Submission to the Office of the Privacy Commissioner of Canada

Consultation on draft privacy guidance on facial recognition for police agencies

Presented by the
International Civil Liberties Monitoring Group

20 October 2021

International Civil Liberties Monitoring Group
Coalition pour la surveillance internationale des libertés civiles
4-210 Florence Street, Ottawa, ON, K2P 0W7
Tel. (613) 241-5298

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.

ICLMG's positions on FR technology

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 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 15 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

Our concerns around the use of FR technology by law enforcement are based on four primary concerns:

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

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, or activists at a protest.

The Supreme Court has ruled that individuals retain a right to privacy even when in a public space.[3] 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.[4] 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.

2. 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.[5]

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.[6]

---

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

[4] 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

[5] 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

[6] 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

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? The same can be argued for even those who were found guilty of a criminal offence, especially given what we know of the disproportionate arrest and conviction rates of racialized or otherwise marginalized individuals. Their inclusion in a facial recognition database could result in a feedback loop, whereby since they can be identified, they are more likely to be criminalized through automatic identification, or suffer the consequences of false positives.

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 that claims to identify terrorists.[7] It is unclear how this service determines which individuals to include, or where they obtain these images from, but they boast that their facial image database contains more than 700,000 individuals. An unregulated database of potential terrorists raises significant concerns around accuracy and racial profiling, knowing what we do of the flaws in approach to anti-terrorism policing in Canada, the United States and internationally.

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."

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

As demonstrated in the OPC's guidance document, and evidenced by RCMP and other law enforcement agencies misleading of the public regarding their use of facial recognition technology, the current legal framework is wholly inadequate. The current patchwork of privacy rules at the provincial, territorial and federal levels do not 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.[8]

---

[7] 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/

[8] 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

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.[9] 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.[10]

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 to individual officers using the technology without authorization.[11] Whatever the case, 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.

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 know. We do know that police forces are using such systems to compare facial images of suspects to databases of images that they lawfully possess (ie, mugshot databases). We also know, though, that police forces in Canada, including the RCMP, have had access to technology that would allow them to engage in "real time" facial recognition surveillance, as well as online facial recognition surveillance. For example, the Canada Border Services Agency ran a pilot project using real-time facial recognition surveillance at Toronto's Pearson Airport for six months in 2016, with little no public notice beyond the Privacy Impact Assessment on its website.[12] Meanwhile, the Canadian Security Intelligence Service has refused to confirm whether or not they use facial recognition technology in their work.

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.[13]

---

[9] 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

[10] 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/

[11] 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.

[12] 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/

[13] 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

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.[14]

It is easy to imagine that without proper scrutiny, public debate and regulation, the same will eventually come to Canada.

Feedback on guidance

1. **Will this guidance have the intended effect of helping to ensure police agencies' use of FR is lawful and appropriately mitigates privacy risks? If you don't believe it will, why?**

The OPC's Draft privacy guidance on facial recognition for police agencies is a thorough and important step forward in ensuring that facial recognition technology is appropriately managed and to mitigate the associated risks to privacy and other rights.

It demonstrates clearly and effectively the strengths and weaknesses of Canada's current legislative framework in this area, and clearly delineates the obligations and best practices that police agencies should follow. In those regards, it goes further than any framework we have seen to date.

Unfortunately, while the guidance will clearly help, we do not believe that is will have the intended goal overall of ensuring that police agencies' uses of facial recognition are either lawful or that privacy risks are mitigated. The current legal framework is too fragmented, and law enforcement agencies have already shown that they are unwilling to adhere to guidance as opposed to legal obligations in the form of judicial authorizations, etc.

As the OPC notes in the draft guidance:

> The process of establishing appropriate limits on FR use remains incomplete. Unlike other forms of biometrics collected by law enforcement such as photographs, fingerprints or DNA profiles, FR use is not subject to a clear and comprehensive set of rules. Instead, its use is regulated through a patchwork of statutes and case law that, for the most part, do not specifically address the risks

[14] 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

> posed by FR. This creates room for uncertainty concerning what uses of FR may be acceptable, and under what circumstances.[15]

At worse, we fear that guidance without commensurate increases in OPC enforcement powers, new legislative restrictions or increased obligations for transparency and accountability will allow police forces to publicly commit to examining the guidance, while continuing to privately engage in activities that violate privacy rights and other fundamental freedoms.

Further, while we recognize the reason for this guidance being limited to police forces, we are concerned that other law enforcement and intelligence agencies may avoid scrutiny or shirk responsibility for adopting the guidance and framework the OPC proposes. This is particularly important given the close collaboration between agencies such as the Canadian Security Intelligence Service and the Canada Border Services Agency and the RCMP and other law enforcement agencies, for example via INSETs. We would suggest that guidance regarding what legal obligations police agencies have in regard to either requesting support from other agencies that may have access to facial recognition technology or the sharing of information derived from facial recognition technology be added to the final version of this guidance.

2. **Can this guidance be practically implemented?**

   What best practices and techniques might law enforcement agencies implement for operationalizing this guidance? Where operationalization may be difficult, please explain and provide examples and details when possible.

We believe that there are aspects of this guidance that can and should be implemented. This includes:

- Ensuring that any use of FR technology is lawfully authorized, including by obtaining a legal opinion. This should include the possibility that certain forms of FR can never be used, not to find ways for it *to* be used.
- That any FR technology being used is, itself, lawful (ie, that a third-party provider is not acting unlawfully)
- That privacy and other rights-based risks are appropriately addressed
- That police forces engage in public consultation before adopting new, rights-sensitive technology.
- Engage in Privacy Impact Assessments and obtain opinion of relevant privacy body
- Essential that law enforcement commit to transparency, accountability.

In order to operationalize, law enforcement agencies should ensure to dedicate resources to engaging in public consultation, hiring third party consultants and seeking out independent legal opinions.

[15] Office of the Privacy Commissioner of Canada, "Draft privacy guidance on facial recognition for police agencies," 10 June 2021. Online at: https://www.priv.gc.ca/en/opc-news/speeches/2021/s-d_20210610/.

However, again, we would be concerned that such efforts are used to justify and support the use of facial recognition technology, rather than truly ensure that it is being used (or not used, as the case may be) in a way that protects privacy and other rights.

We would also be concerned that while establishing many of these best practices could aid in minimizing risk and address privacy concerns associated with the adoption of any new technology, it can also lead to calls for greater resources to go to police forces at a time when there are real concerns about allocating resources away from policing. It is important that, in pushing police forces to implement these practices, that they are resourced via existing budgets. This is another area where a clear legal framework would help by granting clarity and reducing the need for consultation on, for example, facial recognition surveillance (ideally, but clearly limiting its use).

3. Are the recommendations in the "accuracy" section sufficient to help ensure police agencies meet their accuracy obligations in FR initiatives?

In your response, we invite comments on best practices for setting an appropriate threshold for FR matches and determining acceptable error rates, if any.

We do not have anything further to add to the "accuracy" section of the draft guidance, except that concerning the obligations of police agencies in regard to private vendors, the obligation to ensure external testing and accuracy should eventually be the subject of a legislative framework and not simply a best practice.

Finally, we would note that this is a crucial section of the guidance and that paragraph 78, in regard to the accuracy and fairness of face databases, is particularly relevant and often overlooked.

4. Can the recommendations in the guidance concerning the retention and disposal of personal information collected and used during a FR initiative be appropriately operationalized in a law enforcement context? If not, why?

While we do not maintain expertise on what challenges may be faced in operationalizing the guidance around retention and disposal of personal information collected during FR, we would argue that if proper handling of such information is not possible, then the use of facial recognition technology should not be authorized.

It is incumbent upon law enforcement agencies that when they take on new technology, they ensure that they have the policies and procedures – and resources – in place in order to ensure they are respecting the associated rights that are placed at risk. If implementing proper procedures for the retention and disposal of personal information is not possible, then the collection of such information simply should not take place.

5. What measures or practices can police agencies implement to help ensure any third parties involved in FR initiatives operate with lawful authority?

Third parties could include, for example, vendors of FR software or those in control of faceprint databases accessed by police.

In order to ensure that third parties operate with lawful authority, police agencies should contract independent review of their FR partner's operations.

Such third parties could be relevant privacy officials. At the same time, police forces should be cognizant that concerns with use of facial recognition go beyond privacy, and they would be well served to also engage human rights specialists.

The results of this independent review should be made public, with clear criteria for deciding the lawfulness of the third party's activities.

We would also suggest that an independent reviewer or government agency maintain a database of findings with regards to third party facial recognition vendors. Such a database would be helpful both to police agencies in deciding whether to partner with certain third parties and would be useful for researchers and legislators who are examining issues with facial recognition.

While it would require legislative changes, granting privacy commissioners greater enforcement powers in relation to third party providers would help to ensure compliance and to take action should it be found that third party operators are not in compliance with the law.

6. Do you foresee any negative consequences arising from the recommendations outlined in this guidance, and if so, what are they?

We do not see any negative consequences arising from any specific recommendation. However, we would reiterate our concern that, absent a legal framework, it is possible that police agencies will agree to self-regulated implementation of guidance as a way to avoid more stringent legal frameworks. We would also be concerned that the guidance be used by police services to legitimize their use of facial recognition technology. This is through no fault of the guidance, but rather the lack of action on the part of the federal, provincial and territorial governments to appropriately legislate in this area.

Feedback on the legal and policy framework for police use of FR

Currently, there are comprehensive statutory regimes governing the use of other forms of biometrics by law enforcement, namely, fingerprints and photographs under the *Identification of Criminals Act*, and DNA profiles under the *DNA Identification Act*.

Given the sensitive nature of these biometrics, and the substantial implications for individuals' rights and freedoms, their collection and use is limited to specific circumstances and purposes. There are also specific provisions governing their expungement. As faceprints are another form of biometric, we are seeking feedback on the legal and policy framework applicable to police use of FR in Canada.

7. Is police use of FR appropriately regulated in Canada under existing law? If not, what are your concerns about the way police use of FR is currently regulated, and what changes should be made to the current legal framework?

Would these changes be better addressed through a standalone regulatory framework specific to FR use, or through reform of privacy laws of general application?

As outlined above, and as made clear in the draft guidance, the current legislative framework is fragmented and unclear. We have already seen the impacts of this in the way police forces have adopted recognition technology with little to no regulation or repercussions. In some instances, it is possible that the lack of a legal framework resulted in law enforcement agencies (as well as specific officers) being unaware of their obligations – although this is granting an extreme benefit of the doubt. More likely, though, is that the lack of a binding legal framework simply allows agencies and officers to act without considering the impacts of this technology, and to do so without any consequences.

Overall, we believe this needs to be addressed through reform of privacy laws in general. This includes both private sector laws (for example, in regard to third party vendors) and public sector laws (those regulating law enforcement, as well as empowering privacy regulators). In particular, this should include (but not be limited to):

- Privacy commissioners require greater powers of enforcement in private sector, along with stronger order making powers in 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
- Legislation must bring greater clarity around the collection, retention and use of so-called "publicly availbale 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 that grant exceptions to law enforcement and national security agencies when it comes to divulging privacy and other rights-impacting methods, such as facial recognition

We are also open to the idea of specific legislation addressing the use of facial images, similar to the *Identification of Criminals Act* and the *DNA Identification Act*. However, we have

reservations about a piece-meal approach that deals with each kind of biometric data separately. Technology is constantly evolving, and new forms of biometric surveillance will most certainly be developed. A kind of *Facial Identification Act* may be effective, but the issue would need to be re-visited in the future for other emerging forms of surveillance. This is why we believe that addressing underlying gaps in Canada's privacy and biometric frameworks would be more effective and help "future proof" any legislative framework.

8. What protections should be granted to individuals whose biometric information is included in a faceprint database?

Protections might include, for example:

- *statutory rules related to notice that individuals are in the database*
- *a right to seek removal and destruction of one's faceprint*
- *a duty for police (or third parties) to automatically expunge faceprints in certain circumstances.*

We believe that all three of these examples are important and necessary as safeguards. We would possibly add two further safeguards:

- The ability of an individual to request to verify and/or contest the accuracy of the faceprint being held. These rules should apply to public and private faceprint databases alike, and should be extended to include all law enforcement and security agencies.
- Providing notice if images from a database are shared with another entity; for example, if one police force shares its image database with another, or with agencies such as the CBSA or CSIS.

Even before reaching this point, though, it is crucial that the government clarify the legal basis for creating and maintaining a faceprint database. What legal authorizations do either public or private sector entities have to be collecting facial images, retaining them (including for purposes other than for which they were shared), the possibility of commercializing that database, using it as the basis for taking enforcement action, etc. This is especially crucial for existing facial image databases that were created for purposes other than facial recognition.

This brings to mind the example of Insurance Corporation of British Columbia (ICBC) offering the use of its facial recognition system of drivers' licenses to the Vancouver Police Department in order to identify alleged rioters following a sporting match. The BC Privacy Commissioner determined at the time that, "the change in use of ICBC's facial recognition database was not authorized under FIPPA. ICBC must receive a warrant, subpoena or court order before it uses its facial recognition software to assist police with their investigations."

9. Should police use of FR, including the collection of faceprints, be limited to a defined set of purposes (such as serious crimes or humanitarian reasons, e.g., missing persons)? Should they be able to use or retain faceprints beyond those of individuals who have been arrested or convicted?

Are there circumstances in which police should never be allowed to use FR, or specific applications of FR that should not be permitted (i.e., 'no-go zones' such as the indiscriminate scraping of images from the Internet)? Should there be special rules for (or a prohibition against) the application of FR to youth?

Without knowing the full implication and breadth of facial recognition technology currently being used, it is difficult to say whether facial recognition technology should even be allowed for specific, limited purposes. While use for finding missing persons or other humanitarian reasons would appear uncontroversial, without associated protections regarding the establishing of facial databanks, accuracy of tools, and scope of use, there remains tremendous opportunity for error or even abuse. Before making any such determinations, it is necessary to have a more fulsome public debate and consultation around the use of facial recognition technology by law enforcement and related agencies.

Further, we would be concerned around who defines what is considered a serious crime and how it could justify broader use. While never implemented, the CBSA could likely argue that preventing individuals who are barred from Canada on serious grounds from entering would fall in this category, thereby justifying real-time surveillance of millions of travellers at airports. The same could be said of the RCMP's use of the previously mentioned private, 700,000 strong "terrorist" image database. As we have seen over the past twenty years, national security and anti-terrorism, considered areas of "serious crime", have been used to justify police and intelligence agency over-reach, particularly in the realm of surveillance.

While more discussion is needed to determine under which circumstances the use of facial recognition technology is acceptable, we already have enough information to establish clear no-go zones. ICLMG has already partnered with others to call for a ban on facial recognition surveillance by law enforcement and intelligence agencies. This would include a ban on:

- Facial recognition surveillance of public places, including public gathering places, protests and political events, sporting and entertainment events, etc.
- Facial recognition surveillance of the internet, including the scraping of publicly accessible websites
- The use of public facial image databases by law enforcement without judicial authorization when such databases are collected for purposes other than law enforcement

We would note that such no-go zones must apply both in Canada and internationally. For example, with CSIS being granted the power to collect "Foreign Datasets" under Bill C-59, it would be important to ensure that protections around the collection and use of facial images are not limited to individuals residing in Canada or Canadians abroad.

10. Are there any other important policy issues that should be addressed in relation to police use of FR?

This includes, for example, emerging legal, ethical, or social issues in relation to the development and implementation of faceprint databases by the police. If so, what are these issues, and how do you recommend they should be addressed?

We believe we have covered all the primary issues in the previous sections. In conclusion, though, we would reiterate our call for a ban on facial recognition surveillance, and a moratorium on all other uses of facial recognition by law enforcement agencies until a broader and more in-depth public consultation can take place with the goal of clarifying and adopting new legal requirements around the use of this emerging technology.