

**For immediate release
May 2, 2022**

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

VICTORIA— 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 has enormous capabilities and can offer significant public safety benefits when used responsibly,” says BC Information and Privacy Commissioner Michael McEvoy. “It can also be exceptionally intrusive because it involves the collection and processing of highly sensitive personal information. Biometric facial data is unique to each individual and unlikely to vary significantly over periods of time. In a very real sense, it is at the core of our individual identity.”

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 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 an FR 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 that 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](#)

Media Contact

Michelle Mitchell | Senior Communications Manager
Office of the Information and Privacy Commissioner for BC
250 217-7872 | mmitchell@oipc.bc.ca