BIG BROTHER'S ACCESS LIMITED – CANADIAN PRIVACY COMMISSIONERS RULE CLEARVIEW AI'S FACIAL RECOGNITION TOOL IN BREACH OF CANADIAN PRIVACY LAWS

Posted on February 17, 2021

Categories: Insights, Publications

On February 2, 2021, the Privacy Commissioner of Canada (the "**OPC**") and the Information and Privacy Commissioner for British Columbia, Alberta and Quebec (collectively, the "**Commissioners**") released their joint report (the "**Report**"), finding that an American-based technology company, Clearview AI ("**Clearview**"), was in breach of both federal and provincial privacy laws by collecting publicly-accessible online photos of individuals in Canada without their knowledge or consent.[1] Clearview collects these images to populate its facial recognition database, intended for use by law enforcement but also used by a variety of other organizations, including private sector entities.

The Report addresses the Commissioners' serious concerns with Clearview's activities, which they termed the "mass identification and surveillance" of Canadians, including minors .[2] The Report clarified the Commissioners' stance on several key issues, including the application of Canadian privacy laws to foreign entities, the nature of biometric information and consents required for the use of online information, such as social media. The Report sets out a reasonably clear line for businesses to follow going forward with respect to what consents might be required given the potential for facial recognition or similar technologies to be used in the commercial context, including foreign businesses with no physical presence in Canada.

Background

Clearview created facial recognition software that allows users to upload an image of a person's face and search Clearview's database for similar matches using a facial recognition algorithm. Clearview obtains the images in its database by "scraping" public websites, including Facebook, YouTube, Instagram and Twitter, and storing these individuals' photographs. Clearview's data excludes images protected by privacy settings (for example, Instagram accounts that are set as private). In total, Clearview has "over three billion images of faces and corresponding biometric identifiers, including those of a vast number of individuals in Canada, including children".[3] Clearview asserts that its services are for law enforcement and investigative purposes, with clients such as the RCMP.

In February 2020, the Commissioners launched an investigation into Clearview following significant media controversy over Clearview's alleged collection and use of personal information without consent.[4] In response to the investigation, Clearview ceased offering its facial recognition services in Canada as of July 6, 2020.[5] The Report outlines the findings of the Commissioners' investigation.

The Report

The Commissioners found that Clearview breached the following privacy laws (collectively, the "**Acts**"):

a. the federal Personal Information Protection and Electronic Documents Act ("**PIPEDA**");
b. Quebec's Act Respecting the Protection of Personal Information in the Private Sector and Act to Establish a Legal Framework for Information Technology (the "**Quebec Acts**");
c. British Columbia's Personal Information Protection Act ("**PIPA BC**"); and
d. Alberta's Personal Information Protection Act ("**PIPA AB**").

In coming to this conclusion, the Commissioners considered three central issues:

a. Did Canadian federal and provincial privacy legislation apply to Clearview?
b. Did Clearview obtain necessary consents?
c. Were the purposes for which Clearview used the information appropriate, reasonable or legitimate in the circumstances?

1. ***Did the Commissioners have jurisdiction over Clearview?***

Clearview argued the Acts did not apply to it, as it did not have a real and substantial link to Canada. Clearview relied on the fact that it was located in the United States, the services were not aimed at Canadians and the content on the platform was collected online from around the world. On the provincial level, Clearview argued that it did not do business with or collect, use or disclose personal information in Alberta, British Columbia or Quebec.

The Commissioners found that the Acts did apply to Clearview for several reasons. Clearview actively marketed its services to Canadian organizations and "publicly declared Canada to be part of its core market" through its media statements.[6] Further, a real and substantial connection does not mean that Clearview's content must be exclusively sourced from Canada. Instead, the Commissioner found a real and substantial connection as a significant amount of Clearview's data was sourced from Canadian individuals. While the exact number of images sourced from Canadians was unavailable, the extent of Clearview's online scraping made it a near certainty that Clearview collected images and produced biometric information with respect to millions of individuals in Canada.

The Commissioners also found that Clearview's activities fell within the jurisdiction of provincial privacy laws, as these apply to "any private sector organization that collects, uses and discloses information of individuals within that province".[7] The Commissioners found Clearview's indiscriminate scraping made it obvious that it collected the personal information of individuals who were located in Alberta, British Columbia and Quebec. The fact that Clearview did not have a physical presence in any of these provinces was irrelevant.

2. ***Did Clearview obtain the necessary consents?***

The Commissioners found that the data Clearview collects is particularly sensitive, as it is "key to an individual's identity, supporting the ability to identify and surveil individuals", including minors. [8] Therefore, Clearview needed to obtain express consent for both the collection of the images and its creation of biometric information from such images. The Commissioners clarified that biometric information will be sensitive in almost all circumstances, because it has a distinctive, unique and invariable nature, which permanently links it to a specific person.

Clearview admitted that it had taken no steps to obtain the express opt-in consent of individuals whose images it obtained, but argued that it was exempt from such requirements as the information was publicly available.

The Commissioners rejected Clearview's argument, finding express consent necessary in the circumstances. Information taken from public websites, such as "social media or professional profiles . . . and then used for an unrelated purpose does not fall under the 'publicly available' exception of PIPEDA".[9] As well, while PIPA BC and PIPA AB prescribe certain sources of public information as exempt from consent requirements, social media and networking sites are not included under either Act. In fact, the Commissioners concluded that social media is highly dissimilar to other prescribed publications, such as newspapers or magazines, in part because of the dynamic and ever-changing nature of social media content and the direct control individuals have over their social media accounts and privacy settings. Similarly, the Commissioners determined that personal information is not "by law public" by the mere fact that it is "posted on social media or the Web" and this content is also not exempt from the application of the Quebec Acts.[10]

As a result, any collection from social media or networking sites required express consent and needed to be used for reasonably appropriate purposes.

3. ***Did Clearview have an appropriate, reasonable or legitimate purpose?***

The Commissioners rejected Clearview's argument that its purpose was appropriate as it benefitted law enforcement and national security. Instead, the Commissioners found that Clearview's "real purpose" for the collection is a commercial for-profit enterprise and not law enforcement.[11] This commercial purpose was not appropriate, reasonable or legitimate for "the mass identification and surveillance of individuals" facilitated by

Clearview's technology.[12] Clearview's surveillance and biometric information is often used to the detriment of the identified individuals, as it creates risk of prosecution, embarrassment, or investigation. This poses a significant risk of harm to those whose images are collected, such as through the dangers of misidentification or data breaches. Clearview's commercial purpose could not justify the mass collection of highly sensitive information that could likely only harm the individuals surveilled.

Additional Concerns

The Commissioners also raised some additional concerns that they found important, but ultimately upon which they did not opine.

The Commissioners expressed significant concerns about the accuracy of facial recognition technology, particularly with respect to the risk of misidentification. The Commissioners referred to studies demonstrating that these technologies frequently misidentify people, and especially women, of colour. In some instances, the rate of misidentification was 10 to 100 times higher than for Caucasian individuals. This poses a significant risk of discriminatory treatment, particularly in the law enforcement context where false positives could lead to wrongful criminal sanction.

As well, the Commissioners noted that Clearview had received cease-and-desist letters from Google, Facebook, Twitter, YouTube and LinkedIn, stating that Clearview's practices violated each site's terms of service. The Commissioners did not weigh in on whether the contractual violations occurred, but found that any such violations would be a relevant factor in considering the inappropriateness of Clearview's conduct.

The Commissioners also found that Clearview's large volume of highly sensitive information would likely be a target for data breaches; in fact, Clearview had been the subject of two data breaches in 2020 alone, which included leaks of its client list, source code and pilot project video.

Recommendations

The Commissioners recommended that Clearview:

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

While Clearview voluntarily exited the Canadian market in July 2020, Clearview refused to accept the Commissioners' findings and recommendations in the Report. If Clearview continues to refuse the Commissioners' recommendations, the Commissioners have indicated that they will bring other legal action to

bring Clearview into compliance.

What does the Report mean going forward?

The Commissioners took a strong position with respect to the use of online content, including social media content, by third party companies for commercial purposes. They concluded that a company does not have the right to use such content in whatever way they see fit simply because they have located it online. The real-time, dynamic and user-driven nature of social media makes it inherently different from other publicly accessible, consent-exempt forms of communication. A commercial venture can only use social media with the express consent of the individual about whom the content relates and then only with a reasonable and appropriate purpose. As a result, any company seeking to operate an online business which looks to use content which might be generally available online through social media sites or otherwise, and which can be categorized as personal information, will need to take clear steps to obtain the express consent of the user before appropriating the content for its own purposes. Given the decision of the Commissioners and their reasons in the Report, any other businesses will face a difficult time in trying to assert that they are entitled to collect such information.

The Report also clarifies the Commissioners' stance on biometric information and facial recognition software. These types of technologies can do amazing things but they also run the risk of easily falling afoul of privacy legislation because of the potentially intrusive nature of their functionality. As a result, the Commissioners relied on the decision of the OPC, and the Commissioners of Alberta and BC in Cadillac Fairview, which held that Cadillac Fairview needed express consent of its shoppers to collect, use and disclose their biometric information obtained through facial recognition software.[13] The Commissioners clearly articulated their position that biometric information is highly sensitive and therefore any entity seeking to collect, use or otherwise process such biometric information must seriously consider what steps it will need to take in order to obtain the express consent of affected individuals prior to such collection. The challenge, of course, is whether and how a company can practically and feasibly obtain the consent of potentially thousands or millions of individuals, many of whom it has no way to legitimately contact, prior to collection of such information The Commissioners have made their position very clear on this issue which means a business looking to utilize such technology on a broad scale will need to assess what steps are open to it to ensure it remains onside with the Commissioners' decision in Clearview.

Finally, foreign companies must recognize that they are not immune to the application of Canadian privacy laws simply because they do not have a physical location or presence within Canada for their operations. PIPEDA applies to organizations outside of Canada where a "real and substantial connection" to Canada exists, and the OPC will weigh several factors in considering whether this test is met.[14] PIPA AB, PIPA BC and the Quebec Acts apply to organizations that collect personal information of individuals within those provinces. As a

result, foreign companies will need to carefully consider whether their proposed operations, online or otherwise, might be subject to the Acts.

Any company, whether Canadian or foreign, looking to operate within Canada in an area such as facial recognition technologies which have the potential to intrude on a Canadian individual's privacy rights would be prudent to carefully and strategically assess how they can best provide such services within Canada, whether through obtaining consent from the affected individuals or otherwise, recognizing that they will likely be captured by Canadian privacy laws as currently written.

[1] *PIPEDA Report of Findings #2021-001* (2020) (Can Privacy Commissioner) ["**Report**"].
[2] *Ibid* at "Overview".
[3] *Ibid*.
[4] Office of the Privacy Commissioner of Canada, Announcement, "Commissioners launch joint investigations into Clearview AI amid growing concerns over use of facial recognition technology" (21 February 2020).
[5] Office of the Privacy Commissioner of Canada, News Release, "Clearview AI ceases offering its facial recognition technology in Canada" (6 July 2020).
[6] Report, *supra* note 1 at para 29(i).
[7] *Ibid* at para 33.
[8] *Ibid* at para 74.
[9] *Ibid* at para 45.
[10] *Ibid* at para 46.
[11] *Ibid* at para 88.
[12] *Ibid* at para 76.
[13] *PIPEDA Report of Findings #2020-004, Re* (2020) (Can Privacy Commissioner).
[14] Report, *supra* note 1 at para 28.

by Robert Piasentin, Grace Shaw, and Julianna Ivanyi, Articled Student

A Cautionary Note