Facial Recognition: A Privacy Law Perspective

March 2021 - 4 min read

Humans love to look at faces – our families, our friends, complete strangers.

In some ways, our brains are optimized for facial identity recognition. We're good at it, so of course we want to teach machines how to do it even better than we do. Facial recognition technology is rapidly advancing, and its use is expanding, raising concerns among consumers, privacy regulators, legislators, and privacy advocates.

What does current Alberta privacy law say about the use of this technology?

First, let's clarify what we mean when we talk about "facial recognition technology".

A range of technology components are used, usually combining biometric software that maps an individual's facial features and logs the data as a "faceprint", often coupled with machine-learning algorithms. The software needs a source of images, sometimes collected by video surveillance cameras. Social media platforms also serve up a rich source of images of human faces, as seen in the Clearview AI case, discussed below.

The technology is readily available – many smartphones have it integrated with their cameras. The smartphone software immediately starts picking out faces, categorizing them according to known facial images.

Some recent examples illustrate how the technology is deployed and how regulators are responding.

Shopping Mall Directories

The Cadillac Fairview Corporation Limited (CFCL) is one of the largest owners and operators of office buildings and shopping malls in North America. In 2020, the Office of the Privacy Commissioner of Canada (OPC), along with privacy regulators of Alberta (OIPC AB) and British Columbia (OIPC BC), jointly investigated whether CFCL used facial recognition technology to collect personal information without consent. CFCL used so-called AVA (Anonymous Video Analytics) technology which was surreptitiously installed inside wayfinding directory kiosks in about a dozen shopping malls across Canada (including two in Alberta).

While a shopper was standing in front of a wayfinding directory kiosk, the AVA technology caught temporary digital images of the faces, used facial recognition software to convert those images into biometric numerical representations of the individual faces, and used that information to determine age range and gender.

The investigation report was released in October 2020. It revealed that CFCL's AVA service provider had collected and stored approximately 5 million numerical representations of faces "on a decommissioned server, for no apparent purpose and with no justification". The privacy commissioners decided that this did constitute the collection and use of personal information, clarifying that personal information extends to the captured images of faces and the numerical representation assigned to each face and the assessment of age range and gender. (PIPEDA Report of Findings #2020-004)

Clearview AI

Services

Intellectual Property
Privacy + Data Management

Industries

Artificial Intelligence
Emerging Technology

People

Richard Stobbe Partner,
Trademark Agent, CLP
rstobbe@fieldlaw.com

In February 2021, privacy protection authorities for Canada, Alberta, British Columbia and Quebec released their report examining privacy compliance practices of Clearview AI, Inc. (Clearview).

Clearview is a US technology company that sells a facial recognition software tool and a combined database. Clearview's system allows customers to upload a digital image of an individual's face and run a search against a database using artificial intelligence algorithms to find a match. It is essentially the facial image equivalent of running a name search through a database or matching a fingerprint against a database of known fingerprints. Naturally, some Canadian police services were interested in the product.

In January and February 2020, public reports emerged that Clearview was populating its facial recognition database by collecting digital images from various public sources such as Facebook, YouTube, Instagram and Twitter. Their software "crawled" the social media sites, without the consent of individuals, copying and categorizing the images, and then stored the images in Clearview's database to be sourced and served as results for facial recognition searches.

In the report's summary, the commissioners noted that "…the indiscriminate nature of Clearview's scraping renders it a relative certainty that it collected millions of images of individuals in Canada, and used them to derive biometric image vectors for its database."

This indiscriminate scraping triggered a review by Alberta's privacy commissioner under Alberta's *Personal Information Protection Act* (PIPA) and raised two interesting issues:

1. Clearview objected on jurisdictional grounds. Suppose an American company accesses the websites operated by other American companies, like Facebook, YouTube, Twitter and Instagram. How could a Canadian privacy commissioner claim jurisdiction over this kind of activity?

   The commissioners had no trouble in asserting their jurisdiction to exert investigative powers. While the commissioners cannot generally impose significant monetary penalties, they can make public findings and recommendations following an investigation. This power alone can be powerful for a company that wants to avoid the reputational damage that comes with a public dressing down by the privacy commissioner.

2. Clearview also argued that consent was not required as the images were publicly available. Under this argument, there could be no reasonable expectation of privacy in images where individuals made those images publicly available on social media.

   The commissioners concluded that Clearview should have obtained express opt-in consent before it collected the images of any individual in Canada. The final report stated clearly that the collection of images and creation of biometric facial recognition arrays by Clearview constitutes "the mass identification and surveillance of individuals by a private entity in the course of commercial activity." [and] "…a reasonable person would not consider this purpose to be appropriate, reasonable, or legitimate."

In the end, Alberta's privacy commissioner agreed with the conclusions of the joint investigation and recommended that Clearview:

- Cease offering its facial recognition services in Canada;
- Cease the collection, use and disclosure of images and biometric facial arrays collected from individuals in Canada; and
- Delete images and biometric facial arrays collected from individuals in Canada in its possession.

These were merely recommendations, not a conviction under the offence provisions of privacy legislation, and Clearview has disputed these findings, essentially rejecting the recommendations. Clearview also announced that it has ceased commercial operations in Canada.

Takeaways

Both CFCL and Clearview provide some common and important takeaways:

1. Both facial identity **and** the numerical codes assigned to each face can be considered "personal information" for privacy law purposes.
2. Privacy laws protect the rights of individuals in Canada, and foreign companies, regardless of where they conduct business, will be subject to Canadian privacy laws if the personal information of Canadians is collected, used or disclosed.
3. Individuals can have a reasonable expectation of privacy even if the image or personal information is displayed on a publicly available website.

Organizations should exercise caution when collecting, using, or disclosing information that they believe is publicly available and is less sensitive. While PIPA provides some exceptions for “publicly available” information, that term is specifically defined under its regulations and is more limited than one may think. As technology evolves, more personal information may be available on public sites – but privacy is not a game of finders keepers. For advice on handling practices and the collection, use and disclosure of information under your applicable legislation, please contact Richard Stobbe or any member of our Privacy + Data Management Team.