Facial Recognition Technology in Canada: A Brief Overview of Harms and Potential Benefits

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

Christelle Tesssono
May 4, 2022

EXECUTIVE SUMMARY

This submission recommends that the Standing Committee on Access to Information, Privacy, and Ethics implement a ban on the use of facial recognition technology by law enforcement.[1] The harms associated with misidentification and the lack of oversight of law enforcement agencies outweigh the potential benefits of its use. However, if the Committee wishes to use this technology under special circumstances, it should first develop the necessary safeguards to protect the privacy of Canadians.

A. INTRODUCTION

I grew up in Saint-Michel, a beautiful immigrant borough located in the Montreal East End. As a kid, I, like all the other children from the neighborhood, often played in the François-Perrault Park. The pool, tennis and basketball courts were quite popular during the summer months. And over the course of the pandemic, the park became a place where I could safely spend a lot of time reflecting during my daily walks.

In October 2021, the municipal police service announced the installation of CCTV surveillance cameras in the park to combat the rise of gun violence in the city.[2] There was no community consultation on this and like many people in the neighborhood, I was left confused and wondered what the footage would be used for. But more significantly, I was concerned about its impact on the frequent users of the park: immigrants, working class people, racialized youth, and elders. CCTV surveillance footage collected in places like François-Perrault Park is particularly useful when running facial recognition technology.

In June 2020, 77 privacy, human rights and civil liberties advocacy experts and groups called on Public Safety Minister, Bill Blair, to "enact a ban on facial recognition surveillance by federal law enforcement and intelligence" and "establish clear and transparent policies and laws regulating the use of facial recognition in Canada".[3] As the Canadian Civil Liberties Association argues, the police's use of facial recognition technology "points to a larger crisis in police accountability when acquiring and using emerging surveillance tools".[4] Given the growing market of companies supplying this technology to law enforcement and the continued absence of legislative provisions protecting Canadians, the Standing Committee on Access to Information, Privacy and Ethics needs to respond to the urgency of this matter before any more harm occurs.

I am deeply concerned about my community's safety and the impact facial recognition technology has on Canadians. To provide solutions to the challenges that I see in my community and in the country, I recommend a ban on the use of facial recognition technology by law

---

[1] Christelle is an Emerging Scholar at Princeton University's Center for Information Technology Policy (CITP). She served as a parliamentary intern at the House of Commons of Canada as part of the Parliamentary Internship Programme where she supported the legislative work of both opposition and government Members of Parliament. Views expressed in this submission are my own.

[2] Poirier, Y. (2021, October 25). *Le SPVM installera Neuf Nouvelles Caméras de Surveillance*. TVA Nouvelles. Retrieved April 27, 2022, from https://www.tvanouvelles.ca/2021/10/25/le-spvm-installera-neuf-nouvelles-cameras-de-surveillance

[3] *Ban on use of facial recognition surveillance by federal law enforcement and intelligence agencies*. (2020, July 8). https://ccla.org/wp-content/uploads/2021/07/facial-recognition-letter-08072020.pdf

[4] McPhail, B. (2021, November 17). *CCLA and privacy international collaborate on submissions regarding facial recognition guidelines for police agencies*. CCLA. Retrieved April 27, 2022, from https://ccla.org/privacy/ccla-and-privacy-international-collaborate-on-submissions-regarding-facial-recognition-guidelines-for-police-agencies/

enforcement. I begin with a brief outline of the harms of facial recognition technology. Next, I provide an overview of the legislative landscape in the United States to illustrate how different jurisdictions have dealt with this technology. Finally, I outline the key arguments supporting a ban and why those overcome the potential benefits of using facial recognition technology.

B. TECHNICAL OVERVIEW

What is facial recognition technology?

Facial recognition technology refers to computational tools used to identify, recognize, and analyze human faces in images, videos, and/or in real-time.[5] On a technical level, this broadly encompasses the set of systems that take in as input one or more images of faces, and outputs a score such as the similarity of two faces, the gender of one face, or a match to a face in a database.

What are the uses of facial recognition?

Facial recognition technology is used for a variety of purposes. The common uses are verification, identification, and characterization/categorization.

- *Verification*: Otherwise known as one-to-one (1:1) matching, the software confirms whether a face is the same as the one on record.[6] We encounter verification when trying to unlock our smartphones or accessing our bank account apps via facial recognition.

- *Identification*: This is often referred to as a one-to-many (1:n) system as it seeks to identify a specific individual using an image from them and comparing it to a database. It is commonly used when trying to identify an unknown individual – for example, when the police are comparing a photo to a database consisting of mugshots.[7]

- *Categorization/Characterization*: When software is used to ascribe characteristics such as gender, race, and emotions to a face.[8] There is a growing scholarship[9] and market[10] of facial recognition technology for characterization. However, despite the claims the literature and products make about the accuracy of their models, they have been widely criticized for reinforcing racism and sexism.[11]

---

[5] Kroll, J. A. (2022). *ACM TechBrief: Facial Recognition Technology*. ACM. https://dl.acm.org/doi/pdf/10.1145/3520137 p.2
[6] Crumpler, W., & Lewis, J. A. (2021). *How Does Facial Recognition Work?: A Primer*. Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep32894 p.3
[7] Balasubramaniam, L., Cooper-Simpson, C., Morello, J., & Pietrusiak, P. (2021). *Interim Report: Facial Recognition Technology in Canada*. Retrieved April 24, 2022, from https://ccla.org/wp-content/uploads/2021/07/Interim-Report-Compiled-BM.pdf p.8
[8] Crumpler, W., & Lewis, J. A. (2021). *How Does Facial Recognition Work?* p.3
[9] Peterson, J. C., Uddenberg, S., Griffiths, T. L., Todorov, A., & Suchow, J. W. (2022). Deep models of superficial face judgments. *Proceedings of the National Academy of Sciences*, *119*(17), e2115228119. https://doi.org/10.1073/pnas.2115228119
[10] *Facial personality analytics*. faception. (n.d.). Retrieved April 27, 2022, from https://www.faception.com/
[11] Stark, L., & Hutson, J. (2021). Physiognomic Artificial Intelligence. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3927300

What are the core problems with this technology?

1. *Inaccuracy and Discrimination*: A study conducted by the US National Institute of Standards and Technology (NIST) tested 189 different algorithms on 18 million photos to examine the models' accuracy. The study found a significantly higher proportion of incorrect matches amongst Asians, African Americans, and Indigenous peoples. Furthermore, the study found that women, children, and the elderly were also more likely to be misidentified by the algorithms.[12,13,14] Seeing as marginalized peoples experience over-surveillance from the police, inaccurate models put them at greater risk of misidentification and can lead to real-world harms.[15] In a recent account of this technology's failure in the United States, a young Black man was wrongly arrested and spent 10 days in detention at a corrections center and fought for a year to get his charges dropped.[16]

2. *Brittleness*: This technology is prone to adversarial attacks, meaning that actors can trick models into misidentification.[17] For example, scholarship has explored how wearing accessories such as a pair of glasses impacts these models significantly.[18]

3. *Interpretability*: Facial recognition systems develop their own sets of patterns and rules by analyzing large collections of data. It is very difficult for researchers to identify these rules and how the model makes its decisions. As a result, when someone is misidentified by a model, there is no clear way for the engineer who built the model to understand how this decision was made.[19]

4. *Unethical model development*: Facial recognition systems are trained on large datasets often comprising millions of images which have not been collected with meaningful consent.[20] For instance, Clearview AI admitted to collecting data available on websites such as Flickr, Google, and Facebook. In its investigation report, the Office of the Privacy Commissioner of Canada stated that Clearview AI argued that information collected was deemed publicly available to them and that there was no reasonable expectation of privacy for people who uploaded their pictures online. However, the OPC noted that PIPEDA, in addition to provincial privacy commissioners in British Columbia and Alberta, set out a distinction between publicly available and publicly accessible. As a

---

[12] Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face recognition vendor test part 3: Demographic effects* (NIST IR 8280; p. NIST IR 8280). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280

[13] This study found that darker-skinned females were the most misclassified group, with an error rate of 34,7% compared to lighter-skinned males who experienced an error rate of 0.8%: Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on fairness, accountability and transparency*. PMLR. https://proceedings.mlr.press/v81/buolamwini18a.html

[14] Melendez, S. (2018)."Uber Driver Troubles Raise Concerns About Transgender Face Recognition." *Fast Company*.

[15] Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Duke University Press.

[16] Johnson, K. (2022, March 7). *How wrongful arrests based on AI derailed 3 men's lives*. Wired. Retrieved April 25, 2022, from https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/

[17] Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). *Explaining and Harnessing Adversarial Examples*. https://doi.org/10.48550/ARXIV.1412.6572

[18] Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016). Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1528–1540. https://doi.org/10.1145/2976749.2978392

[19] Linardatos, P., Papastefanopoulos, V., & Kotsiantis, S. (2020). Explainable AI: A Review of Machine Learning Interpretability Methods. *Entropy*, *23*(1), 18. https://doi.org/10.3390/e23010018

[20] Balasubramaniam, L., et al. (2021). *Interim Report* p.6

result, information from social media websites does not fall under the publicly available exception set out by PIPEDA. Therefore, collection from these platforms can only be authorized with consent.[21]

C. LEGISLATIVE STRATEGIES IN THE UNITED STATES

At the federal level, the United States does not have a comprehensive statutory approach to regulating facial recognition technology. Instead, there exists a patchwork of state and local ordinances.[22] This patchwork can be divided into three legislative strategies: bans & moratoriums, permitted uses with oversight, and unregulated uses.

Moratoriums

Moratoriums refer to the temporary prohibition of the use of this technology. They are often used to provide policymakers with the time to develop legislation. In the United States, moratoriums have been adopted in very few states, such as California, Virginia, Vermont, and New York. They have a very limited scope as they only focus on certain uses of this technology, rather than encompassing all potential applications.

For instance, the State of California has banned law enforcement from "installing, activating, or using biometric surveillance with an officer camera or data collected by an officer camera" until 2023. The bill outlines how facial recognition technology poses "unique and significant threats to civil rights and civil liberties of residents and visitors" and has the potential to "diminish effective policing and public safety".[23] However, the bill does not prohibit the police from using this technology on footage from other sources they have access to.[24] While Vermont and Virginia also focus on law enforcement, their moratorium applies to all potential uses of facial recognition technology, does not have a set expiry date, and will instead be lifted only upon further legislation on the matter.[25] The State of New York has also implemented a ban on the use of this technology in public, private, and charter elementary and secondary schools, pending a report from the Commissioner of Education.[26]

Bans

Complete bans have been implemented by several municipal authorities across the United

---

[21] Office of the Privacy Commissioner of Canada. (2021). *Police use of facial recognition technology in Canada and the way forward: Special report to Parliament on the OPCs investigation into the RCMPs use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology*. https://epe.lac-bac.gc.ca/100/201/301/weekly_acquisitions_list-ef/2021/21-50/publications.gc.ca/collections/collection_2021/cpvp-opc/IP54-110-2021-eng.pdf p.15-16

[22] Feigelson, J., Gesser, A., Skrzypczyk, J., Gressel, A., & Gutierres, A.S. Face Forward: Strategies for Complying with Facial Recognition Laws. *Debevoise & Plimpton*. October 19, 2021. https://www.debevoisedatablog.com/2021/10/19/part-1-of-face-forward-strategies-for-complying-with-facial-recognition-laws/

[23] California State Assembly. *An act to add and repeal Section 832.19 of the Penal Code, relating to law enforcement, no. 1215*, (2019). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215

[24] Samsel, H. (2019, October 10). *California becomes third state to ban facial recognition software in police body cameras*. Security Today. Retrieved May 2, 2022, from https://securitytoday.com/articles/2019/10/10/california-to-become-third-state-to-ban-facial-recognition-software-in-police-body-cameras.aspx

[25] Feigelson, J. et al. Face Forward

[26] *Ibid*.

States. Similar to the moratoriums, the implementation of these bans has been motivated by concerns over civil liberties violations and the disproportionate negative impact the use of this technology has on racialized peoples.[27] As it currently stands, over 15 city councils have implemented these bans (e.g. Oakland, San Francisco, Boston, Portland, Minneapolis).[28] Like moratoriums, the scope of bans is often limited to law enforcement. However, there are a few notable exceptions: the State of Maryland bans employers from using facial recognition technology, and the City of Portland also bans private entities within its city limits.[29]

The implementation of bans and moratoriums in the United States is motivated by privacy and civil liberties concerns. Moreover, they both operate in the same fashion as they prohibit the use of facial recognition technology. However, they differ insofar as the ban makes the prohibition permanent, while the moratorium provides policymakers more time to develop a legislative framework. In essence, moratoriums defer addressing the privacy and human rights issues around the use of this technology.[30]

Permitted Use with Oversight: Massachusetts Law Enforcement

In July 2018 and March 2019, the American Civil Liberties Union (ACLU) of Massachusetts filed over 400 public records requests to get a better understanding of the use of facial recognition technology within the state.[31] In reviewing the released records, they discovered that government agencies, schools, private companies, town and city law enforcement had used facial recognition technology with little oversight.[32] This prompted state assembly legislators to pass the *Act Relative to Justice, Equity and Accountability in Law Enforcement in the Commonwealth* in December 2020.

The Act forbids law enforcement agencies in Massachusetts from "acquiring, accessing, or using any software that performs facial recognition except the Registry of Motor Vehicles".[33] It requires the agencies to obtain a warrant before requesting a search to the Registry of Motor Vehicles (except in emergency situations, such as immediate danger of death or serious physical injury). Furthermore, the Registry of Motor Vehicles is required to document each request from law enforcement and make it available in public record on its website. This includes information such as the total annual e numbers of searches by each police agency, searches conducted with a warrant, and searches conducted for emergency situations on an annual basis. And lastly, the act

---

[27] Guariglia, M. (2020, June 26). *Victory! Boston bans government use of face surveillance*. Electronic Frontier Foundation. Retrieved April 27, 2022, from https://www.eff.org/deeplinks/2020/06/victory-boston-bans-government-use-face-surveillance

[28] Feigelson, J. et al. Face Forward

[29] City of Portland has a 3 exceptions to the ban: 1) when needed to comply with local, state, or federal laws 2) when needed to verify individuals on personal or employer-issued communication devices (e.g. Apple's FaceID for iPhone), and lastly 3) in social media platforms such as Instagram and Snapchat. City of Portland. *Prohibit the acquisition and use of Face Recognition Technologies by City bureaus*, n190113 (2020). https://efiles.portlandoregon.gov/Record/13945278

[30] Owen, T., Ruths, D., Cairns, S., Parker, S., Reboul, C., Rowe, E., & Solomun, S. (2020). *Facial Recognition Moratorium Briefing #1: Implications of a Moratorium on the Use of Facial Recognition Technology in Canada*. McGill's Centre for Media, Technology and Democracy. https://www.mediatechdemocracy.com/work/facial-recognition-moratorium-briefing-1 p.11

[31] Peaslee, E. (2021, May 7). *Massachusetts pioneers rules for police use of Facial Recognition Tech*. NPR. Retrieved April 29, 2022, from https://www.npr.org/2021/05/07/982709480/massachusetts-pioneers-rules-for-police-use-of-facial-recognition-tech

[32] *The data for Justice Project: ACLU of Massachusetts - facial recognition in Massachusetts*. The Data for Justice Project | ACLU of Massachusetts. (2021, February 27). Retrieved April 29, 2022, from https://data.aclum.org/public-records/frt-ma/

[33] Massachusetts Police Association. (n.d.). *Legislative Summary: An Act relative to justice, equity and accountability in law enforcement in the Commonwealth*. Massachusetts Police Association. https://masspolice.com/wp-content/uploads/2020/07/legislativesummary.pdf p.4

establishes a legislative commission tasked with studying the use of facial recognition by the Massachusetts Department of Transportation.

The Act is one of the first attempts in the state and in the country to regulate facial recognition technology. However, privacy experts, most notably the ACLU of Massachusetts do not believe the bill goes far enough. The organization's executive director, Carol Rose, argues that, while it "prevents the use of it by the police when it's not relevant to an investigation" – which is important – it represents a "fairly low standard".[34]

Jurisdictions with no legislation

In jurisdictions with no legislation, the use of facial recognition technology by the police occurs with no oversight. Civilians may be arrested after the use of this technology without their knowledge. False arrests may occur because of the inaccuracy of facial recognition, as was the case with Robert Williams, Michael Oliver, and Nijeer Parks. Williams, Oliver, and Parks were wrongly arrested in states and cities with no protections against facial recognition surveillance by law enforcement. Although charges were dropped against them, these arrests bear heavy consequences. Parks spent 10 days in jail, and it took a year for his charges to be dropped. Williams was arrested by the police in front of his 4-year-old daughter and was held by the police for 30 hours. Oliver lost his job because of the false arrest and spent over a year building his life back to normal.[35]

D. RECOMMENDATIONS

1. **Ban the use of automated facial recognition technology by law enforcement.**
2. **Including, banning the use of real-time and recorded footage for automated facial recognition technologies by law enforcement;**
3. **And banning law enforcement from procuring automated facial recognition technologies from third-party entities.**

Reasons for banning facial recognition technology use by law enforcement

The technical issues associated with facial recognition are not solvable in the foreseeable future. As discussed in my technical overview, automated facial recognition technologies have been tested and proven to be inaccurate. Researchers continue to experience difficulty when attempting to interpret why and when models misidentify people.

Moreover, the inaccuracy of the technology exacerbates discrimination against historically marginalized groups. Research has proven that this technology discriminates against women, racialized peoples, youth, and the elderly. As a result of racial profiling, these groups are at further risk of harms associated with surveillance.

And lastly, companies that provide facial recognition technology to law enforcement agencies are susceptible to data breaches. Facial recognition databases contain very sensitive

---

[34] Peaslee, E. *Massachusetts pioneers rules for police use of Facial Recognition Tech*.
[35] Johnson, K. (2022, March 7). *How wrongful arrests based on AI derailed 3 men's lives*. Wired. Retrieved April 25, 2022, from https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/

information, and we have yet to account for the harms that occur when these databases are breached. For example, in 2020, police stations in Toronto reported a security breach which compromised the list of customers, the number of user accounts and the number of searches that had been conducted using facial recognition technology.[36]

Counter-arguments based on the potential benefits of the technology are not persuasive

Critics of a ban point to the potential benefits associated with using facial recognition technology. Police agencies say they have been able to solve investigations faster and at a cheaper cost thanks to this technology.[37] Notably, they point to it successfully being used to find children who are victims of abuse and their perpetrators.[38]

Children's safety must be taken seriously, and I agree with critics that having all the tools at our disposal is imperative. However, I do not believe that facial recognition technology is the tool we need to solve these investigations. Research shows that facial recognition technology is "not designed to consider children and may, in fact, perform poorly when applied to children".[39] As a result, even in optimistic cases, the technical and social challenges associated with the use of this technology are very much present and cannot be ignored.[40]

Following the attempted insurrection in the U.S. Capitol on January 6th, 2021, law enforcement in the United States has been working to identify the perpetrators by using facial recognition technology.[41] This has sparked a lot of debate, specifically about whether this technology should have been used in cases of national emergencies such as these. Looking back at the "freedom convoy" occupation in Ottawa this past year, the question should also be raised here. Could we justify using this technology in Canada for cases such as these? I argue we should not.

Despite its potential usefulness in extreme circumstances like these, banning facial recognition technology remains important because, in the absence of oversight, law enforcement in Canada cannot be held accountable. We have seen how the presence of systemic racism in law enforcement puts racialized Canadians at risk. Moreover, facial recognition technology is used to oppress and surveil in other countries. By implementing a ban, our government has an opportunity to show the international community how to use technology responsibly.

---

[36] Owen, T. et al. *Facial Recognition Moratorium Briefing #1* p.8
& Aguilar, B. (2020, February 26). *Company behind controversial facial recognition software used by Toronto Police Suffers Data Breach*. Toronto. Retrieved April 26, 2022, from https://toronto.ctvnews.ca/company-behind-controversial-facial-recognition-software-used-by-toronto-police-suffers-data-breach-1.4829200

[37] Hill, K. (2021, March 18). *What happens when our faces are tracked everywhere we go?* The New York Times. Retrieved April 28, 2022, from https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html

[38] Hill, K., & Dance, G. J. X. (2020, February 7). *Clearview's facial recognition app is identifying child victims of abuse*. The New York Times. Retrieved April 26, 2022, from https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html

[39] Berman, G., Carter, K., García-Herranz, M. and Sekara, V. (2020). *Digital Contact Tracing and Surveillance during COVID-19: General and Child-specific Ethical Issues*. https://www.unicef-irc.org/publications/pdf/WP2020-01.pdf. p.15

[40] Stark, L. (2021). *Facial Recognition & Canadian Youth* (Kids & Technology Essay Series). McGill's Centre for Media, Technology and Democracy. https://www.mediatechdemocracy.com/work/facial-recognition-and-canadian-youth

[41] Kelley, J. (2021, January 12). *Face surveillance and the capitol attack*. Electronic Frontier Foundation. Retrieved May 2, 2022, from https://www.eff.org/deeplinks/2021/01/face-surveillance-and-capitol-attack

In its investigation on Clearview AI, the Office of the Privacy Commissioner of Canada found that the Royal Canadian Mounted Police "erroneously told our office that it was not using Clearview AI" and that when it later acknowledged its use, it "did not satisfactorily account for the vast majority of the searches it made".[42] The Office of the Privacy Commissioner argued that the "RCMP has serious and systemic gaps in its policies and systems to track, identify, assess and control novel collections of personal information," which is a critical element needed to comply with the law.[43] In the absence of provisions protecting biometric information, Canadians are at "greater risk of surveillance by law enforcement as well as violations of our fundamental rights protected under the Charter of Rights and Freedoms".[44] The "cumulative weaknesses in Canada's legal system can be exploited by law enforcement and tech companies," as was the case with the use of Clearview AI by the RCMP. Without strong safeguards, Canadians remain at risk of greater harms, both at the national and international level.[45]

In June of 2021, the Standing Committee on Public Safety and National Security published a report on Systemic Racism in Policing in Canada. The report outlined in detail the ways in which systemic racism affected racialized Canadians, more specifically Indigenous women, girls, Two-Spirit peoples, and other members of the LGBTQ+ community. The effect of systemic racism included "disproportionate exposure to police discrimination, such as racial profiling and excessive use of force", but also in "a failure of police agencies to protect these women from gender-based violence and homicide".[46] The committee report included a list of 42 recommendations, which have yet to be fully implemented and whose consequences have yet to be examined. As a result, deploying facial recognition technology, an inaccurate and ineffective tool, poses significant risks in Canada to overpoliced communities. Reports of police investigating activists and their supporters are not new; for example, the Toronto police compiled intelligence email reports on Black Lives Matters activists in 2016.[47]

Internationally, facial recognition technology is being used to oppress marginalized communities. For instance, Uighurs in China are being racially profiled by law enforcement through facial recognition technology, as is the case in Brazil for Afro-Brazilians.[48,49] And in Myanmar, the military junta uses it to counter dissent by surveilling civilians.[50] Given these

---

[42] Privacy Commissioner of Canada. *Police use of facial recognition technology in Canada* p.2-3
[43] *Ibid*, p.3
[44] Stevens, Y., & Brandusescu, A. (2021). *Weak Privacy, Weak Procurement: The State of Facial Recognition in Canada*.*https://www.mediatechdemocracy.com/work/weak-privacy-weak-procurement-the-state-of-facial-recognition-in-canada* p.13
[45] Stevens, Y., & Brandusescu, A. *Weak Privacy* p.16
[46] Canada, Parliament. Standing Committee on Public Safety and National Security. (2021). *Systemic Racism in Policing in Canada*. 43rd Parl, 2nd sess. Retrieved from the Parliament of Canada website: https://www.ourcommons.ca/Content/Committee/432/SECU/Reports/RP11434998/securp06/securp06-e.pdf p.45
[47] Davis, S. (2018, May 3). *Police monitored black lives matter Toronto protesters in 2016, documents show | CBC News*. CBCnews. Retrieved May 2, 2022, from https://www.cbc.ca/news/canada/toronto/police-monitored-black-lives-matter-toronto-protesters-in-2016-documents-show-1.4645628
[48] Ormerod, A. G. (2022, April 22). *How AI reinforces racism in Brazil*. Rest of World. Retrieved April 26, 2022, from https://restofworld.org/2022/how-ai-reinforces-racism-in-brazil/
[49] Mozur, P. (2019, April 14). *One month, 500,000 face scans: How China is using A.I. to profile a minority*. The New York Times. Retrieved April 26, 2022, from https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html
[50] *Myanmar: Facial recognition system threatens rights*. Human Rights Watch. (2021, March 12). Retrieved April 26, 2022, from https://www.hrw.org/news/2021/03/12/myanmar-facial-recognition-system-threatens-rights

harmful practices, I believe the Canadian government has an opportunity here to show the international community how to effectively protect civilians from law enforcement surveillance.

As a fallback, the Committee could consider enacting a moratorium

Should the Committee come to the decision to allow the use of facial recognition technology under special circumstances, it should build the legislative framework to ensure that Canadians are not put at risk of misidentification and mass surveillance. A moratorium in this case would provide the time to build this legislative framework. It could include, but not be limited to, ensuring that facial recognition technology is used only when court-issued warrants are made in formal criminal investigations. Furthermore, facial recognition technology in these cases should only be used on recorded footage, instead of real-time footage.

Moreover, I would urge the Committee to follow the policy recommendations outlined by the Office of the Privacy Commissioner of Canada and researchers at institutions such as the Canadian Civil Liberties Association, Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, and Citizen Lab. [51],[52] The Center on Privacy & Technology at Georgetown University in the United States offers a legislative model and 30 key recommendations I urge Canadian policy makers to follow.[53] And most notably, the Centre for Media, Technology and Democracy outlines key considerations such as the development of a data governance framework and accountability mechanisms.[54] In Europe, the Law Enforcement Directive is also a model of policy to follow.[55]

But most importantly, I urge the committee to center the voices of victims of police brutality, who include, but are not limited to LGBTQ+, disabled, poor, immigrant and undocumented, Black, Indigenous, and other racialized peoples. Their experiences must inform regulation in the country, as they hold key knowledge about the extent to which police surveillance impacts them and their communities.

---

[51] See following reports: Balasubramaniam, L. et al. (2021). *Interim Report,* Israel, T. (2020). Facial recognition at a crossroads: Transformation at our borders and beyond. *Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC).* *https://cippic.ca/uploads/FR_Transforming_Borders.pdf* , Robertson, K., Khoo, C., & Song, Y. (2020). *To surveil and predict: A human rights analysis of algorithmic policing in Canada*. Citizen Lab and International Human Rights Program, University of Toronto. https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf

[52] Office of the Privacy Commissioner of Canada. (2022, May 2). *News release: Privacy Regulators Call for legal framework limiting police use of facial recognition technology*. Privacy regulators call for legal framework limiting police use of facial recognition technology - Office of the Privacy Commissioner of Canada. Retrieved May 4, 2022, from https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/nr-c_220502/

[53] Garvie, C. (2016). *The perpetual line-up: Unregulated police face recognition in America*. Georgetown Law, Center on Privacy & Technology. https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf

[54] Owen, T., Ruths, D., Cairns, S., Reboul, C., Rowe, E., & Solomun, S. (2020). *Facial Recognition Moratorium Briefing #2: Conditions for Lifting a Moratorium on Public Use of Facial Recognition Technology in Canada*. McGill's Centre for Media, Technology and Democracy. https://www.mediatechdemocracy.com/work/facial-recognition-moratorium-briefing-1-wfgs7

[55] Directive (EU) 2016/680 (Law Enforcement Directive), Article 10. https://eur-lex.europa.eu/eli/dir/2016/680/oj

E. CONCLUSION

Neighborhoods that house working-class peoples, immigrants, and people of color have been the site for racial profiling for decades in Montreal.[56] In the name of safety, secondary school students in Saint-Michel encounter municipal police officers everyday outside the school premises waiting for them. Apparently, this police presence is meant to foster links between the youth and the officers, to eliminate conflict. However, this only results in students being put at greater risk of profiling. But more concerning is the fact that plans to deploy a similar program in elementary schools are well underway.[57] With youth bearing the brunt of this surveillance through street checks and excessive use of force, I am deeply concerned about the potential ramifications of the use of facial recognition technology.

Facial recognition technology is part of a broader trend on algorithmic policing. As such, this Committee's future work should look to regulate the other types of automated tools used by law enforcement. Furthermore, although facial recognition technology is already used widely in law enforcement, it can also be used in the commercial sector and by other government agencies. As a result, I would urge this Committee to also consider the biometric technologies, which include but are not limited to facial recognition, in those sectors.

---

[56] Livingston, A.-M., Rutland, T., Alix, S., Jean-Claude, R., Abidou, Z. Y., Guillaume, W., Harim, R., Milien, M.-K., & Rémé, L. (2018). *Le profilage racial dans les pratiques policières: Points de vue et expériences de jeunes racisés à Montréal*. https://drive.google.com/file/d/1yCYtzCL-_mTHEZmsVv0hJu4yHL7j3n3Z/view

[57] Marin, S. (2022, April 25). *Avant les coups de feu, Le filet de prévention du spvm dans saint-michel*. Le Devoir. Retrieved April 29, 2022, from https://www.ledevoir.com/societe/703068/montreal-avant-les-coups-de-feu-le-filet-de-prevention-du-spvm-dans-saint-michel

References List

Aguilar, B. (2020, February 26). *Company behind controversial facial recognition software used by Toronto Police Suffers Data Breach*. Toronto. Retrieved April 26, 2022, from https://toronto.ctvnews.ca/company-behind-controversial-facial-recognition-software-used-by-toronto-police-suffers-data-breach-1.4829200

Balasubramaniam, L., Cooper-Simpson, C., Morello, J., & Pietrusiak, P. (2021). *Interim Report: Facial Recognition Technology in Canada*. Retrieved April 24, 2022, from https://ccla.org/wp-content/uploads/2021/07/Interim-Report-Compiled-BM.pdf

Ban on use of facial recognition surveillance by federal law enforcement and intelligence agencies. (2020, July 8). https://ccla.org/wp-content/uploads/2021/07/facial-recognition-letter-08072020.pdf

Berman, G., Carter, K., García-Herranz, M. and Sekara, V. (2020). *Digital Contact Tracing and Surveillance during COVID-19: General and Child-specific Ethical Issues*. https://www.unicef-irc.org/publications/pdf/WP2020-01.pdf.

Browne, S. (2015). *Dark matters: On the surveillance of blackness*. Duke University Press.

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. In *Conference on fairness, accountability and transparency*. PMLR. https://proceedings.mlr.press/v81/buolamwini18a.html

California State Assembly. *An act to add and repeal Section 832.19 of the Penal Code, relating to law enforcement, no. 1215*, (2019). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215

Canada, Parliament. Standing Committee on Public Safety and National Security. (2021). *Systemic Racism in Policing in Canada*. 43rd Parl, 2nd sess. Retrieved from the Parliament of Canada website: https://www.ourcommons.ca/Content/Committee/432/SECU/Reports/RP11434998/securp06/securp06-e.pdf

City of Portland. *Prohibit the acquisition and use of Face Recognition Technologies by City bureaus*, n190113 (2020). https://efiles.portlandoregon.gov/Record/13945278

Crumpler, W., & Lewis, J. A. (2021). *How Does Facial Recognition Work?: A Primer*. Center for Strategic and International Studies (CSIS). http://www.jstor.org/stable/resrep32894

Davis, S. (2018, May 3). *Police monitored black lives matter Toronto protesters in 2016, documents show | CBC News*. CBCnews. Retrieved May 2, 2022, from https://www.cbc.ca/news/canada/toronto/police-monitored-black-lives-matter-toronto-protesters-in-2016-documents-show-1.4645628

Facial personality analytics. faception. (n.d.). Retrieved April 27, 2022, from https://www.faception.com/

Feigelson, J., Gesser, A., Skrzypczyk, J., Gressel, A., & S. Gutierres, A.S. "Face Forward: Strategies for Complying with Facial Recognition Laws." *Debevoise & Plimpton*. October 19, 2021. https://www.debevoisedatablog.com/2021/10/19/part-1-of-face-forward-strategies-for-complying-with-facial-recognition-laws/

Garvie, C. (2016). *The perpetual line-up: Unregulated police face recognition in America*. Georgetown Law, Center on Privacy & Technology. https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf

Goodfellow, I. J., Shlens, J., & Szegedy, C. (2014). *Explaining and Harnessing Adversarial Examples*. https://doi.org/10.48550/ARXIV.1412.6572

Grother, P., Ngan, M., & Hanaoka, K. (2019). *Face recognition vendor test part 3: Demographic effects* (NIST IR 8280; p. NIST IR 8280). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8280

Guariglia, M. (2020, June 26). *Victory! Boston bans government use of face surveillance*. Electronic Frontier Foundation. Retrieved April 27, 2022, from https://www.eff.org/deeplinks/2020/06/victory-boston-bans-government-use-face-surveillance

Hill, K. (2021, March 18). *What happens when our faces are tracked everywhere we go?* The New York Times. Retrieved April 28, 2022, from https://www.nytimes.com/interactive/2021/03/18/magazine/facial-recognition-clearview-ai.html

Hill, K., & Dance, G. J. X. (2020, February 7). *Clearview's facial recognition app is identifying child victims of abuse*. The New York Times. Retrieved April 26, 2022, from

https://www.nytimes.com/2020/02/07/business/clearview-facial-recognition-child-sexual-abuse.html

Israel, T. (2020). Facial recognition at a crossroads: Transformation at our borders and beyond. *Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)*. *https://cippic.ca/uploads/FR_Transforming_Borders.pdf*

Johnson, K. (2022, March 7). *How wrongful arrests based on AI derailed 3 men's lives*. Wired. Retrieved April 25, 2022, from https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/

Johnson, K. (2022, March 7). *How wrongful arrests based on AI derailed 3 men's lives*. Wired. Retrieved April 25, 2022, from https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/

Kelley, J. (2021, January 12). *Face surveillance and the capitol attack*. Electronic Frontier Foundation. Retrieved May 2, 2022, from https://www.eff.org/deeplinks/2021/01/face-surveillance-and-capitol-attack

Kroll, J. A. (2022). *ACM TechBrief: Facial Recognition Technology*. ACM. p.2 https://doi.org/10.1145/352013

Linardatos, P., Papastefanopoulos, V., & Kotsiantis, S. (2020). Explainable AI: A Review of Machine Learning Interpretability Methods. *Entropy*, *23*(1), 18. https://doi.org/10.3390/e23010018

Livingston, A.-M., Rutland, T., Alix, S., Jean-Claude, R., Abidou, Z. Y., Guillaume, W., Harim, R., Milien, M.-K., & Rémé, L. (2018). *Le profilage racial dans les pratiques policières: Points de vue et expériences de jeunes racisés à Montréal*. https://drive.google.com/file/d/1yCYtzCL-_mTHEZmsVv0hJu4yHL7j3n3Z/view

Marin, S. (2022, April 25). *Avant les coups de feu, Le filet de prévention du spvm dans saint-michel*. Le Devoir. Retrieved April 29, 2022, from https://www.ledevoir.com/societe/703068/montreal-avant-les-coups-de-feu-le-filet-de-prevention-du-spvm-dans-saint-michel

Massachusetts Police Association. (n.d.). *Legislative Summary: An Act relative to justice, equity and accountability in law enforcement in the Commonwealth*. Massachusetts Police Association. https://masspolice.com/wp-content/uploads/2020/07/legislativesummary.pdf

McPhail, B. (2021, November 17). *CCLA and privacy international collaborate on submissions regarding facial recognition guidelines for police agencies*. CCLA. Retrieved April 27, 2022, from https://ccla.org/privacy/ccla-and-privacy-international-collaborate-on-submissions-regarding-facial-recognition-guidelines-for-police-agencies/

Melendez, S. (2018)."Uber Driver Troubles Raise Concerns About Transgender Face Recognition." *Fast Company*.

Mozur, P. (2019, April 14). *One month, 500,000 face scans: How China is using A.I. to profile a minority*. The New York Times. Retrieved April 26, 2022, from https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

Myanmar: Facial recognition system threatens rights. Human Rights Watch. (2021, March 12). Retrieved April 26, 2022, from https://www.hrw.org/news/2021/03/12/myanmar-facial-recognition-system-threatens-rights

Office of the Privacy Commissioner of Canada. (2021). *Police use of facial recognition technology in Canada and the way forward: Special report to Parliament on the OPCs investigation into the RCMPs use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology*. https://epe.lac-bac.gc.ca/100/201/301/weekly_acquisitions_list-ef/2021/21-50/publications.gc.ca/collections/collection_2021/cpvp-opc/IP54-110-2021-eng.pdf

Office of the Privacy Commissioner of Canada. (2022, May 2). *News release: Privacy Regulators Call for legal framework limiting police use of facial recognition technology*. Privacy regulators call for legal framework limiting police use of facial recognition technology - Office of the Privacy Commissioner of Canada. Retrieved May 4, 2022, from https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/nr-c_220502/

Ormerod, A. G. (2022, April 22). *How AI reinforces racism in Brazil*. Rest of World. Retrieved April 26, 2022, from https://restofworld.org/2022/how-ai-reinforces-racism-in-brazil/

Owen, T., Ruths, D., Cairns, S., Parker, S., Reboul, C., Rowe, E., & Solomun, S. (2020). *Facial Recognition Moratorium Briefing #1: Implications of a Moratorium on the Use of Facial Recognition Technology in Canada*. McGill's Centre for Media, Technology and Democracy. https://www.mediatechdemocracy.com/work/facial-recognition-moratorium-briefing-1

Owen, T., Ruths, D., Cairns, S., Reboul, C., Rowe, E., & Solomun, S. (2020). *Facial Recognition Moratorium Briefing #2: Conditions for Lifting a Moratorium on Public Use of Facial Recognition Technology in Canada*. McGill's Centre for Media, Technology

and Democracy. https://www.mediatechdemocracy.com/work/facial-recognition-moratorium-briefing-1-wfgs7

Peaslee, E. (2021, May 7). *Massachusetts pioneers rules for police use of Facial Recognition Tech*. NPR. Retrieved April 29, 2022, from https://www.npr.org/2021/05/07/982709480/massachusetts-pioneers-rules-for-police-use-of-facial-recognition-tech

Peterson, J. C., Uddenberg, S., Griffiths, T. L., Todorov, A., & Suchow, J. W. (2022). Deep models of superficial face judgments. *Proceedings of the National Academy of Sciences*, *119*(17), e2115228119. https://doi.org/10.1073/pnas.2115228119

Poirier, Y. (2021, October 25). *Le SPVM installera Neuf Nouvelles Caméras de Surveillance*. TVA Nouvelles. Retrieved April 27, 2022, from https://www.tvanouvelles.ca/2021/10/25/le-spvm-installera-neuf-nouvelles-cameras-de-surveillance

Robertson, K., Khoo, C., & Song, Y. (2020). *To surveil and predict: A human rights analysis of algorithmic policing in Canada*. Citizen Lab and International Human Rights Program, University of Toronto. https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf

Samsel, H. (2019, October 10). *California becomes third state to ban facial recognition software in police body cameras*. Security Today. Retrieved May 2, 2022, from https://securitytoday.com/articles/2019/10/10/california-to-become-third-state-to-ban-facial-recognition-software-in-police-body-cameras.aspx

Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016). Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 1528–1540. https://doi.org/10.1145/2976749.2978392

Stark, L. (2021). *Facial Recognition & Canadian Youth* (Kids & Technology Essay Series). McGill's Centre for Media, Technology and Democracy. https://www.mediatechdemocracy.com/work/facial-recognition-and-canadian-youth

Stark, L., & Hutson, J. (2021). Physiognomic Artificial Intelligence. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3927300

Stevens, Y., & Brandusescu, A. (2021). *Weak Privacy, Weak Procurement: The State of Facial Recognition in Canada*.*https://www.mediatechdemocracy.com/work/weak-privacy-weak-procurement-the-state-of-facial-recognition-in-canada*

The data for Justice Project: ACLU of Massachusetts - facial recognition in Massachusetts. The Data for Justice Project | ACLU of Massachusetts. (2021, February 27). Retrieved April 29, 2022, from https://data.aclum.org/public-records/frt-ma/