Consultation on Facial Recognition Technology

Brief Submitted by the

To the Standing Committee on Access to Information, Privacy and Ethics

House of Commons

April 15, 2022

Table of Contents

Introduction to the Ligue des droits et libertés

Founded in 1963, the Ligue des droits et libertés (LDL) is an independent, non-partisan non-profit organization whose purpose is to raise awareness, defend and promote the universality, indivisibility and interdependence of the rights recognized in the *International Bill of Human Rights*. The LDL is also affiliated with the International Federation for Human Rights (FIDH).

As it has done throughout its history, the LDL continues to fight against discrimination and all forms of abuse of power, in defense of civil, political, economic, social and cultural rights. It has influenced many public policies and helped create institutions dedicated to defending and promoting human rights, notably the adoption of the Quebec *Charter of Human Rights and Freedoms* and the creation of the Commission des droits de la personne et des droits de la jeunesse.

It lobbies governments at home and abroad to adopt legislation, measures and policies that are consistent with their commitments to international human rights instruments and to condemn rights violations for which they are responsible. The LDL carries out information, training and awareness-raising activities to broadly communicate rights issues relating to all aspects of society. These actions are aimed at the general public as well as certain groups that face discrimination in various contexts.

We applaud the Standing Committee on Access to Information, Privacy and Ethics for holding a consultation on facial recognition technology. Facial recognition is an artificial intelligence (AI) application that poses a serious threat to rights and freedoms. The LDL is very concerned that the current uncontrolled development of this technology is currently jeopardizing any claim to anonymity.

Introduction

We believe that federal and provincial privacy laws adopted in the 1980s and 1990s are totally inadequate in the age of the Internet, particularly with the unrestrained development of AI, including machine learning, deep learning and big data. Mass data siphoning on social networks, facial recognition, the Internet of Things, GPS tracking systems, AI-powered drones, smart city data sensors and voice assistants with comforting names: we are surrounded by technology that is being developed without public scrutiny or debate and appears to be on its way to wiping out any possibility of privacy, in addition to jeopardizing many other human rights. As author Nick Srnicek points out, ". . . the suppression of privacy is at the heart of this business model. This tendency involves constantly pressing against the limits of what is socially and legally acceptable in terms of data collection."[1]

Facial recognition is one of the most intrusive applications of AI in terms of rights and freedoms. And yet, it is becoming more and more insidious in our lives, without any real legal control. In this context, the use of facial recognition by police departments and national security agencies is particularly worrying.

Main issues raised by facial recognition

1. Threats to privacy and democracy

The Supreme Court of Canada has recognized that privacy is linked to the person, not the place; even in public places, the individual retains autonomy and the right to anonymity, which are components of the right to privacy:

> The mere fact that someone leaves the privacy of their home and enters a public space does not mean that the person abandons all of his or her privacy rights . . . we must recognize anonymity as one conception of privacy.[2]

This right to anonymity, a fundamental prerequisite to the self-fulfilment of individuals and the exercise of their democratic rights,[3] is directly compromised by facial recognition (FR). It makes mass surveillance of public places and online activities possible, opening the door to a totalitarian society.

2. Other human rights at risk

The **freedoms of expression and peaceful assembly** are incompatible with state and police surveillance. The Supreme Court emphasized that:

---

[1] Srnicek, Nick, *Platform Capitalism*, Polity Press, 2017, p. 101.

[2] *R v. Spencer,* [2014] 2 S.C.R. 212, para. 44. Online: https://canlii.ca/t/g7dzn

[3] Ibid., para. 15:

> This Court has long emphasized the need for a purposive approach to s. 8 that emphasizes the protection of privacy as a prerequisite to individual security, self-fulfilment and autonomy as well as to the maintenance of a thriving democratic society.

> A number of empirical studies have confirmed the "chilling effect" of government surveillance on online behaviour. These studies suggest that state electronic surveillance leads individuals to self-censor their online expression.[4]

The same "chilling effect" could extend to the rights to protest and to assemble. As the Citizen Lab notes: "Surveillance tools such as facial recognition technology threaten the anonymity of the crowd that has traditionally protected the identities of protesters."[5]

FR also affects the **right to equality**. Studies show numerous errors in identifying racialized people, especially Black women. FR can also stigmatize certain groups and communities by subjecting them to disproportionate surveillance based on biased historical data:

> Algorithms trained on dirty data reflect the dynamics that underlie the data's original collection and, thus, perpetuate disadvantage against the affected individuals and groups with protected characteristics.[6]

RF could also enable police profiling based on ethnicity, gender or other characteristics.

The **right to freedom** is also at risk. False matches can lead to serious consequences: abusive police street checks, unlawful arrest, arbitrary detention,[7] etc.

FR could also increase the risk of miscarriages of justice in cases where the identity of a suspect is in doubt. As researcher Castets-Renard points out, "there is a fear that the technology, often seen as infallible and credible in court, will reinforce the certainty of police officers, witnesses and judges."[8]

It could also compromise the physical and psychological safety of individuals by disclosing their identity (doxing[9]).

---

[4] *R. v. Mills*, [2019] 2 SCR 320, para. 99. Online: https://canlii.ca/t/hzv2r

[5] Robertson, Khoo and Song, *To Surveil and Predict. A Human Rights Analysis of Algorithmic Policing in Canada*, The Citizen Lab, 2020, p. 100. Online: https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysisof-algorithmic-policing-in-canada

[6] Ibid., p. 108.

[7] Ibid., p. 146:

> Individuals whose images are captured by facial recognition technology may suffer a number of civil liberties violations, including harms associated with being detained or arrested, or invasions of privacy occasioned by other police investigative techniques (e.g., searches of an individual's home, accessing the private contents of a confiscated computer, or strip searches on arrest). Such harms may occur even if the ensuing investigation does not ultimately lead to a criminal charge.

[8] Castets-Renard, *Use of facial recognition by police forces in the public space in Quebec and Canada. Elements of comparison with the United States and Europe — English Summary*, 2020, pp 9–10. Online: https://www.docdroid.com/sf8aLuy/report-use-of-facial-recognition-by-police-forces-in-the-public-space-in-quebec-and-canada-elements-of-comparison-with-the-united-states-and-europe-pdf

[9] Doxing: Searching for and publishing private information about an individual on the Internet.

3. Unproven effectiveness

Despite the threat it poses to human rights, and the significant costs involved,[10] few studies seem to establish the real effectiveness of FR:

> The growing use of these technologies contrasts sharply with the lack of empirical studies on their effectiveness and efficiency in practical application. Most of the available sources on the use of facial recognition for security purposes are limited to news articles and institutional work reports.[11] [TRANSLATION]

Another researcher states:

> Like video surveillance, their use is justified by risks, although their effectiveness is not proven (Castagnino, 2017; Gormand, 2017; Lemaire, 2019). For example, upstream intelligence would be more effective in preventing attacks. Moreover, to date, use of facial recognition to identify wanted persons, notably in the United Kingdom, shows little effectiveness.[12] [TRANSLATION]

4. Undemonstrated need

It is important to note that even if a law enforcement action or technique proves "effective," that does not mean that it is "necessary" or "justified." As the Supreme Court stated in 2019 in *Fleming*:

> [T]he mere fact that a police action was effective cannot be relied upon to justify its being taken if it interfered with an individual's liberty. For an intrusion on liberty to be justified, the common law rule is that it must be "reasonably necessary". If the police can reasonably attain the same result by taking an action that intrudes less on liberty, a more intrusive measure will not be reasonably necessary no matter how effective it may be. An intrusion upon liberty should be a measure of last resort, not a first option. To conclude otherwise would be generally to sanction actions that infringe the freedom of individuals significantly as long as they are effective. That is a recipe for a police state, not a free and democratic society.[13]

5. Security weaknesses

Given the specificity of biometric data, any security breach can lead to irreparable harm. Personal information (PI) leaks occur frequently and have increased in Canada in recent years. They have involved

---

[10] Sûreté du Québec's contract with Idemia is valued at more than $4.4 million. Online: https://www.sq.gouv.qc.ca/wp-content/uploads/2021/06/2021-06-08-contrat-societeidemia.pdf [Available in French only]

[11] Jacquet and Grossrieder, "Enjeux et perspectives de la reconnaissance faciale en sciences criminelles," *Criminologie*, 54 (1), 2021, pp. 135–170. Online: https://doi.org/10.7202/1076696ar

[12] Picaud, *La reconnaissance faciale : un marché en construction ?*, Association Futuribles, 2020. Online: https://halshs.archives-ouvertes.fr/halshs-02923698/document

[13] *Fleming v. Ontario*, 2019 SCC 45, para. 98. Online: https://canlii.ca/t/j2pd2

well-known financial and government institutions whose lack of concern for protecting personal or even sensitive data has been measurable.[14]

Lastly, the possible storage of biometric data outside of Canada or Quebec is likely to dilute the PI protection afforded by Canada's applicable laws.[15] [TRANSLATION]

6. Partnership with the private sector

The non-regulation of the lucrative FR private market[16] further increases the fear of abuse. Police departments (PDs) are a prime target for the sale of such products:

> The growing emphasis on facial recognition can be analyzed in terms of the lucrative market it covers. With regard to security, these markets are largely based on public clients.[17] [TRANSLATION]

The lack of control over the products sold and the limited expertise of PDs creates a dangerous relationship, as researcher Castets-Renard points out:

> Also, a dependency issue may arise if police forces become dependent on a private solution that they do not control. There is a risk of losing technological control and possibly being subjected to monetary pressure, which could result in a high financial cost for the administration.[18] [TRANSLATION]

The uncontrolled development of FR by the private sector can also lead to pernicious cooperation, with PDs recovering, for FR purposes, images and data collected in the private sector for other purposes. **In the current state of affairs, and for all these reasons, the LDL opposes the use of FR by PDs.**

---

[14] In Quebec, institutions include the Department of Families, the Régie de l'assurance maladie du Québec (RAMQ), the Department of Education and the Department of Revenue. At the federal level, the Canada Revenue Agency ". . . suspended 800,000 user accounts out of precaution after discovering that their sign-in information was accessible to 'unauthorized third parties.'" Online: https://www.journaldemontreal.com/2021/03/12/explosiondu-piratage-a-lagence-de-revenu-du-canada-800-000-comptes-ont-ete-compromis

[15] Castets-Renard, supra, p. 35:

> Moreover, the choice of foreign private operators also raises the risk of loss of control over state sovereignty, which is particularly worrying. The risks of interference and data security are high, especially if the data is stored outside Quebec or Canada.

[16] Global market estimated at $7 billion by 2024. See Picaud, supra.

[17] Ibid.

[18] Castets-Renard, supra, p. 35.

Facial recognition uses that should be banned

In our opinion, three FR uses should be immediately prohibited through legislation:

(a) mass surveillance of public places;

(b) online mass surveillance (digital platforms, social networks, etc.);

(c) use of image banks created by public agencies or departments.

Such legally questionable practices should be clearly prohibited by law. A moratorium should also apply to:

(d) all other uses of FR by PDs until a legislative framework ensuring respect for human rights is established.

(a) Mass surveillance of public places

The European Commission uses the term "remote biometric identification" for all biometric data that can help identify an individual:

> Remote biometric identification is when the identities of multiple persons are established with the help of biometric identifiers (fingerprints, facial image, iris, vascular patterns, etc.) at a distance, in a public space and in a continuous or ongoing manner by checking them against data stored in a database.[19]

Another term is "Live Facial Recognition Technology":

> Faces on video footage are extracted and then compared against the facial images in the reference database to identify whether the person on the video footage is in the database of images.[20]

[19] European Commission, *White Paper. On Artificial Intelligence*, 2020, Brussels. Online: https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

[20] European Union Agency for Fundamental Rights, *Facial recognition technology: fundamental rights considerations in the context of law enforcement*, 2019. Online: https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerationscontext-law

Many organizations are calling for a ban on such a practice, including Amnesty International,[21] the European Data Protection Supervisor[22] and the United Nations High Commissioner for Human Rights.[23]

On October 6, the European Parliament adopted a resolution to ban FR for mass surveillance purposes in public places:

> . . . a ban on any processing of biometric data, including facial images, for law enforcement purposes that leads to mass surveillance in publicly accessible spaces.[24]

The resolution also calls for a ban on other forms of biometric recognition:

> . . . the permanent prohibition of the use of automated analysis and/or recognition in publicly accessible spaces of other human features, such as gait, fingerprints, DNA, voice, and other biometric and behavioural signals.[25]

The LDL fully supports that request.

(b) Online mass surveillance (digital platforms, social networks, etc.)

The same permanent ban should apply to online surveillance by PDs. Citing *Clearview* as an example, the European Parliament "calls for a ban on the use of private facial recognition databases in law enforcement."[26]

In *Clearview*, Canada's commissioners ruled that a photo posted on the Internet is not public information. In the case of Quebec, the decision stated:

> There are no Quebec statutes under which personal information is deemed to be public solely based on the fact that it has been posted on social media or the Web. Moreover, the CAI has previously ruled that, even where personal information has been posted on a public website, it

---

[21] Amnesty International, *Amnesty International and more than 170 organisations call for a ban on biometric surveillance*, June 7, 2021. Online: https://www.amnesty.org/en/latest/news/2021/06/amnesty-international-and-more-than-170-organisations-call-for-a-ban-on-biometric-surveillance/

[22] European Data Protection Board, *EDPB & EDPS call for ban on use of AI for automated recognition of human features in publicly accessible spaces, and some other uses of AI that can lead to unfair discrimination*, June 21, 2021. Online: https://edpb.europa.eu/news/news/2021/edpb-edps-call-ban-use-ai-automated-recognition-humanfeatures-publicly-accessible_en

[23] United Nations High Commissioner for Human Rights, "New technologies must serve, not hinder, right to peaceful protest, Bachelet tells States," Geneva, June 25, 2020. Online: https://www.ohchr.org/en/press-releases/2020/06/new-technologies-must-serve-not-hinder-right-peaceful-protest-bachelet-tells

[24] European Parliament, *Resolution on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*, 2021, para. 31. Online: https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.html

[25] Ibid., para. 26.

[26] Ibid., para. 28.

> does not mean that the information may be used for other purposes without the consent of the person concerned. The fact that images are published on a website does not necessarily mean that their author has consented to their use by a third party.[27]

However, we believe that PDs cannot collect images from the Internet for FR purposes. It can be argued that this would be a violation of privacy laws and possibly an illegal search under the Quebec *Charter of Human Rights and Freedoms* and the *Canadian Charter of Rights and Freedoms.*[28]

(c) Use of image banks created by public agencies or departments

PDs should not be permitted to use image banks created by public agencies or departments in carrying out their duties.

PI collected by public agencies or departments must be collected for a specific purpose. It may only be used or disclosed for that purpose (or a compatible purpose).

In 2012, the British Columbia Privacy Commissioner prohibited the Insurance Corporation of British Columbia from making its driver photo database available to the police.[29] As summarized by the Office of the Privacy Commissioner of Canada in 2013:

> The BC Privacy Commissioner ruled that while ICBC can use the technology to detect and prevent driver's licence fraud, the corporation cannot use its database to help police identify riot suspects because this is a different purpose, of which customers were not notified.[30]

According to the LDL, PDs should be strictly prohibited from using government banks for FR purposes.

---

[27] Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta. PIPEDA Findings #2021-001, February 2021, para. 46. Online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/

[28] Commission des droits de la personne et des droits de la jeunesse, *Mémoire présenté à la Commission des institutions dans le cadre des consultations particulières et auditions publiques sur le projet de loi 64*, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, 2020, p. 55. Online: https://www.cdpdj.qc.ca/storage/app/media/publications/memoire_PL64_renseignements-personnels.pdf. This means that when the government collects data generated by online activity, without a search warrant and without obtaining the authorization of citizens, it is likely to violate section 24.1 of the Charter.

[29] Office of The Information & Privacy Commissioner for British Columbia, *Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia*, Investigation Report F12-01, February 16, 2012. Online: https://www.oipc.bc.ca/investigation-reports/1245

[30] Office of the Privacy Commissioner, *Automated Facial Recognition in the Public and Private Sectors*, 2013, p. 4. Online: https://www.priv.gc.ca/media/1765/fr_201303_e.pdf

(d) Moratorium on all other uses of facial recognition by police departments until a legislative framework ensuring respect for human rights is established

In the absence of evidence establishing the need for the use of FR by PDs, and in the absence of a legal framework that ensures respect for human rights, sets strict limits and ensures, in particular, transparency, accountability and judicial oversight of this technology, a moratorium should be imposed on its use, even with regard to mug-shot databases.

Mug-shot databases are not trivial. They include photos of people who have been acquitted or simply investigated. Moreover, photos are apparently not automatically destroyed once a file is closed.[31]

Another consideration is the discriminatory bias of such databases. As long as Indigenous, racialized and marginalized populations are over-represented in the justice and prison systems, they may also be subject to disproportionate FR surveillance.

The LDL's request is consistent with that of the European Parliament which, in its resolution of October 6, 2021:

> […] *Calls, however, for a moratorium on the deployment of facial recognition systems for law enforcement purposes that have the function of identification, unless strictly used for the purpose of identification of victims of crime, until the technical standards can be considered fully fundamental rights compliant, results derived are non-biased and non-discriminatory, the legal framework provides strict safeguards against misuse and strict democratic control and oversight, and there is empirical evidence of the necessity and proportionality for the deployment of such technologies; notes that where the above criteria are not fulfilled, the systems should not be used or deployed;*[32] [Our emphasis]

Conclusion

There are increasing calls for a moratorium on the use of this technology. On July 8, 2020, a coalition of organizations across Canada, including LDL, called on federal Public Safety Minister Bill Blair to ban the use of facial recognition by all police departments and federal intelligence agencies, including the Royal

---

[31] Robertson, Khoo and Song, supra, p. 91:

> Multiple law enforcement agencies in Canada report using (or are planning to use) facial recognition technology against their mug-shot databases. However, *mug-shot databases can contain photos of individuals who have never been charged with a criminal offence, who have had their charges withdrawn, or who have been found innocent of allegations*. Individuals have a constitutionally protected right to privacy in relation to their fingerprints and mug-shot images. In particular, the unauthorized retention of images is unconstitutional. In practice, however*, each police service has its own internal policies with respect to the destruction of biometric data, and those policies typically entail a discretionary, request-based, or even feebased process.* [Our emphasis]

[32] European Parliament, *Resolution on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters*, supra, para. 27.

Canadian Mounted Police. The group also called on Minister Blair to "launch a meaningful public consultation on all aspects of facial recognition technology in Canada" [TRANSLATION] and to "establish clear and transparent policies and legislation governing the use of facial recognition in Canada, including reforms to the *Personal Information Protection and Electronic Documents Act* and the *Privacy Act*."[16] [TRANSLATION]

For the LDL, **three facial recognition uses should be immediately prohibited through legislation:**

1. Mass surveillance of public places;
2. Online mass surveillance (digital platforms, social networks, etc.); and
3. Use of image banks created by public agencies or departments.

In addition, the LDL believes that **a moratorium on all other uses of facial recognition by police departments is necessary** until legislation commensurate with the issues at stake is passed, based on an informed and transparent public debate.