OpenMedia is a community-based organization that safeguards
the possibilities of the open Internet.

April 29, 2021

The Special Committee on Reforming the Police Act
c/o Parliamentary Committees Office
Room 224, Parliament Buildings
Victoria, BC V8V 1X4
Canada

Dear Minister Nicholas Simons,

I'm writing on behalf of OpenMedia, a community of hundreds of thousands from all across Canada that work together to keep the Internet open, affordable, and surveillance-free. I'd like to share our concerns surrounding how law enforcement in British Columbia are able to procure technologies that have a negative impact on our rights, including our fundamental right to privacy, and how law reform can help address the situation.

Facial Recognition Technology and Canada's Inadequate Legal Framework

As it stands, Canada's legal framework does not meaningfully address the negative privacy impacts that are unlocked through technologies that make use of artificial intelligence, like facial recognition. Under Canadian law (the *Privacy Act*) and British Columbian law (the *Freedom of Information and Protection of Privacy Act*), our faces and other sensitive biometric information are treated the same as our names or addresses. But unlike our names and addresses, our faces are seldom subject to change, and are perpetually present in our worldly interactions.

Through the use of facial recognition technology, it becomes possible for law enforcement to identify and monitor people during the course of constitutionally protected activity, like speech and peaceful demonstration in public spaces. For this reason, special protections should be enacted through law that restrain law enforcement from infringing upon our constitutional rights through the use of facial recognition. However, as the Department of Justice looks to Modernize Canada's *Privacy Act*, they have stated that they are not interested in creating a special category for sensitive biometric information.[1] Therefore, it becomes imperative that Canada's provincial legislation account for how law enforcement is using technologies that infringe upon our constitutional rights, like facial recognition, through legislative amendment.

Facial Recognition Technology and Clearview AI

[1] Centre for Media, Technology, and Democracy at McGill University – 'Weak privacy, weak procurement: The state of facial recognition in Canada'
https://www.mediatechdemocracy.com/work/weak-privacy-weak-procurement-the-state-of-facial-recognition-in-canada

Unfortunately, in the space between where our laws fail to account for technological leaps, and where private companies demonstrate a willingness to create ethically and legally questionable software, British Columbia's law enforcement agencies have felt free to experiment.

Most prominent is the case of Clearview AI, a facial recognition company that scraped the Internet for faces and amassed a database of more than three billion images. Clearview AI then made this database available to law enforcement, who could upload an image of a person and compare it against the more than three billion other images in the database — essentially making every person with an image of their face on the Internet a suspect in criminal investigations.

Earlier this year, the Privacy Commissioner of Canada, along with its provincial counterpart in British Columbia, concluded an investigation that determined Clearview AI was an illegal form of mass surveillance.[2] Clearview AI failed to achieve, or even attempt to seek, consent for any of the personal information they scraped from the Internet. Nonetheless, dozens of law enforcement agencies across Canada, including several in British Columbia, were found to be using Clearview AI.

In March of 2020, despite initial denials, the RCMP and the Vancouver Police Department (along with many others) admitted to using Clearview AI after the client list for the company was leaked.[3] In the case of the Vancouver Police Department, they claimed that the software had only been used once, without official approval from the department. However, as we said in our presentation to the Vancouver Police Board earlier this year, it's very hard to understate the significance of the privacy violation that occurred with that singular use.

Thousands of members of our community, including many of us on staff, have filed requests for personal information with Clearview AI and found out that our faces were in their database. We learned that the company possessed numerous images of OpenMedia staff members, and thousands of others in our community, including children. Also troubling, we learned that Clearview AI did not respect the legislated timelines and request mechanisms required under federal and Canadian privacy law.

So when the Vancouver Police Department used Clearview AI's software even once, they violated the privacy rights of thousands of people in our community; every person in their database of billions of images became a defacto suspect in the criminal investigation that the

---

[2] OPC Report of Findings – #2021-001
https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/

[3] The Vancouver Sun – 'Vancouver detective used controversial facial-recognition software once'
https://vancouversun.com/news/vancouver-police-used-controversial-clearview-facial-recognition-software-a-single-time

department was investigating. And, because of the legal void between the advancement of technology and our laws that was described earlier, more “misunderstandings” are sure to occur in the future: if not with Clearview AI, then with the next company looking to extract profits by infringing on our fundamental privacy rights.

Facial Recognition Technology and the Vancouver Police Board

When we addressed the Vancouver Police Board about the Vancouver Police Department’s use of Clearview AI, we spoke about the broad-based harms of facial recognition technology and how it has been shown to present a bias against women and people of colour. Without any safeguards in place, facial recognition technology in the hands of the police will negatively impact those in our community who are already experiencing the harms of over policing. In the United States, at least three black men have been wrongfully arrested due to faulty facial recognition technology, one of whom spent time in jail.[4]

In our presentation to the Vancouver Police Board, we described the policy vacuum that allowed the officer at the Vancouver Police Department to use Clearview AI. The department has made their internal policies public.[5] Nowhere in that document was there any mention of facial recognition; the department had no internal policy governing the use of this technology.

The only comparable policy was for the use and creation of “photo packs” that consist of no more than ten lawfully obtained images. To create a “photo pack”, an officer is required to complete at least three forms. One then wonders how many forms would be required to compile a “photo pack” of more than three billion images, like that of Clearview AI’s database? A few hundred million forms? As mentioned before: like the department’s own policies, British Columbia’s privacy laws offer no special protections for the use of sensitive biometric information, like our faces.

After pointing these concerns out during our presentation to the Vancouver Police Board, and reinforcing this point through a complaint we filed through the Office of the Police Complaints Commissioner, the Vancouver Police Department announced a moratorium on the use of facial recognition technology.[6] In order to use facial recognition again, the department has committed to creating an internal policy on its use, consulting with the Office of the Privacy Commissioner

[4] The New York Times – ‘Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match’ https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html
[5] Vancouver Police Department – ‘Regulations and Procedures Manual’ https://vpd.ca/police/organization/planning-research-audit/regulations-procedures-manual.html
[6] Vancouver is Awesome – ‘VPD looks to develop policy for use of facial recognition technology’ https://www.vancouverisawesome.com/vancouver-news/vpd-looks-to-develop-policy-for-use-of-facial-recognition-technology-3646584

of Canada, completing a privacy impact assessment, and seeking approval from the Vancouver Police Board.[7]

At the bare minimum, these are the necessary conditions for law enforcement to be able to use facial recognition technology in a way that might lead towards accountability and transparency. Other concerns may arise throughout this process but, without these minimal conditions, the use of facial recognition technology by law enforcement is an absolutely unconscionable abuse of power and leads to the erosion of our fundamental rights.

OpenMedia's Recommendation to the Special Committee

To this special committee reviewing the *Police Act*: we implore you to hear the concerns we've raised here and to recommend that the laws be updated to include protections against the abuse of new technologies that make use of artificial intelligence. In the name of accountability and transparency, we ask that the special committee put forward a recommendation that all law enforcement in British Columbia implement a moratorium on the use of facial recognition until such time that our laws are updated to account for its broad-based harms.

At the absolute bare minimum, the moratorium must be in place until such a time that British Columbia's *Police Act* requires its law enforcement agencies to:

- create internal policies on the use of facial recognition technology;
- receive approval of these policies by their respective governance bodies;
- complete privacy impact assessments and make them public;
- consult with the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner of British Columbia.

Without these basic measures, British Columbians will be unable to trust that law enforcement is operating in the best interests of the public and respecting our fundamental rights.

Sincerely,

Bryan Short
Digital Rights Campaigner
OpenMedia

[7] Vancouver Police Department – 'Report to the Vancouver Police Board'
https://vancouverpoliceboard.ca/police/policeboard/agenda/2021/0415/SP-5-2-2104C03-SP-Complaint-Facial-Recognition.pdf