deleted.

Big data and other concerns

Facial recognition technologies such as the Clearview Ai app have significant, concerning, implications for other, non-law enforcement, uses. Clearly, facial recognition information can be linked to "big data" databases identifying individuals for marketing and other targeting purposes. Offline retail and streetscape image captures of individuals can be linked through the technology to such databases. Interestingly, some major online

databases have directed Clearview to stop using images scraped from their platforms,² as contrary to their terms and conditions of use. However concerns with the technology go beyond unauthorized collection and use. For example, accuracy is understood to be only 75%. Concerns regarding importing racial and other biases based on facial data compound the potential for improper or inaccurate applications.

The results of the regulators' investigations, both in Canada and elsewhere, should provide insight into the future potential for the technology.

For more information please contact:

David Young 416-968-6286 david@davidyounglaw.ca

Note: The foregoing does not constitute legal advice. Readers are cautioned that for application to specific situations, legal advice should be obtained.

² <https://www.cnet.com/news/clearview-ai-hit-with-cease-and-desist-from-google-over-facial-recognition-collection/>

© David Young Law 2020