OIPC

Office of the Information
& Privacy Commissioner
Nova Scotia

News release

Privacy regulators call for legal framework limiting police use of facial recognition technology

GATINEAU, QC, May 2, 2022 – The heads of Canada's privacy protection authorities today issued a joint statement recommending legislators develop a legal framework that establishes clearly and explicitly the circumstances in which police use of facial recognition may be acceptable.

Facial recognition has emerged as a tool of significant interest for police agencies in Canada. Used responsibly and in the right circumstances, the technology could provide public safety benefits such as helping solve serious crimes, locating missing persons and supporting national security objectives.

At the same time, the use of facial recognition involves highly sensitive biometric information, and raises concerns for privacy and human rights.

"Facial Recognition Technology (FRT) is a powerful tool that has beneficial potential. However, it can also be a significantly privacy-invasive tool," says Tricia Ralph, Information and Privacy Commissioner for Nova Scotia. "Without regulation and proper oversight, the deployment of this technology could seriously and negatively impact the privacy rights of Nova Scotians. The privacy provisions in Nova Scotia's *Municipal Government Act* are over 20 years old. Under Nova Scotia's current privacy laws, my Office has no oversight over the privacy practices of municipalities or their police forces. Existing legislation is wholly inadequate to the task of regulating the unique privacy risks posed by FRT and modern technology generally. Clear and rigorous laws must be put in place to govern any future use of this emerging technology in Nova Scotia."

Canada currently has a patchwork of laws governing facial recognition, which are insufficient to address the risks to privacy and other fundamental rights associated with the technology. A new legal framework should therefore set appropriate limits on police use of facial recognition.

In the joint statement, privacy regulators say a new legal framework for regulating police use of facial recognition technology should include:

- **A clear and explicit definition of the limited purposes for which police use of facial recognition would be authorized, and a list of prohibited uses. "No-go zones"** should include a prohibition on any use of facial recognition that can result in mass surveillance.

- **Strict necessity and proportionality requirements.** Legislation should require police use of facial recognition to be both necessary and proportionate for any given deployment of the technology.

- **Independent oversight.** Police use of facial recognition technology should be subject to strong independent oversight. Oversight should include proactive engagement measures. Police should be required to obtain pre-authorization from an oversight body at the program level, or provide it with advance notice of a proposed use, before launching a facial recognition initiative.

- **Privacy rights and protections.** Appropriate privacy protections should be put in place to mitigate risks to individuals, including measures to ensure the accuracy of information and limits to how long images can be retained in police databanks**.**

Privacy guardians also released final guidance to clarify police agencies' privacy obligations relating to the use of facial recognition under the current law. The guidance and joint statement follow a public consultation launched in June 2021 to seek feedback on both a draft version of the guidance and a future legal and policy framework to govern police use of the technology.

The consultation followed an investigation into Clearview AI that found the private sector platform was involved in mass surveillance. A separate investigation found the RCMP's use of Clearview to be unlawful, since it relied on the illegal collection and use of facial images.

The consultation received 29 written submissions from stakeholders representing civil society, academia, government, police, legal and industry sectors, as well as individuals. Meetings were also held with law enforcement agencies, civil society groups, organizations representing marginalized communities and equity seeking groups, as well as federal, provincial and territorial human rights commissioners to seek feedback.

Some stakeholders called for the guidance to include more details to help apply the advice in specific situations. The feedback led to a number of amendments and privacy regulators intend to advise police agencies on specific use cases as they are developed.

There was general agreement among stakeholders on the need to develop a legal framework for police use of facial recognition. A large majority of stakeholders agreed that legislative gaps exist and new legislation specifically governing facial recognition use by police is required.

Related documents:

Recommended legal framework for police agencies' use of facial recognition – Joint Statement by Federal, Provincial and Territorial Privacy Commissioners

Privacy guidance on facial recognition for police agencies

Opening statement – Appearance before the Standing Committee on Access to Information, Privacy and Ethics (ETHI) on their Study of the Use and Impact of Facial Recognition Technology

-30-

Contact:

Office of the Information and Privacy Commissioner for Nova Scotia
Tel: 902-424-4684
Email: oipcns@novascotia.ca