CLEARVIEW AI ORDERED TO COMPLY WITH PROVINCIAL REGULATORS' PRIVACY RECOMMENDATIONS

Posted on January 5, 2022

Categories: Insights, Publications

Following an investigation by privacy regulators in 2020, Clearview AI ("**Clearview**") has ceased offering its facial recognition services in Canada. However, it has not stopped collecting images of Canadians, nor has it deleted the images it already collected. Now, Canada's provincial privacy regulators have issued legally binding orders against Clearview forcing it to do just that.

Background

In February 2020, the federal Office of the Privacy Commissioner of Canada (the "**OPC**") and the provincial privacy regulators in British Columbia, Alberta and Québec (collectively, the "**Commissioners**") launched a joint investigation into a US-based technology company, Clearview.

Clearview has developed a program that gathers images of individuals from across the internet (including from public social media pages), analyzes the images for biometric data, and compiles them into its database. Clearview then markets a search tool that allows its users to search the database using an image of a face, and receive in return images of that face found from across the web. Clearview has sold its tool to law enforcement agencies, as well as private sector entities.

In February 2021, the Commissioners issued a report (the "**Report**") finding that Clearview breached federal and provincial private sector privacy laws by collecting online images of individuals in Canada without their knowledge or consent. More information on the Report can be found here.

The Report included non-binding recommendations that Clearview:

a. stop offering its facial recognition services in Canada;
b. stop collecting, using, and disclosing images and biometric information of Canadians; and
c. delete images and biometric facial information collected from Canadians

(collectively, the "**Recommendations**").

The Orders

Clearview advised the Commissioners that it had complied with the first recommendation in July 2020. However, as of December 2021, Clearview had not deleted or stopped processing the images and biometric information of Canadians.

Accordingly, the Commissioners (with the exception of the OPC) have now ordered Clearview to comply with the Recommendations as they relate to British Columbia, Alberta and Québec.[1]

The Office of the Information and Privacy Commissioner of Alberta provided a timeline, stating that Clearview must report on its good faith steps to comply with the Recommendations within 50 days of the order.[2] Similarly, the Commission d'accès à l'information du Québec ordered that Clearview destroy all images and biometric identifiers collected without consent within 90 days of the order.[3]

Clearview can seek judicial review, meaning it can ask the appropriate provincial court(s) to reconsider and overturn the order(s). However, if the orders are not overturned on review, Clearview could be subject to monetary penalties for non-compliance.

What Does This Mean?

The orders highlight the active role the Commissioners are willing to take in following up on reports and investigations. If the Commissioners are ultimately granted broader enforcement mechanisms by proposed legislative changes, this role is likely to expand.

The OPC took this announcement as an opportunity to comment on the gaps in existing federal privacy legislation, noting that it currently does not have order-making powers under the *Personal Information Protection and Electronic Documents Act* ("**PIPEDA**") and must instead refer evidence of the commission of an offence to the Attorney General of Canada, who is responsible for any prosecution. The result is that individuals in provinces other than British Columbia, Alberta and Québec are not protected by the provincial regulators' orders to Clearview. The OPC therefore called for amendments to strengthen the enforcement mechanisms in PIPEDA, including by providing the OPC the ability to issue orders and impose monetary penalties, noting that similar recommendations have been proposed in British Columbia (discussed here) and Ontario (discussed here), and adopted in Québec (discussed here).

Finally, the investigation into Clearview AI's services, and the resulting Recommendations and orders, speak to the importance of assessing the privacy law implications of new products, services and initiatives early in their development and prior to their implementation. Failure to design and implement offerings in a manner that complies with Canada's patchwork of privacy legislation can lead to privacy regulators' intervention and/or civil liability, as well as the costs of redesigning or scrapping offerings that are found not to be privacy compliant.

If you have any questions about these orders, the collection of ostensibly "publicly available" information, the

processing of biometric information, or Canadian privacy laws more generally, a member of our Privacy & Data Protection Group would be happy to assist you.

[1] Office of the Privacy Commissioner of Canada. News Release. *Clearview AI ordered to comply with recommendations to stop collecting, sharing images.* (14 December 2021), online: Office of the Privacy Commissioner of Canada.
[2] Office of the Information and Privacy Commissioner of Alberta. News Release. *Announcement: Clearview AI Ordered to Comply with Alberta's Privacy Law*. (14 December 2021), online: Office of the Information and Privacy Commissioner of Alberta.
[3] Commission d'accès à l'information du Québec. News Release. *La Commission ordonne à Clearview AI de cesser ses pratiques de reconnaissance faciale non conformes*. (14 December 2021), online: Newswire.

by Robbie Grant, Kristen Pennington, Julia Loney, Kristen Shaw (Articling Student)

A Cautionary Note