July 8, 2020

The Honourable Bill Blair
Minister of Public Safety and Emergency Preparedness
269 Laurier Avenue West
Ottawa, Canada K1A 0P8

VIA EMAIL ONLY

Subject: Ban on use of facial recognition surveillance by federal law enforcement and intelligence agencies

Minister Blair:

We are writing to you during uncertain times. As we live through the COVID-19 pandemic, many are asking themselves what will come next. The killing of George Floyd by a Minneapolis police officer, as well as multiple recent incidents of police killing and mistreatment of Black people, Indigenous people and people of colour in Canada – including D'Andre Campbell, Chantel Moore, Rodney Levi and Ejaz Ahmed Choudry – have placed a spotlight on racial discrimination by law enforcement, with people across Canada demanding changes to policing.

At a time like this, the public should be certain of the fact that their rights and freedoms are protected.

This is why we are contacting you to express our grave concern about recent revelations of the use of facial recognition technology by federal law enforcement agencies. Facial recognition technology is highly problematic, given its lack of accuracy and invasive nature, and poses a threat to the fundamental rights of people in Canada. In the absence of meaningful policy or regulation governing its use, it cannot be considered safe for use in Canada.

We are therefore asking that the federal government:

- Enact a ban on facial recognition surveillance by federal law enforcement and intelligence agencies;
- Initiate a meaningful, public consultation on all aspects of facial recognition technology in Canada;
- Establish clear and transparent policies and laws regulating the use of facial recognition in Canada, including reforms to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and the *Privacy Act*.

Our concerns go beyond the revelations about the use of Clearview AI technology, recognizing that there are other facial recognition systems available and used. Clearview AI is simply one egregious example of why there must be immediate action.

Facial recognition surveillance presents grave risks to the fundamental rights of Canadians and people in Canada by allowing for the "mass, indiscriminate, disproportionate, unnecessary, warrantless search of innocent people."[1]

This inappropriately broad application is compounded by the lack of oversight, accountability and transparency around its use. There have been multiple examples of law enforcement services either being unaware of the use of facial recognition technology by its officers, or knowingly misinforming the public about their activities.

The RCMP denied use of Clearview AI for several weeks, until it was compelled to reveal its use of the software just as the media was about to publish a list of the company's clients.[2] [3] The admission itself was vague and lacking in details, and the force did not immediately commit to suspending use of facial recognition. News reports also revealed that the RCMP has used facial recognition since 2002, despite previously denying any use of the technology.[4] While they have now stated they will limit the use of facial recognition technology, this does not go nearly far enough.

The Canada Border Services Agency has thus far remained silent about their use of facial recognition technology, and Canadian intelligence agencies have refused to acknowledge at all whether or not they use the technology.[5]

This widespread lack of openness and transparency is deeply troubling. Across the country, police forces have admitted to hiding their use of facial recognition tools, as well as to officers using new technology without the knowledge or approval of their superiors. Federally, the Privacy Commissioner was not consulted by the RCMP before it began using Clearview AI technology, and a search of Privacy Impact Assessments on the RCMP website returns no mention of facial recognition. These issues signal a severe and stunning lack of accountability around the adoption of this technology, further undermining the rights of people in Canada.

There are also clear, documented examples of the problems that facial recognition entails.

---

1 Canadian Civil Liberties Association, "Deputation on Facial Recognition Technology", 30 May 2019, https://ccla.org/ccla-deputation-facial-recognition-technology-used-toronto-police-services/

2 Tunney, C., "RCMP denied using facial recognition technology - then said it had been using it for months", *CBC News*,

2 Tunney, C., "RCMP denied using facial recognition technology - then said it had been using it for months", *CBC News*, 4 March 2020. Available at: https://www.cbc.ca/news/politics/clearview-ai-rcmp-facial-recognition-1.5482266

3 Allen, K., W. Gillis & A. Boutilier, "Facial recognition app Clearview AI has been used far more widely in Canada than previously known", *Toronto Star*, 27 February 2020. Available at: https://www.thestar.com/news/canada/2020/02/27/facial-recognition-app-clearview-ai-has-been-used-far-more-widely-in-canada-than-previously-known.html

4 Carney, B., "Despite Denials, RCMP Used Facial Recognition Program for 18 Years", *The Tyee*, 10 March 2020. Available at: https://thetyee.ca/News/2020/03/10/RCMP-Admits-To-Using-Clearview-AI-Technology/

5 C. Freeze & T. Cardoso, "Privacy watchdogs launch joint investigation into Clearview AI's facial-recognition technology", *Globe & Mail*, 21 February 2020. Available at: https://www.theglobeandmail.com/canada/article-privacy-commissioners-launch-joint-investigation-into-clearview-ai/

Facial recognition technology has been shown to be inaccurate and particularly prone to produce biased outcomes for people of colour and women. Many top systems have been found to mis-identify the faces of women and people with darker skin 5 to 10 times more often than those of white men.[6]

Another study from the National Institute of Standards and Technology found that facial recognition technology falsely identified African-American and Asian faces 10 to 100 times more than white faces, and that among databases used by law enforcement the highest error rates came in identifying Native Americans.[7]

These errors can lead already marginalized communities to be even more likely to face profiling, harassment and violations of their fundamental rights. This is especially concerning when we consider the technology's use in situations where biases are common, including when individuals are traveling and crossing borders as well as in the context of criminal investigations, national security and anti-terrorism operations and the pursuit of the so-called "war on terror."

While unscrupulous companies like Clearview AI are using deeply questionable – and in some areas, illegal – tactics to develop databases of images for agencies to screen against, the use of what some may consider more "lawful" databases also raises concerns: in 2012, the BC privacy commissioner ruled that police require a court order to use the database of photographs maintained by the Insurance Corporation of British Columbia, after the agency offered to provide the Vancouver Police Department access without a warrant.[8] The lack of regulations regarding biometrics raises questions about how often such offers take place, and whether federal agencies accept them.

The current context of protests against police violence and racial profiling places a stark light on the problem. Across the United States, there are reports of law enforcement using facial recognition technology known to misidentify people of colour, and Black people in particular, in order to identify and prosecute people protesting police brutality and anti-Black racism.[9] The lack of regulation, though, means that it is impossible to know how many police forces are using this technology.

This same problem exists in Canada: it is currently impossible to know which police forces and intelligence agencies are using facial recognition in our country, and to what ends, including during protests. If, as federal officials have said, the Canadian government is serious about ending racial disparities in policing, banning facial recognition surveillance is a clear first step.

Troublingly, we are also seeing growing calls to use facial recognition technology in order to combat the COVID-19 pandemic. China's government has vaunted its use,[10] and Clearview AI is reportedly in talks with US federal and state governments to provide them with pandemic-related surveillance

---

6 Simonite, T. "The Best Algorithms Struggle to Recognize Black Faces Equally", *Wired*, 22 July 2019. Available at: https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/

7 Singer, N. & C. Metz, "Many Facial-Recognition Systems Are Biased, Says U.S. Study", *New York Times*, 19 December 2019. Available at: https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html

8 CBC News, "Police can't use ICBC facial recognition to track rioters", *CBC News*, 16 February 2012. Available at: https://www.cbc.ca/news/canada/british-columbia/police-can-t-use-icbc-facial-recognition-to-track-rioters-1.1207398

9 Gershgorn, D. "Facial Recognition Is Law Enforcement's Newest Weapon Against Protesters", OneZero, 3 June 2020. Available at: https://onezero.medium.com/facial-recognition-is-law-enforcements-newest-weapon-against-protestors-c7a9760e46eb

10 Jakhar, P. "Coronavirus: China's tech fights back", 3 March 2020. Available at: https://www.bbc.com/news/technology-51717164

tools.[11] We recognize that governments must take important, even unprecedented, steps in order to limit the spread of this virus and protect public health. In a time of crisis, though, governments must still ensure to protect the rights of their constituents. Too often, we have seen rights undermined because of a crisis, to devastating and lasting effects. We have also seen that temporary, emergency measures that undermine human rights often end up becoming permanent after a crisis has passed.

At the same time, both public and governmental concerns around facial recognition in North America are rising. Several communities across the United States have banned the use of facial recognition by law enforcement, including San Francisco.[12] IBM recently disclosed that it "will stop offering facial recognition software and opposes any use of such technology for purposes of mass surveillance and racial profiling."[13] There are several bills currently before the US Congress calling for a moratorium and greater regulations.[14] The State of Vermont is suing Clearview AI for unlawfully acquiring data from consumers and businesses in violation of multiple state laws.[15] More than 100 leading organizations on privacy and civil liberties have signed a call for an international moratorium.[16] EU officials have raised concerns that the technology's use for surveillance violates the General Data Protection Regulation.[17]

In Canada, more than 11,000 people have signed a call from OpenMedia for a moratorium on facial recognition technology.[18] There are open investigations by the federal Privacy Commissioner, as well as three provincial bodies.[19] [20] The Standing Committee on Ethics, Privacy and Access to Information has voted to study the impact of facial recognition technology.[21]

---

11 Pascu, L. "Governments looking into advanced surveillance, biometric tech to contain coronavirus", BiometricUpdate.com, 18 March 2020. Available at: https://www.biometricupdate.com/202003/governments-looking-into-advanced-surveillance-biometric-tech-to-contain-coronavirus

12 Bailey Jr., E. "Portland considering strictest ban on facial recognition technology in the U.S.", *Oregon Live*, 21 February 2020. Available at: https://www.oregonlive.com/portland/2020/02/portland-considering-strictest-ban-on-facial-recognition-technology-in-the-us.html

13 CBC News, "IBM exits facial recognition business, calls for police reform", CBC News, 9 June 2020. Available at: https://www.cbc.ca/news/technology/ibm-exits-facial-recognition-1.5604331

14 Wyrich, A. "Senators introduce facial recognition bill proposing moratorium on government use", *Daily Dot*, 13 February 2020, https://www.dailydot.com/layer8/facial-recognition-moratorium-bill-merkley-booker/

15 Cox, K. "Vermont sues Clearview, alleging "oppressive, unscrupulous" practices", *Ars Tecnica,* 3 March 2020. Available at: https://arstechnica.com/tech-policy/2020/03/vermont-sues-clearview-alleging-oppressive-unscrupulous-practices/

16 "Declaration: A Moratorium on Facial Recognition Technology for Mass Surveillance", The Public Voice, October 2019. Available at: https://thepublicvoice.org/ban-facial-recognition/

17 Macaulay, T., "Automated facial recognition breaches GDPR, says EU digital chief", *TNW News*, 17 February 2020. Available at: https://thenextweb.com/neural/2020/02/17/automated-facial-recognition-breaches-gdpr-says-eu-digital-chief/

18 "Stop Facial Recognition in Canada", OpenMedia, accessed on 13 March 2020. Available at: https://act.openmedia.org/StopFacialRecognition

19 "Commissioners launch joint investigation into Clearview AI amid growing concerns over use of facial recognition technology", Office of the Privacy Commissioner of Canada, 21 February 2020. Available at: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200221/

20 "OPC launches investigation into RCMP's use of facial recognition technology", Office of the Privacy Commissioner of Canada, 28 February 2020. Available at: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200228/

21 "Minutes of Proceedings: 24 February 2020", Standing Committee on Access to Information, Privacy and Ethics (ETHI), accessed on: 13 March 2020. Available at: https://www.ourcommons.ca/DocumentViewer/en/43-1/ETHI/meeting-2/minutes

With all of this considered, it is urgent that the federal government recognize the need for in-depth study, and new policies and laws regarding the use of facial recognition technology in Canada. Given this, we ask that you implement these three actions without delay:

- Enact a ban on facial recognition surveillance by federal law enforcement and intelligence agencies;
- Initiate a meaningful, public consultation on all aspects of facial recognition technology in Canada;
- Establish clear and transparent policies and laws regulating the use of facial recognition in Canada, including reforms to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) and the *Privacy Act*.

We hope to receive a prompt reply to these concerns, and look forward to discussing them with you further.

Sincerely,

Tim McSorley, National Coordinator
International Civil Liberties Monitoring Group

Laura Tribe, Executive Director
Open Media

Endorsed by:

Organizations:

Access Now
Amnesty International Canada
British Columbia Civil Liberties Association
Canadian Association of University Teachers
Canadian Civil Liberties Association
Canadian Federation of Students
Canadian Friends Service Committee (Quakers)
Canadian Muslim Lawyers Association
Canadian Office & Professional Employees, Local 342
Canadian Union of Postal Workers

Canadian Unitarians for Social Justice
Canadian Voice of Women for Peace
Criminalization and Punishment Education Project
Electronic Privacy Information Center (EPIC)
Fight for the Future
FNEEQ-CSN
Freedom of Information and Privacy Association
Greenpeace Canada
Human Rights Research and Education Centre, University of Ottawa
Independent Jewish Voices Canada
Inter Pares
Lawyers' Rights Watch Canada
Ligue des droits et libertés
MiningWatch Canada
National Union of Public and General Employees
PEN Canada
Privacy International
Right to Know Coalition of Nova Scotia
Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)

Individuals:

Alisa Gayle
Andi Wilson Thompson, New America's Open Technology Institute
Andrew Clement, Professor emeritus, Faculty of Information, University of Toronto
Azeezah Kanji (journalist and legal academic)
Bérengère Marin-Dubuard
Chandler Davis, Professor, University of Toronto
Cheryl Gaster, LL.B., C. Med
Darrell Evans, Director, Canadian Institute for Information and Privacy Studies
David Murakami Wood, Associate Professor, Sociology, Queen's University
Denis Barrette, lawyer
Diana Chaplin
Dominique Peschard
Dr. Jennifer Barrigar
Elisabeth Dupuis
Elizabeth Block
Enver Domingo
James L. Turk, Director, Centre for Free Expression, Ryerson University
Jason Haggkvist
Jeffrey Monaghan, Associate Professor, Carleton University Institute of Criminology and Criminal Justice
John Packer, Associate Professor, Faculty of Law, University of Ottawa
John Stetch
John Wunderlich, Kantara Initiative, MyData, IEEE Standards
Karen Filipcic
Kathryn M. Campbell
Khaled Al-Qazzaz
Laura von Hausen

Lynda Khelil, community sector worker
Maritza Felices-Luna Department of Criminology, University of Ottawa
Mark Filipcic
Martin Klein, Retired, University of Toronto
Martine Eloy, Ligue des droits et libertés
Mathieu Parent
P. M. Campbell
Penny Fancy
Professor Line Beauchesne, Department of criminology, University of Ottawa
Professor Valerie Steeves, University of Ottawa
Roch Tassé
Roger Baird
Sharaf Sharafeldin
Sheila Paul
Teresa Scassa, University of Ottawa
Tony Bunyan, Director Statewatcch
Ursula Shbib
Will Dubitsky
Wolfe Erlichman
Yavar Hameed, lawyer, Hameed Law