7. Facial Recognition and Facial Detection

The Privacy Officer’s Guide to Personal Information Protection and Electronic Documents Act, 2024 Ed.

Timothy M. Banks

The Privacy Officer's Guide to Personal Information Protection and Electronic Documents Act, 2024 Ed. (Banks) > Chapter 2 WHAT IS PERSONAL INFORMATION? > C. Types of Personal Information

Chapter 2 WHAT IS PERSONAL INFORMATION?

C. Types of Personal Information

7. Facial Recognition and Facial Detection

The OPC has conducted two important investigations into the use of facial recognition and facial detection technologies in collaboration with other Privacy Commissioners in Canada. In *Report of Findings #2021-001*,[1] the OPC summarized its joint investigation with other Privacy Commissioners into the practices of Clearview AI. According to the Report of Findings, Clearview AI had collected over 3 billion images of faces and biometric identifiers, which it made available to law enforcement. In *Report of Findings #2020-004*,[2] the OPC summarized its joint investigation with other Privacy Commissioners into the use of an anonymous video analytics tool by shopping centres managed by Cadillac Fairview. What is clear from these investigations is that the OPC considers biometric identifiers derived from facial images to be very sensitive.

Based on the OPC’s description of Clearview AI’s technology, it appears that Clearview AI was providing facial recognition services. In other words, law enforcement could upload an image to Clearview AI, which would then process the image and compare it to other images it had processed in order to identify a match. Clearview AI obtained its repository of over 3 billion images by using web crawlers to crawl publicly available sites (including social media) to gather images of individuals, it would then take copies of these image and the metadata associated with the images (*e.g.*, the title, source, link and description). Clearview AI’s technology would then analyze the digital images of faces and turn them into numerical representations to identify unique features of the individual’s face.[3]

Clearview AI argued that it did not need consent to collect and use the images because they were publicly available. This aspect of the decision is discussed in section D.2 of this chapter. For present purposes, the important aspect of the Report of Findings is the debate between the Commissioners and Clearview AI regarding the sensitivity of the images. Once the OPC dismissed the argument that the images could be collected and used without consent, the issue was whether express consent would be required because the data was sensitive. As reported by the Commissioners, Clearview AI argued that the images were not sensitive because they were already publicly accessible online. Further Clearview AI argued that the numerical representations of the photographs were hashed and so could not be used for facial recognition outside of the Clearview AI software application.[4] The Commissioners rejected this argument and stated that biometric information is sensitive in almost all circumstances because it is distinctive, unlikely to vary over time, is difficult to change, and largely unique to the individual. For the

Commissioners, facial biometric information was particularly sensitive because of its potential for identifying individuals and surreptitious surveillance.[5]

The Commissioners in the Cadillac Fairview investigation came to the same conclusion on sensitivity even though the context was much less intrusive and much less likely to lead to surreptitious surveillance and even though the technology was not used by law enforcement. The investigation arose out of (among other things), a pilot project for anonymous video analytics ("AVA"). Some shopping centre directories were equipped with cameras that took images which were retained only for a few milliseconds and then discarded. The images were then converted to a unique random identifier that could be used to distinguish one face from another and assign an age and gender probability. However, this unique identifier was also associated with additional information, including a numerical representation of the image, the location of the camera and the directory, the name of the mall, and the estimated age and gender of the individual.[6] The Commissioners asserted (without *any* evidence) that there was a serious possibility that an individual could be identified. As in the subsequent Clearview AI decision, the OPC concluded that the biometric identifier was inherently sensitive.[7] This Report of Findings is an example of some of the worst results-based reasoning of Privacy Commissioners. The Commissioners' findings were based on conjecture rather than any evidence of a risk of the information being about an identifiable individual in any practical senses. No serious attempt was made by the Commissioners to explain just how an individual could be reidentified from the data or why the collection of the images was any more sensitive than video recording for security purposes. It is difficult to reconcile the OPC's approach with the OPC's and the Federal Court's approach to voiceprints discussed below.

Footnote(s)

[1] *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta*, [2021] C.P.C.S.F. No. 3 (Can. Priv. Comm.) ("Clearview AI").

[2] *Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia*, [2020] C.P.C.S.F. No. 4 (Can. Priv. Comm.).

[3] *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta*, [2021] C.P.C.S.F. No. 3 at para. 13 (Can. Priv. Comm.).

[4] *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta*, [2021] C.P.C.S.F. No. 3 at para. 21 (Can. Priv. Comm.).

[5] *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta*, [2021] C.P.C.S.F. No. 3 at para. 41 (Can. Priv. Comm.).

[6] *Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia*, [2020] C.P.C.S.F. No. 4 at para. 50 (Can. Priv. Comm.).

[7] *Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia*, [2020] C.P.C.S.F. No. 4 at para. 79 (Can. Priv. Comm.).