Brief presented to the
House of Commons Standing Committee on
Access to Information, Privacy and Ethics

by the
International Civil Liberties Monitoring Group

in regards to the
Committee's study of the
Use and Impact of Facial Recognition Technology

April 13, 2022

About the ICLMG

The International Civil Liberties Monitoring Group (ICLMG) is a national coalition of Canadian civil society organizations that was established after the adoption of the *Anti-Terrorism Act* of 2001 in order to protect and promote human rights and civil liberties in the context of the so-called "War on Terror." The coalition brings together 45 NGOs, unions, professional associations, faith groups, environmental organizations, human rights and civil liberties advocates, as well as groups representing immigrant and refugee communities in Canada.

Our mandate is to defend the civil liberties and human rights set out in the Canadian Charter of Rights and Freedoms, federal and provincial laws (such as the Canadian Bill of Rights, the *Canadian Human Rights Act*, provincial charters of human rights or privacy legislation), and international human rights instruments (such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment).

Active in the promotion and defense of rights within their own respective sectors of Canadian society, ICLMG members have come together within this coalition to share their concerns about national and international anti-terrorism legislation, and other national security measures, and their impact on civil liberties, human rights, refugee protection, minority groups, political dissent, governance of charities, international cooperation and humanitarian assistance.

Since its inception, ICLMG has served as a round-table for strategic exchange — including international and North/South exchange — among organizations and communities affected by the application, internationally, of new national security ("anti-terrorist") laws.

An important aspect of the role of the ICLMG is the dissemination of information related to human rights in the context of counter-terrorism and the expanding – and largely unaccountable – national security apparatus. This information is distributed to members of the coalition who in turn broadcast it to their own networks.

Finally, further to its mandate, the ICLMG has intervened in individual cases where there have been allegations of serious violation of civil liberties and human rights. The ICLMG has also intervened to contest proposed legislation, regulations and practices that contravene the Canadian Constitution, other Canadian laws and international human rights standards.

A. ICLMG’s positions on facial recognition technology (FRT)

A central part of our coalition’s work has been around the need for accountability, transparency and clear legal frameworks to govern surveillance activities by federal law enforcement and intelligence agencies.[1] Surveillance activities by law enforcement must be sure to obey the Canadian Charter of Rights and Freedoms, including seeking out judicial authorization for surveillance that would otherwise constitute a breach of the charter.

We have regularly raised concerns around surveillance that unduly targets particular communities in the form of racial, religious or political profiling, as well as mass surveillance of public places or of specific events. These forms of surveillance are never justified, in that they violate not just privacy rights, but also rights to assembly, association and movement, and equality rights. This includes both visual surveillance – i.e., via camera – but also online surveillance of social media, communications and associated metadata.

More specifically in regard to facial recognition technology, our coalition has advocated for a ban on certain forms of facial recognition surveillance, as well as a moratorium on other forms of use of facial recognition technology, for all federal law enforcement and intelligence agencies, including the RCMP, the CBSA and CSIS.

In July 2020, we sent an open letter to that effect to Minister of Public Safety Bill Blair, co-signed by 30 other organizations and more than 40 individuals, all active in protecting privacy, human rights and civil liberties. In it, we wrote:

> 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.[2]

While there have been important developments in the 20 months since we sent this letter, including the Office of the Privacy Commissioner’s reports on both Clearview AI and the RCMP’s use of Clearview AI technology, nothing has changed to substantively improve the transparency, accountability or legal framework around law enforcement’s use of facial recognition technology in Canada.

[1] Given that our coalition’s mandate is to focus on federal activities, our comments are primarily geared to that level of government. However, we believe that our concerns are also more broadly applicable and that the issues relating to facial recognition technology must be addressed at all levels of government.

[2] ICLMG, “Letter to Minister Bill Blair re: Ban on use of facial recognition surveillance by federal law enforcement and intelligence agencies,” 8 July 2020. Online at: https://iclmg.ca/wp-content/uploads/2020/07/facial-recognition-letter-08072020.pdf

Facial recognition technology continues to be used by Canadian law enforcement and intelligence agencies at a growing pace. The technology has been found to be biased and inaccurate. It also allows for gross violations of fundamental rights and freedoms protected under both Canadian and international law. This includes violation of Canadian Charter rights protecting against unreasonable search or seizure (s. 8), as well as infringing upon the right to peaceful assembly (s. 2(c)), to free expression (s. 2(d)) and to equality (s. 15(1)). Similarly, it violates Articles 17 (right to privacy) and 21 (free assembly) of the International Covenant on Civil and Political Rights. Gaps in Canadian law mean that this technology is being adopted without any meaningful accountability or transparency.

Our concerns around the use of FRT by law enforcement can be further broken down into four areas:

1. Facial recognition systems are inaccurate and biased.

Multiple independent studies have shown that the algorithms on which some of the most widely used facial recognition matching technology is based are biased and inaccurate. This is especially true in regard to people of colour, who already face heightened levels of surveillance and profiling by law enforcement and intelligence agencies in Canada.

For example, a 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 US law enforcement the highest error rates came in identifying Indigenous people.[3]

The City of Detroit has regulated the use of facial recognition, but according to the Detroit Police Department's own 2020 statistics, it was used almost exclusively against Black people and misidentified people 96% of the time.[4]

Even if the algorithms could be improved, there are also concerns about the kinds of databases that are used to match and identify facial patterns. For instance, some police forces use mugshot databases as the comparison dataset. However, these databases are flawed and should be questioned in terms of their reliability or whether they increase further stigmatization. For example, while a mugshot database would contain images of people who have been arrested, it would also include those whose charges were dropped or who have been acquitted. Is it reasonable that they would continue, by virtue of their arrest, to be included in a dataset that could result in false positives and have dire consequences?

Facial recognition can also exacerbate the racial profiling and targeting of racialized communities already seen in law enforcement surveillance operations. This is exemplified by a

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

[4] Koebler, J. "Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time", *Vice*, 29 June 2020, Available at: https://www.vice.com/en_us/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time

Feb. 2022 report from Amnesty International, which concluded that facial recognition technology has been reinforcing racist stop-and-frisk policing in New York. Among their findings:

- the New York Police Department's vast surveillance operation particularly affects people already targeted for stop-and-frisk across all five boroughs of New York City.
- In the Bronx, Brooklyn and Queens, the research also showed that the higher the proportion of non-white residents, the higher the concentration of facial recognition compatible CCTV cameras.[5]

This issue can also be seen in the area of counter-terrorism. The RCMP has been revealed to have contracted the services of a facial recognition service known as IntelCentre. This company claims to offer access to facial recognition tools and a database of more than 700,000 images of people associated with "terrorism."[6] According to the company, these images are acquired from various sources online, including social media, using the same controversial methods as other companies. Of additional concern, it is unclear how they determine which individuals to include in their database, and how they verify the accuracy of the information they provide, or how they define a link to "terrorism." An unregulated database of potential terrorists raises significant concerns around accuracy and racial profiling, knowing what we do of the flaws and biases in approach to anti-terrorism policing in Canada, the United States and internationally. It is clear that this kind of system will have devastating impacts on someone who is falsely accused, since, unlike other facial recognition services, this system comes with the added stigma of being allegedly linked to terrorism.

All of these issues 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 protests against government policies and actions, when individuals are traveling and crossing borders as well as in the context of criminal investigations, national security operations and the pursuit of the so-called "War on Terror."

2. Facial recognition allows for mass, indiscriminate and warrantless surveillance

Even if FRT was 100% accurate, this could not justify its use, since other significant problems would persist. Both real-time (live) and after-the-fact facial recognition surveillance systems subject members of the public to intrusive and indiscriminate surveillance. This is true whether it is used to monitor travellers at an airport, individuals walking through a public square, people online, or activists at a protest.

[5] Amnesty International, "Facial recognition technology reinforcing racist stop-and-frisk policing in New York – new research," amnesty.org, 15 February 2022. Online at: https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/

[6] Bryan Carney, "RCMP Secret Facial Recognition Tool Looked for Matches with 700,000 'Terrorists'," *The Tyee*, 28 April 2021. Online at: https://thetyee.ca/News/2021/04/28/RCMP-Secret-Facial-Recognition-Tool-Looked-Matches-Terrorists/

The Supreme Court has ruled that individuals retain a right to privacy even when in a public space.[7] This should undoubtedly apply to the collection, retention and identification of individuals' facial images. However, while it is mandatory for law enforcement to seek out judicial authorization to surveil individuals either online or in public places, there are gaps in current legislation as to whether this applies to surveillance or de-anonymization via facial recognition technology.[8] Further, these gaps also leave open questions not just of tracking a particular individual, but engaging in mass surveillance in the hopes of being able to identify a person of interest, either in real-time or after the fact, thereby submitting all passerby to unjustified mass surveillance.

3. Lack of regulation of the technology and a lack of transparency and accountability from law enforcement and intelligence agencies

As demonstrated in the Office of the Privacy Commissioner's draft guidance for law enforcement on the use of FRT,[9] and evidenced by the RCMP and other law enforcement agencies misleading the public regarding their use of facial recognition technology, the current legal framework governing facial recognition technology is wholly inadequate. This patchwork of privacy rules at the provincial, territorial and federal levels fails to ensure that law enforcement use facial recognition technology in a way that respects fundamental rights.

Further, a lack of transparency and accountability means that such technology is being adopted without public knowledge, let alone public debate or independent oversight.[10]

This allowed the RCMP, for example, to use Clearview AI facial recognition technology for months without the public's knowledge, and to then lie about it before being forced to admit the truth.[11] Moreover, we now know that the RCMP has used one form of facial recognition or another for the past 20 years, without any public acknowledgement, debate or clear oversight.[12]

And as documented by Citizen Lab, it was eventually revealed that at least seven Canada law enforcement agencies also used Clearview AI technology, with some initially denying use. This was explained as being due to individual officers using the technology without authorization – a

[7] R. *v.* Spencer, 2014 SCC 43, [2014] 2 S.C.R. 212 at para. 44

[8] Kate Robertson, Cynthia Khoo, and Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (September 2020), Citizen Lab and International Human Rights Program, University of Toronto, p. 90.

[9] Office of the Privacy Commissioner of Canada, "Draft privacy guidance on facial recognition for police agencies," Government of Canada, 10 June 2021. Online at: https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/gd_frt_202106/#toc3-1-1

[10] Allen, K., W. Gillis & A. Boutilier, "Facial recognition app Clearview AI has been used far more widely in Canada than previously known", *The 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

[11] 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

[12] 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/

completely unacceptable excuse.[13] Regardless of the attempted explanation, it is clear that without regulation and greater transparency and accountability, it is impossible to know whether this is what actually occurred, and that it will not occur again with other facial recognition systems or other police forces.

Following an investigation, the Office of the Privacy Commissioner of Canada found that Clearview AI violated Canadian law, and that the RCMP's use of Clearview AI was unlawful.[14] The RCMP has rejected that finding, though, stating that they cannot be held responsible for the lawfulness of services provided by third parties. This essentially allows them to continue contracting with other services that violate Canadian law.

The RCMP's above-mentioned contracting of "anti-terrorism" facial recognition service IntelCentre has received less coverage, but mimics the problems with Clearview AI very closely. For example, according to the company, they acquire the images in their database from various sources online, including social media, just like Clearview AI. Also, like Clearview AI, it is unclear how these images are verified, or the legal justification for collecting these images. We also have no idea how the RCMP used this tool, let alone the force's legal basis for using it.

The Tyee's investigation also found that the force broke rules and worked to mislead the public. In particular, RCMP policy requires the reporting and sign-off on any software purchases of over $500 (and any other purchase over $10,000). This was never done, despite the contract being worth $20,000. Members of the RCMP also applied varying labels to the purchase – including "software", "database" and "photography services" – which allowed them to skirt oversight and disclosure rules. [15]

In another example of weak transparency rules, the CBSA ran a pilot project using real-time facial recognition surveillance at Toronto's Pearson Airport for six months in 2016, with little to no public warning beyond a vague notice posted to their website. In all, nearly 3 million travellers had their faces scanned against a database of 5,000 images.[16]

Finally, CSIS has refused to confirm whether they use facial recognition technology in their work, stating they have no obligation to do so. While intelligence agencies may not be able to go

[13] Kate Robertson, Cynthia Khoo, and Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (September 2020), Citizen Lab and International Human Rights Program, University of Toronto. Online at: https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/

[14] Office of the Privacy Commissioner of Canada, "Police use of Facial Recognition Technology in Canada and the way forward: Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology," Government of Canada, 10 June 2021. Online at: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/

[15] Bryan Carney, "RCMP Secret Facial Recognition Tool Looked for Matches with 700,000 'Terrorists'," *The Tyee*, 28 April 2021. Online at: https://thetyee.ca/News/2021/04/28/RCMP-Secret-Facial-Recognition-Tool-Looked-Matches-Terrorists/

[16] Lauren O'Neill, "Canada under fire for secretly using facial recognition at Toronto's Pearson airport," *BlogTO*, 19 July 2021. Online at: https://www.blogto.com/tech/2021/07/canada-secretly-using-facial-recognition-toronto-pearson-airport/

into the specifics of ongoing operations, there is no reason why they should not engage in a fulsome, public debate about the use of such controversial technology.

4. Facial recognition technology is a slippery slope.

Currently, the scope and use of facial recognition technology in Canada by law enforcement is not entirely known. Even if we take for granted that the current use of facial recognition technology by Canadian law enforcement is limited, it must be recognized that the unregulated nature of this use remains harmful in and of itself. It also presents a slippery slope, whereby the technology gains ground and acceptance over time, allowing its use to spread until it can no longer be put back in the box.

We have seen this in other jurisdictions: Limited use of facial recognition by law enforcement in other countries has typically led to greater and much broader rollouts of the technology. In the U.S., for example, former president Donald Trump issued an executive order requiring facial recognition identification for all international travellers in the top 20 U.S. airports by 2021.[17]

In the UK, facial recognition is already being used at sports matches, street festivals, protests, and even on the streets to constantly monitor passers-by.[18]

It is easy to imagine that without proper scrutiny, public debate and regulation, the same will eventually come to Canada – if it's not already the case without our knowledge.

B. Recommendations & next steps

Given all this, there is a clear urgency for Canadian parliamentarians to act to restrict and regulate the use of facial recognition technology in Canada.

Our coalition is calling for three key actions:

1. That the federal government immediately ban the use of facial recognition surveillance by law enforcement and intelligence agencies, and undertake consultations for the regulation of facial recognition technology in general;
2. That the government undertake reforms to both private and public sector privacy laws to address gaps in the regulation of FRT and other biometric surveillance;
3. That the Privacy Commissioner be granted greater enforcement powers, both with regards to public sector and private sector violations of Canadian privacy laws.

[17] Alba, D. "The US Government Will Be Scanning Your Face At 20 Top Airports, Documents Show", *Buzzfeed*, 11 March 2019. Available at: https://www.buzzfeednews.com/article/daveyalba/these-documents-reveal-the-governments-detailed-plan-for

[18] Smith, A. "Football fans demand end to facial recognition cameras being used at matches", *Metro*, 7 August 2018. Available at: https://metro.co.uk/2018/08/07/football-fans-demand-end-to-facial-recognition-cameras-being-used-at-matches-7808677/; Bowcott, Owen. "Police face legal action over use of facial recognition cameras", *The Guardian*, 14 June 2018. Available at: https://www.theguardian.com/technology/2018/jun/14/police-face-legal-action-over-use-of-facial-recognition-cameras; BBC Click. "Are you ready for a world of facial recognition? Several UK police forces have been trialling the technology", *Twitter*, 13 May 2019. Available at https://twitter.com/BBCClick/status/1127961872286789634

While a ban on the use of facial recognition technology for surveillance purposes by law enforcement may appear controversial, it is in line with the positions being taken in many other jurisdictions.

For example, more than a dozen US cities have banned the use of FRT at the municipal level, including: San Francisco and Oakland, California; Boston, Brookline, Cambridge, Northampton, Easthampton, and Somerville in Massachussetts; Jackson, Mississippi; King County, Washington; Madison, Wisconsin; New Orleans, Louisiana; Minneapolis, Minnesota; Portland, Maine; and Portland, Oregon.[19]

Various U.S. states have also enacted strict regulation, including bans on facial recognition surveillance in public places, rules around seeking legislative approval before use of facial recognition technology, and strictly limited warrants for exceptional cases. These include Vermont, Maine, Massachusetts, Virginia, Oregon, Washington and California.[20]

In a landmark ruling, the British Court of Appeal ruled that facial recognition in public places violates human rights.[21]

The Australia Human Rights Commission has called for a ban on facial recognition technology's use "in decision-making that has a legal, or similarly significant, effect for individuals, or where there is a high risk to human rights, such as in policing and law enforcement" until further study and regulations are put in place.[22]

Finally, the European Parliament voted in October 2021 for a ban on the use of facial recognition technology by law enforcement in public spaces. They are still considering official legislation on the issue.[23]

Canada would be in good company to move forward with strict restrictions and regulations on all use of facial recognition technology by law enforcement, including a ban on its use for surveillance purposes.

Beyond this ban on FRT surveillance, we believe that other issues must be addressed through reform of privacy laws in general. This includes both private sector laws (for example, in regard

[19] Kay Lively, T. "Facial Recognition in the United States: Privacy Concerns and Legal Developments," *Security Management Magazine*, 1 December 2021. Online at:https://www.asisonline.org/security-management-magazine/monthly-issues/security-technology/archive/2021/december/facial-recognition-in-the-us-privacy-concerns-and-legal-developments/

[20] *ibid.*

[21] Fernandez, E. "Facial Recognition Violates Human Rights, Court Rules," *Forbes*, 13 August 2020. Online at: https://www.forbes.com/sites/fernandezelizabeth/2020/08/13/facial-recognition-violates-human-rights-court-rules/?sh=5cc7f2b65d44

[22] Hendry, J. "Human Rights Commission calls for temporary ban on 'high-risk' govt facial recognition," *IT News*, 28 May 2021. Online at: https://www.itnews.com.au/news/human-rights-commission-calls-for-temporary-ban-on-high-risk-govt-facial-recognition-565173

[23] Peets, L. et al, "European Parliament Votes in Favor of Banning the Use of Facial Recognition in Law Enforcement," *InsidePrivacy.com*, 12 October 2021. Online at: https://www.insideprivacy.com/artificial-intelligence/european-parliament-votes-in-favor-of-banning-the-use-of-facial-recognition-in-law-enforcement/

to third party vendors) and public sector laws (those regulating law enforcement, as well as empowering privacy regulators). In particular, this includes (but is not limited to):

- Private and public sector privacy laws must be amended to recognize that privacy is a human right and to adopt a human rights framework to privacy protections;
- Privacy commissioners must be granted greater powers of enforcement in the private sector, along with stronger order-making powers in the public sector;
- Privacy laws must bring in stronger transparency regulations in both public and private sectors, and stricter Privacy Impact Assessment rules for the public sector;
- Changes must be made in regard to regulations on the use of AI and algorithmic decision-making in both the public and private sector to require greater transparency, independent third-party review, and ongoing oversight (among others);
- Legislation must bring greater clarity and institute stronger restrictions around the collection, retention and use of so-called "publicly available information" in both public and private sector, particularly when it comes to the collection of biometric information, information with a reasonable expectation of privacy, or information shared for one purpose but collected and retained for another;
- Future legislation must remove exceptions for law enforcement and national security agencies when it comes to divulging activities that impact privacy and other rights, including the use of facial recognition technology.

C. Conclusion

We thank the committee for taking on this important issue, and urge you to make strong, specific recommendations regarding the use of facial recognition technology by law enforcement and intelligence agencies in Canada. We re-iterate the three main steps we believe must be taken by parliamentarians and the government on this issue:

1. That the federal government immediately ban the use of facial recognition surveillance by law enforcement and intelligence agencies, and undertake consultations for the regulation of facial recognition technology in general;
2. That the government undertake reforms to both private and public sector privacy laws to address gaps in the regulation of FRT and other biometric surveillance;
3. That the Privacy Commissioner be granted greater enforcement powers, both with regard to public sector and private sector violations of Canadian privacy laws.

While these are framed as calls on the government to act, the current political context also allows for parliamentarians to bring forward motions for these reforms, including changes to legislation to limit the use of FRT and to grant more powers to the Office of the Privacy Commissioner, as well as a motion to initiate a broader, formal inquiry and consultation into the use, impact and reforms needed in regards to FRT and Canada's privacy laws overall.

We would be happy to discuss these issues with members of the committee or other parliamentarians further.