Canadian human rights commission | Commission canadienne des droits de la personne

CANADIAN HUMAN RIGHTS COMMISSION

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

Facial Recognition Technology use in Policing

April 2022

INTRODUCTION:

"Technology and privacy are fundamental to the next generation of human rights. Everyone in Canada should be able to benefit from technology without fear."

Marie-Claude Landry, Chief Commissioner of the Canadian Human Rights Commission

The Canadian Human Rights Commission (the CHRC) is pleased to provide this report as a written submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics on the use of facial recognition technology (FRT) in policing.

The CHRC is currently studying broader artificial intelligence (AI) and human rights issues, and this initial report is focused on consideration of FRT use in policing in the federal jurisdiction and the Royal Canadian Mounted Police (RCMP). An earlier version of this report was previously provided to the Office of the Privacy Commission of Canada (OPC), in response to their request for input on the *Draft privacy guidance on facial recognition for police agencies*[1] which was jointly developed and issued by the federal and provincial privacy agencies.

The CHRC is Canada's national human rights institution, accredited "A-status" by the Global Alliance of National Human Rights Institutions.[2] The CHRC was established by Parliament through the Canadian Human Rights Act (CHRA) in 1977.[3] It has a broad mandate to promote and protect human rights. The Constitution of Canada divides jurisdiction for human rights matters between the federal and provincial or territorial governments. The CHRC, pursuant to the CHRA, has jurisdiction to receive discrimination complaints against federal government departments and agencies, Crown corporations, First Nations governments, and federally regulated private sector organizations such as banks, airlines, and telecommunications companies. The CHRC also has a broad mandate to support research, raise public awareness, and issue reports on human rights issues. Provincial and territorial governments have their own human rights codes and are responsible for provincially/territorially-regulated sectors such as provincial and municipal governments, schools, universities, hospitals, and most businesses.

POSITION OF CANADIAN HUMAN RIGHTS COMMISSION:

The CHRC's position is that:

1. **the current legal and policy framework for the use of FRT in policing is inadequate, and a new framework is needed;**
2. **Parliament should immediately undertake a study that examines the use of FRT in policing and puts in place a new legal framework;**
3. **a new framework must take a human rights based approach;**
4. **a new framework must fully consider and integrate human rights protections for children and youth, and;**
5. **until a new legal and policy framework is put in place, FRT use in policing should be prohibited through a moratorium.**

---

1 Office of the Privacy Commissioner of Canada, *Draft privacy guidance on facial recognition for police agencies*, 2021 www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/gd_frt_202106/

2 Global Alliance of National Human Rights Institutions ganhri.org/membership/

3 Canadian Human Rights Act R.S.C., 1985, c. H-6 at laws-lois.justice.gc.ca/eng/acts/h-6/page-1.html

1. **The CHRC's position is that the current legal and policy framework for the use of FRT in policing is inadequate, and a new framework is needed**.

1.1. The CHRC applauds the OPC on its recent investigations[4] and special report to Parliament[5] raising concerns about the use of FRT in policing in Canada. The CHRC shares many of the views of the OPC reflected in these reports, in the Draft Guidance and consultation documents. The CHRC looks forward to working together to continue to address issues at the intersection of human rights and privacy.

1.2. AI-powered FRT is a new and rapidly growing part of the technology sector, worth billions of dollars. It often relies on capturing and utilizing millions of images of faces.

1.3. This technology has far reaching and alarming implications for human rights and privacy.

1.4. FRT use in policing has not yet been carefully examined by Parliament. But government departments and agencies, including the RCMP, have already been experimenting with AI-powered FRT.[6]

1.5. Following the OPC's recent report concluding the use of FRT by the RCMP was unlawful under privacy law, the RCMP announced that it had put in place an internal directive which "stated that facial recognition technology will only be used in exigent circumstances for victim identification in child sexual exploitation investigations, or in circumstances where threat to life or grievous bodily harm may be imminent."[7]

1.6. AI-powered FRT has not been sufficiently studied, tested, or proven safe for the public. Although general laws still apply (including human rights and privacy laws), and federal treasury board guidance exists for other AI use by government,[8] no specific standards exist for the use of FRT in policing.

1.7. Research has proven FRT to be inaccurate and biased against people with darker skin, especially women.[9] Recent civil society research has raised alarms about questionable FRT use by policing agencies in Canada.[10]

1.8. The fact that colonialism and systemic racism is embedded in historic and current police and criminal justice systems – including in the over-policing of Indigenous, Black and racialized communities – has been well-documented[11] and acknowledged by

---

4 www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/

5 priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/

6 Robertson, K., Khoo, C., and Song, Y. "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada." Citizen Lab and International Human Rights Program, 2020 at citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/

7 www.grc-rcmp.gc.ca/en/news/2021/response-the-report-the-office-the-privacy-commissioner-the-rcmps-use-clearview-ai

8 www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai.html

9 See Buolamwini, J. and Gebru, T. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification." In Conference on fairness, accountability and transparency, 2018 at news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212 ; Cathy O'Neil, Weapons of Math Destruction: How Big Data Increases Inequality, Penguin Random House, 2016; Danielle Groen, "How We Made AI as Racist and Sexist as Humans", The Walrus, 2019 at https://thewalrus.ca/how-we-made ai-as-racist-and-sexist-as-humans/; Hao, K. "A US Government Study Confirms Most Face Recognition Systems are Racist," MIT Technology Review, 2019 at www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software

10 Robertson, *supra* note 6.

11 For example the Report of the House of Commons Standing Committee on Public Safety and National Security on Systemic Racism In Policing in Canada, 2021 at www.ourcommons.ca/DocumentViewer/en/43-2/SECU/report-6/ ; Reclaiming Power and Place: The Final Report of the National Inquiry into Missing and Murdered Indigenous Women and Girls, 2019 at www.mmiwg-

government.[12] This system also affects other marginalized groups including 2SLGBTQI individuals, those with mental illnesses, and low-income communities.[13]

1.9. FRT is a powerful surveillance tool that can further amplify systemic racism against over-surveilled and over-policed communities.

1.10. Black and Indigenous people in Canada are subject to invasive police surveillance that makes it difficult to exist in public space.[14] Disproportionate policing of racialized communities and racial profiling have been reported across Canada, including in Toronto[15], Montreal[16], Halifax[17], Edmonton[18], Calgary, and Vancouver.[19]

1.11. As noted in Policing Black Lives, "surveillance or police encounters that occur because of stereotypes regarding race, ethnicity or religion — serves an important role in determining policing practices. The assumption, then, that Black people are likely to be criminals, results in more Black people being watched, caught, charged and incarcerated. It is Black people who will be made into criminals by the very policing strategies that target them. In other words: "Profiling is a self-fulfilling prophecy."[20]

1.12. In 2017, the UN Working Group of Experts on People of African Descent concluded that Canada's Black population experiences "endemic" racial discrimination by law enforcement. Encounters often escalate "into police violence, resulting in injuries and even deaths" of Black Canadians.[21]

1.13. Any FRT use in policing is inherently high risk because it puts liberty and human rights in jeopardy within an environment of profound asymmetries of information and power between the state and the citizen. FRT potential use by police in public and on crowds is especially alarming. The combination of police powers and commercial FRT raises risks even further.

1.14. Despite these implications, risks, and experiments, there is only a patchwork of laws that apply to this technology, and there is currently no regulation specifically addressing FRT use in policing.

---

ffada.ca ; Reports of the Truth and Reconciliation Commission of Canada, 2015 at ; Report of the Royal Commission on Aboriginal Peoples, 1996 at www.bac-lac.gc.ca/eng/discover/aboriginal-heritage/royal-commission-aboriginal-peoples/Pages/final-report.aspx ; Aboriginal Justice Inquiry of Manitoba, 1991 at legislativelibrary.mb.catalogue.libraries.coop/eg/opac/record/107400530

12 www.justice.gc.ca/eng/rp-pr/jr/oip-cjs/p4.html

13 Eubanks, Virginia. *Automating Inequality: How High-Tech Tools Profile, Police, & Punish the Poor*, NY. St Martin's Press, 2018.

14 Maynard, Robyn. *Policing Black Lives: State Violence in Canada from Slavery to the Present*. Black Point, NS ; Winnipeg, Man. Fernwood Publishing, 2018.

15 Ontario Human Rights Commission reports "Framework for change to address systemic racism in policing," 2021, at www.ohrc.on.ca/en/framework-change-address-systemic-racism-policing ; and "Under suspicion: Research and consultation report on racial profiling in Ontario," 2017, at www.ohrc.on.ca/en/under-suspicion-research-and-consultation-report-racial-profiling-ontario

16 Ted Rutland, "Profiling the Future: The Long Struggle against Police Racial Profiling in Montreal, American Review of Canadian Studies," 50:3, 2020, pp 270-92, at www.tandfonline.com/doi/full/10.1080/02722011.2020.1831139

17 Wortley, Scot, University of Toronto Centre for Criminology & Sociolegal Studies "Halifax, Nova Scotia: Street Checks Report 2019 at humanrights.novascotia.ca/sites/default/files/editor-uploads/halifax_street_checks_report_march_2019_0.pdf

18 Huncar, Andrea, CBC News, "Indigenous women nearly 10 times more likely to be street checked by Edmonton police, new data shows," 2017 at www.cbc.ca/news/canada/edmonton/street-checks-edmonton-police-aboriginal-black-carding-1.4178843

19 Dhillon, Sunny, Globe and Mail, "Vancouver Police Department's use of carding disproportionately targets Indigenous people," 2018 at www.theglobeandmail.com/canada/british-columbia/article-vancouver-police-departments-use-of-carding-disproportionately/

20 Maynard, *supra* note 14.

21 UN Human Rights Council, *Report of the Working Group of Experts on People of African Descent on its mission to Canada*, A/HRC/36/60/Add.1, 16 August 2017, at www.refworld.org/docid/59c3a5ff4.html

1.15. Human rights defenders at the United Nations, and civil society organizations in Canada have raised serious concerns about the unacceptable risks of FRT use by police and law enforcement, especially in public and on crowds. In September 2021, the UN High Commissioner for Human Rights raised an alarm in a public statement which concluded that "Action is needed now to put human rights guardrails on the use of AI, for the good of all of us." The report noted that "States should also impose moratoriums on the use of potentially high-risk technology, such as remote real-time facial recognition, until it is ensured that their use cannot violate human rights."[22]

1.16. In November 2021, the first global standard – the UNESCO Recommendation on the Ethics of AI -- was adopted by 193 member states, including Canada. The UNESCO Recommendation explicitly bans the use of AI systems for mass surveillance. It states in the section on the principle of proportionality and do no harm "In particular, AI systems should not be used for social scoring or mass surveillance purposes."[23] The recommendation notes that this type of technology is very invasive, infringes on human rights and fundamental freedoms, and is used too broadly.

1.17. In addition to these global actions, many jurisdictions, including in the EU and the U.S., are moving towards total or partial bans or moratoria on the use of AI-powered FRT in policing. Where there are partial bans, these prohibit its use on crowds and in public. Some jurisdictions have recommended or instituted a specific independent AI Safety Office. For example, the Australian Human Rights Commission has recommended the establishment of an AI Safety Commissioner "to support regulators, policy makers, government and business apply laws and other standards in respect of AI-informed decision making."[24] More detailed examples are included in Annex A.

1.18. Although the RCMP has reported that they are voluntarily limiting the use of FRT, the CHRC's position is that strong mandatory regulation is required to ensure that human rights are fully protected and that even when faced with internal and external pressures to preserve public safety, as well as time and resource constraints, human rights obligations will not be de-prioritized in favour of investigative efficiency.

1.19. The profound risks to liberty, human rights, and privacy are unlikely to be mitigated through voluntary internal directives, or through self-regulation approaches such as the operational *Draft Guidance.* Overall, a new legal and policy framework is required to regulate the use of FRT and other AI-powered policing tools.

---

22 Statement available at: www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=27469&LangID=E . Full report: United Nations High Commissioner for Human Rights, report to the Human Rights Council "The right to privacy in the digital age," Forty-eighth session, 2021, A/HRC/48/31, par 45 at p 12 www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session48/Documents/A_HRC_48_31_AdvanceEditedVersion.docx

23 See press release at *en.unesco.org/news/unesco-member-states-adopt-first-ever-global-agreement-ethics-artificial-intelligence*. Full text at *UNESCO Recommendation on the Ethics of Artificial Intelligence, Annex of the Report of the Social and Human Sciences Commission (SHS)*, UNESCO General Conference, 41st, 2021, par 26 at unesdoc.unesco.org/ark:/48223/pf0000379920.page=21

24 Australian Human Rights Commission, *Human Rights and Technology Final Report*, 2021, section 10.2 at p 127 tech.humanrights.gov.au/downloads. Project outlined *at tech.humanrights.gov.au*.

2. **The CHRC's position is that Parliament should immediately undertake a study that examines the use of FRT in policing and puts in place a new legal framework.**

2.1. Parliamentary studies by the House of Commons Standing Committee on Justice and Human Rights or Senate Standing Committee on Human Rights should include public hearings with human rights, privacy, legal experts, civil society, and rights holders and their advocates.

3. **The CHRC's position is that a new legal framework put in place by Parliament must take a human rights-based approach.**

3.1. Privacy must be explicitly recognized as a human right in any new framework. And privacy laws for both the public and the private sector must be improved. But privacy rights and privacy law alone is insufficient to protect a wide array of human rights in a new framework.

3.2. The Draft Guidance contains many helpful elements for consideration in a new framework. Sections and suggestions of the Draft Guidance overlap in many ways with a human rights-based approach, and share many similar objectives and activities. The Draft Guidance, however, focuses too narrowly on privacy requirements and does not give sufficient consideration to human rights law, standards, and requirements. It leaves many activities as optional or subject to the operational discretion of policing agencies. And it does not sufficiently address specific concerns about systemic racism that arise in both policing and FRT fields.

3.3. The respect, protection and redress of human rights must be central to any new legal framework on the use of AI-powered tools such as FRT in policing. A human rights-based approach uses international human rights as a foundation and a benchmark. It analyses the rights at play and the impacts on them, as well as the entitlements of right-holders and the human rights obligations of duty-bearers (in this case, the government and policing agencies).

3.4. There are 5 general elements which form the basis of a human rights-based approach: legality, non-discrimination, participation, empowerment, and accountability. Some, but not all of these, are often also elements of ethical, trustworthy, or responsible AI frameworks, principles and documents.

3.5. The CHRC suggests that any Parliamentary study should integrate and include at least the following key elements in taking a human rights-based approach to developing a new legal framework. The CHRC provides some detail on how each element might be specifically relevant for the issue of FRT in policing.

3.6. Legality and non-discrimination

3.6.1. Legal protections: Analysis must be made using the principles, standards, obligations and protections of fundamental human rights in international human rights treaties, standards and recommendations, in the Canadian Charter of Rights and Freedoms, and in domestic human rights codes (which are quasi-constitutional). On AI and FRT and policing, this includes applying the recommendations and standards in each of these areas, developed by UN bodies and mechanisms. For example, this would include the recommendations of the Committee on the Elimination of Racial Discrimination (CERD) and the UN High Commissioner for Human Rights on facial recognition and police surveillance, and the UNESCO recommendation to ban mass surveillance.

3.6.2. Specific risks to human rights: Risks to and impacts on specific human rights raised by rights-holders, experts, stakeholders, and advocates should be anticipated, highlighted and analysed. Robust analysis is especially important at this point in time, as there is little case law on these topics, and a new legal and policy framework can provide helpful direction to legal decision-makers. Analysis should include impacts on privacy rights, but also on a broader range of human rights such as the right to freedom of expression, peaceful assembly, and association, autonomy, freedom of thought and opinion, the right to equality and the right to be free from discrimination. It could also include consideration of the impacts of FRT on other Charter rights, or those related to the Criminal Code, administrative law, and common law, such as rights to liberty and due process, or freedom from unreasonable search and seizure. And there may be implications in other areas such as labour or employment rights.

3.6.3. Anti-racism and anti-colonialism: A human rights-based approach must take into specific consideration groups and populations who are likely to be most at risk. Given the history of policing in Canada, it is crucial to ensure that a new legal and policy framework include explicit measures to counteract embedded systemic racism affecting Black, Indigenous, and racialized communities.

3.6.4. Intersectionality: Risks from FRT to rights-holders and groups because of the intersecting impact of multiple forms of discrimination in the policing context must be addressed (e.g. Indigenous women, young Black men, Black trans women[25]).

3.6.5. Root causes: An analysis should be undertaken to examine the root causes of violations of rights that might arise in the AI and FRT field as well as the policing field. Some of this analysis in the policing field has already been done through multiple reports and these have made recommendations for example, for stronger independent RCMP oversight. Examination of root causes of violations in relation to FRT in policing may look more closely at other specific concerns, such as the lack of diversity in the tech field, lack of research funding for human rights or social impact of AI and FRT, high error rates, or racial and gender bias in development, training sets or algorithms.

3.7. Participation and empowerment

3.7.1. Meaningful inclusion and engagement: Experts, stakeholders, rights-holders and their advocates must be meaningfully included and involved in all phases of developing, implementing and evaluating a legal and policy framework, including in exploring the risks and establishing the rationale, parameters and accountability for the way FRT is prohibited or permitted in policing. Participation at Parliamentary hearings is an important first step.

3.7.2. Knowledge and capacity: People cannot claim their rights unless they know their rights. Parliamentary hearings and debates are a key element of building a shared public understanding of the human rights issues at play with AI and FRT. A new legal and policy framework should also establish transparency, explainability, and traceability requirements for public and other types of disclosure of FRT use, and of algorithms for independent examination. A new framework should require an assessment of the knowledge and capacity of

25 The Trans PULSE Canada Team. QuickStat #4 – Anticipated discrimination from police among trans and non-binary participants. 2021-02-12. Available from: https://transpulsecanada.ca/research-type/quickstats/

rights-holders to claim their rights, and of policing agencies--and their contractors or private sector partners--to fulfill their obligations. It should then establish strategies to build and maintain these capacities.

3.7.3. Research, awareness, and public education: Although there are millions of dollars flowing regularly to funding research on AI, the intersection of AI technology with human rights and privacy rights in Canada needs more research and analysis, including techno-social, interdisciplinary and multi-stakeholder research led by diverse research groups. In addition, public information and awareness campaigns are required to better inform duty-bearers (including policing agencies), policy and decision-makers, and the public, on FRT and human rights.

3.8. Accountability, access to justice & remedies

3.8.1. Approval for use: Any proposed use of FRT in policing must also be reviewed and approved by an independent external decision-maker, including any request for an exemption to a moratorium. Any FRT must be subjected to and pass rigorous scientific testing, including tests for accuracy and bias, including in real-world situations, before it is used. Independent human rights experts should be part of this evaluation.

3.8.2. Independent supervision: Use of FRT in policing must be closely and independently supervised by a parliamentary-appointed body, especially during the first years of the implementation of a new legal framework.

3.8.3. Independent audits: FRT use must be subject to regular independent audits, which should include privacy and human rights impact assessments on each proposed use of FRT.[26] These assessments must integrate requirements including, but not limited to, those established by the Supreme Court of Canada in *Meiorin*[27] and *Grismer.*[28]

3.8.4. Private-sector involvement: Legislation must include provisions that remove the potential for policing agencies and private entities to avoid accountability, even when police procure or use FRT from private or commercial organizations.[29]

3.8.5. Legal remedies: The potential harms associated with AI and FRT use in policing are not yet fully understood, but the immense scope and impacts of AI on society will require remedies tailored to this unique context. Appropriate legal remedies must be put in place to ensure accountability and full redress for violations of human rights, including discrimination.

3.8.6. Proactive compliance models of regulation: AI systems create and maintain systems of immense power and information imbalances. These imbalances create and perpetuate barriers to accessing justice. Individuals are unlikely to know their rights, or when these have been violated through police use of FRT.

---

26 Some examples of human rights impact assessment tools are available at: www.humanrights.dk/tools/human-rights-impact-assessment-guidance-toolbox ; www.scottishhumanrights.com/media/1814/shrc_panel_self-assessment_tool_vfinal.pdf ; www.ag.gov.au/sites/default/files/2020-03/Flowchart.pdf *;* www.ifc.org/hriam *;* and an older CHRC impact assessment for security measures is available at www.chrc-ccdp.gc.ca/sites/default/files/publication-pdfs/security_guide_secutrite-eng_0.pdf

27 British Columbia (Public Service Employee Relations Commission) v. BCGSEU, [1999] 3 S.C.R. 3. www.canlii.org/en/ca/scc/doc/1999/1999canlii652/1999canlii652.html

28 British Columbia (Superintendent of Motor Vehicles) v. British Columbia (Council of Human Rights), [1999] 3 S.C.R. 868. www.canlii.org/en/ca/scc/doc/1999/1999canlii646/1999canlii646.html

29 www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_211214/

An effective human rights model must remove the burden on individuals of identifying harms and bringing claims against policing agencies. This might include elements such as administrative monetary penalties and regular audits.

3.8.7. Parliamentary accountability: This new technology has been developing in the private commercial field, and yet has significant impacts for the public and human rights. In a democratic society, such technologies – especially those deployed by the state in policing the public – cannot be allowed to evolve further without greater public oversight. Policing agencies must be required to submit detailed reports to Parliament on the use of FRT in policing.

3.8.8. Human rights evaluation: As part of this Parliamentary accountability, a new legal regime should require specific and publically-available assessments that independently evaluate: whether human rights are being adequately protected in the new framework overall; whether legal requirements and the elements of a human rights approach have been sufficiently met; and, whether amendments or changes to the legal and policy framework are required. This broader evaluation must include views from rights-holders, experts, and stakeholders. It must analyze both outcomes and processes guided by human rights standards and principles.

3.9. Many of the above elements are reflected in the UNESCO recommendation which states that "Governments should adopt a regulatory framework that sets out a procedure, particularly for public authorities, to carry out ethical impact assessments on AI systems to predict consequences, mitigate risks, avoid harmful consequences, facilitate citizen participation and address societal challenges. The assessment should also establish appropriate oversight mechanisms, including auditability, traceability and explainability, which enable the assessment of algorithms, data and design processes, as well as include external review of AI systems. Ethical impact assessments should be transparent and open to the public, where appropriate. Such assessments should also be multidisciplinary, multi-stakeholder, multicultural, pluralistic and inclusive. The public authorities should be required to monitor the AI systems implemented and/or deployed by those authorities by introducing appropriate mechanisms and tools."[30]

4. The CHRC's position is that a new framework must fully consider and integrate human rights protections for children and youth.

4.1. In March 2021, the UN Committee on the Rights of the Child recommended that "States parties should ensure that digital technologies, surveillance mechanisms, such as facial recognition software …are not used to unfairly target children suspected of or charged with criminal offences and are not used in a manner that violates their rights, in particular their rights to privacy, dignity and freedom of association."[31]

4.2. The extension of police presence in, and surveillance of, children's lives at schools is of concern to Black and Indigenous students and parents. The over-policing of Black and Indigenous communities often begins in the schools. In a recent report, the BC Office of the Human Rights Commissioner recommends removal of school liaison officers from schools, unless school boards can "demonstrate an evidence–based need for them that

30 *UNESCO Recommendation on the Ethics of Artificial Intelligence, Annex of the Report of the Social and Human Sciences Commission (SHS)*, UNESCO General Conference, 41st, 2021, at par 53 unesdoc.unesco.org/ark:/48223/pf0000379920.page=26

31 UN Committee on the Rights of the Child recommendation in "General comment No.25 on children's rights in relation to the digital environment," (par 9 and par 119 at pp 19-20), 2021 tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CRC%2fC%2fGC%2f25&Lang=en

cannot be met through other means."[32] Any potential for police surveillance in schools, including FRT, presents a serious potential risk to the human rights well-being of children and youth in their developmental and learning environment, and it should not be permitted.

4.3. It is only in the rarest of circumstances that the use of FRT by police and law enforcement would be justified in situations that involve a child or youth.

5. The CHRC's position is that until a new legal and policy framework is put in place, FRT use in policing should be prohibited through a moratorium.

5.1. The *Draft Guidance* is unlikely to have the intended effect of helping to ensure that police agencies' use of FRT is lawful and appropriately mitigates human rights risks.

5.2. In their RCMP investigation report, the OPC recognizes that the use of FRT is only allowable if it is initially shown to be effective in each specific use. It noted that "police should not use FRT just because it is thought to be "useful" for law enforcement in general…It is not enough to rely on general public safety objectives to justify the use of such an intrusive technology. The pressing and substantial nature of the specific objective should be demonstrable through evidence."[33] The *Draft Guidance* also allows for the possibility that some desired FRT use would not be allowed under these proposed operational rules, if the RCMP concluded either that it did not have the evidence to justify its use, or that it did not have the legal authority to deploy it.

5.3. The CHRC agrees with these requirements to justify the need for the use of AI-powered FRT with clear evidence, and that there must be legal authority to use it.[34] This is consistent not only with privacy law assessments, but also with Charter and human rights law requirements. The CHRC, however, disagrees that the required evidence-based justification and legal authority can or should be assessed by the RCMP itself through internal operations pursuant to voluntary *Draft Guidance.* As noted above, the CHRC is concerned about activities which are presented as optional in the *Draft Guidance*, but which would be required under a human rights-based approach, and which need additional Parliamentary study.

5.4. The CHRC's position is that operational guidance and self-regulation is not the appropriate policy tool for this technology at this time in history,

- when AI and FRT technology itself is developing rapidly in an unregulated environment,[35]
- when the public is increasingly concerned about privacy and surveillance,
- when the world is moving towards reasonable bans and limits on FRT use for mass surveillance, and
- when criminal justice systems and police powers are under intense scrutiny, with increasing calls for stronger public oversight of policing agencies.[36]

---

32 Office of the BC Human Rights Commissioner, "Equity is safer: Human rights considerations for policing reform in British Columbia," 2021, at Recommendation 14, and at p 53. bchumanrights.ca/wp-content/uploads/BCOHRC_Nov2021_SCORPA_Equity-is-safer.pdf

33 www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/

34 Similar tests exist under the Charter, Privacy law and human rights law. The CHRA test is explained more in: "Bona Fide Occupational Requirements and Bona Fide Justifications Under the Canadian Human Rights Act: The Implications of *Meiorin* and *Grismer*" available at www.chrc-ccdp.gc.ca/sites/default/files/bfore_0.pdf

35 www.lco-cdo.org/en/the-lco-releases-a-new-report-regulating-ai-critical-issues-and-choices/

36 See Dec 2021 Mandate Letters pm.gc.ca/en/mandate-letters/2021/12/16/minister-justice-and-attorney-general-canada-mandate-letter, which commit the Justice Minister to addressing systemic discrimination and the overrepresentation of Black and racialized Canadians and Indigenous Peoples in the criminal justice system by consulting on and developing an Indigenous

5.5. The *Draft Guidance* is unlikely to be sufficient to safeguard people from the overall intrusive nature of FRT use and its high risks for negative impact on human rights, such as rights to freedom of expression, peaceful assembly and association, autonomy, freedom of thought and opinion, the right to equality and right to be free from discrimination.

5.6. More importantly, given the RCMP's history of systemic racism, over-surveillance and over-policing of Black, Indigenous and racialized communities, the *Draft Guidance,* would not likely be adequate to mitigate the high risk of harm that could result from discriminatory application and impact of FRT, nor address the public mistrust that currently exists in relation to policing and surveillance. To the contrary, the CHRC's view is that AI-powered FRT is a powerful surveillance tool which, if added to policing tools, is likely to perpetuate and amplify systemic racism.

5.7. This overall context does not support the premise that operational guidance and internal assessments and accountabilities are sufficient to respect and protect human rights. The RCMP needs fewer tools that could perpetuate systemic discrimination and much stronger external oversight.

The CHRC looks forward to more public debate and Parliamentary discussions on these matters.

Justice Strategy, and a Black Canadians Justice Strategy. See also a Nov 2021 poll which found that nearly six in ten Canadians support the creation of an independent civilian oversight body of the RCMP (58 percent) and the development of a Black Canadians Justice Strategy to address anti-Black racism and discrimination in the criminal justice system (55 percent). Survey summary and report available at www.crrf-fcrr.ca/en/news-a-events/articles/item/27447-the-voice-of-canadian-on-racism-discrimination-and-government-action

ANNEX A

Recommendations by CHRC and Other Human Rights Commissions

I. In several of its recent CHRC submissions to the UN Committee Against Torture (2018 and 2021), Committee on the Rights of the Child (2020), and Human Rights Committee (2021), the CHRC has noted that in the areas of policing, law enforcement, border security, immigration, and criminal justice, FRT and other AI technologies can further embed unfairness and systemic racism. The CHRC has echoed growing calls for caution from UN bodies.

II. As stated in the CHRC's *Submission to the Committee on the Rights of the Child in advance of the Committee's development of the List of Issues Prior to Reporting for Canada's 5th-6th periodic review*[37] children and youth are increasingly subject to technological surveillance of their activities by both governments and the private sector. This is often done without children's awareness or informed consent, and presents new and profound risks to privacy and, consequently, to other rights. This increasing surveillance, combined with other technologies such as big data, facial recognition, and AI can put children and youth at risk of having significant parts of their lives and decisions predicted, influenced, monetized and exploited in ways that are inconsistent with, or even contrary to, the best interests of the child.

III. The 2021 final report from the Australian Human Rights Commission on *Human Rights and Technology*[38] recommended a moratorium on FRT use in policing until a new legal framework is put in place. It also recommended the creation of an AI Safety Commissioner "to support regulators, policy makers, government and business apply laws and other standards in respect of AI-informed decision making. Government agencies and the private sector are often unclear on how to develop and use AI lawfully, ethically and in conformity with human rights. Regulators face challenges in fulfilling their functions as the bodies they regulate make important changes in how they operate. Legislators and policy makers are under unprecedented pressure to ensure Australia has the right law and policy settings to address risks and take opportunities connected to the rise of AI. The unprecedented rise in AI presents a once-in-a-generation challenge to develop and apply regulation that supports positive innovation, while addressing risks of harm. An AI Safety Commissioner would provide technical expertise and capacity building. As an independent statutory office that champions the public interest, including human rights, an AI Safety Commissioner could help build public trust in the safe use of AI."[39]

IV. In March 2020, the Equality and Human Rights Commission of Great Britain called for the suspension of the use of automated facial recognition (AFR) and predictive algorithms in

---

37 tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=INT%2fCRC%2fIFN%2fCAN%2f42705&Lang=en

38 humanrights.gov.au/our-work/rights-and-freedoms/projects/human-rights-and-technology

39 tech.humanrights.gov.au/artificial-intelligence/ai-safety-commissioner

policing in England and Wales, until their impact was independently scrutinised and laws are improved.[40]

Recommendations by Canadian Civil Society organizations

V. Canadian civil society organizations have also called for limits on FRT use in policing[41] or for a moratorium.[42] In their submissions to the OPC on the Draft Guidance, Citizen Lab and the Canadian Civil Liberties Association (CCLA) have both called for a moratorium on the use of FRT in policing. In addition, the CCLA believes that "until there is a chance to fully assess the risks, the accuracy of the technology, and the cost of mistakes and failures, this technology should not be used, particularly for law enforcement purposes."[43]

VI. Citizen Lab noted that "above all, community representatives expressed the overriding concern that algorithmic policing tools would perpetuate systemic discrimination against marginalized communities while simultaneously masking the underlying systemic issues and root problems in the criminal justice system that cannot be fixed through technology. Community representatives also viewed the use of algorithmic policing tools as inseparable from Canada's history of colonialism and systemic discrimination against Indigenous, Black, and other racialized and marginalized groups."[44]

Legislative and regulatory bodies issuing bans, prohibitions, and limitations on FRT

United States

VII. In October 2021, the U.S. White House announced that it is exploring the development of an "AI Bill of Rights"[45] and is seeking consultation input on facial recognition technology and other biometric technologies.[46] In June 2021, *The Facial Recognition and Biometric Technology Moratorium Act* was introduced in the U.S. Senate. It would ban use of facial recognition (and other biometric technology) in real time or on a recording or photographs by the federal government or any federal official in the U.S., including in airports, ports of entry, and border zones. [47] As of January 2021, nine U.S.

---

40 Equality and Human Rights Commission "Facial Recognition Technology and Predictive Policing Algorithms Out-Pacing the Law" at www.equalityhumanrights.com/en/our-work/news/facial-recognition-technology-and-predictive-policing-algorithms-out-pacing-law

41 For example : https://observatoire-ia.ulaval.ca/en/observations-sur-document-dorientation-a-lintention-des-services-de-police-sur-lutilisation-de-la-technologie-de-reconnaissance-faciale/

42 citizenlab.ca/2021/10/consultation-on-draft-guidance-for-police-services-privacy-obligations-on-the-use-of-facial-recognition-technology/

43 CCLA and Privacy International collaborate on submissions regarding facial recognition guidelines for police agencies at ccla.org/privacy/ccla-and-privacy-international-collaborate-on-submissions-regarding-facial-recognition-guidelines-for-police-agencies/

44 Kenyon, Miles, *Algorithmic Policing in Canada Explained* (Citizen Lab, University of Toronto, 1 September 2020) at citizenlab.ca/2020/09/algorithmic-policing-in-canada-explained/

45 www.wired.com/story/opinion-bill-of-rights-artificial-intelligence/

46 www.federalregister.gov/documents/2021/10/08/2021-21975/notice-of-request-for-information-rfi-on-public-and-private-sector-uses-of-biometric-technologies

47 www.markey.senate.gov/news/press-releases/senators-markey-merkley-lead-colleagues-on-legislation-to-ban-government-use-of-facial-recognition-other-biometric-technology

jurisdictions have passed unconditional bans on the use of FRT by government as a whole, most of which include private rights of action[48] or statutory damages for individuals harmed by violation of these laws.[49] As of November 2021, 21 U.S. cities[50] have implemented bans on the use of FRT by police. Portland (Ore), adopted the U.S.'s most restrictive laws on face recognition at the time, banning private as well as government use of the technology, in 2020.[51] There are also currently almost 50 local and state legislators who have passed – or have announced – forthcoming laws or regulations on FRT use by police and government.

European Union

VIII. In January 2021, the Council of Europe consultative committee published guidelines proposing strict rules on the use of facial recognition including banning certain uses of facial recognition technology such as live use in uncontrolled environments.[52] In April 2021, the European Commission (EC) proposed draft regulations[53] to restrict the use of FRT in public spaces in the EU. The rules prohibit biometric identification systems like facial recognition in public places for police use — with exceptions in the case of urgent items and "serious crimes,"[54] such as: location of missing children; reunification of families that have been separated while fleeing conflict; to address human trafficking; identification of children and others who are victims of violence or sexual assault/exploitation, and; responding to immediate threats of terrorism. These draft regulations need to be negotiated with EU countries and the bloc's lawmakers before it becomes law.

IX. This EC draft regulation is under intense scrutiny and has faced immense backlash from EU parliamentarians, watchdog agencies, and civil society organizations. Europe's two privacy watchdogs called for a ban on the use of FRT in public spaces[55] and stated "A general ban on the use of facial recognition in publicly accessible areas is the necessary starting point if we want to preserve our freedoms and create a human-centric legal framework for AI." Civil society groups are organizing to oppose the draft rule that it "leaves a worrying gap for discriminatory and surveillance technologies used by governments and companies."[56] The European Parliament has also raised alarms. On October 6, 2021, Members passed a non-binding resolution[57] calling for a ban on the

---

48 A private right of action is when a private citizen is legally entitled to enforce their rights under a given statute. This differs from situations where a state or the federal government enforces legal violations under a statute.

49 Rashida Richardson, "Facial Recognition in the Public Sector: The Policy Landscape," German Marshall Fund of the United States, 2021, at www.jstor.org/stable/resrep28529

50 Future, Fight for the, 'See Where Dangerous Facial Recognition Is Being Used, and Learn What You Can Do about It.', *Ban Facial Recognition* at www.banfacialrecognition.com/map/

51 Simonite, Tom, 'Portland's Face-Recognition Ban Is a New Twist on "Smart Cities"', Wired at www.wired.com/story/portlands-face-recognition-ban-twist-smart-cities/

52 Council of Europe Consultative committee report on facial recognition rm.coe.int/guidelines-on-facial-recognition/1680a134f3

53 'EUR-Lex - 52021PC0206 at eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206 see also artificialintelligenceact.eu

54 Ibid, Sections 5.2.2. and par (23)

55 www.reuters.com/technology/eu-privacy-watchdogs-call-ban-facial-recognition-public-spaces-2021-06-21/

56 www.politico.eu/article/eu-ai-artificial-intelligence-rules-facial-recognition/

57 '"Historic Moment": EU Approves Call for Sweeping Ban on Facial Recognition Surveillance' at www.commondreams.org/news/2021/10/06/historic-moment-eu-approves-call-sweeping-ban-facial-recognition-surveillance

use of FRT in public places by law.[58] The resolution explicitly calls 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. As of Nov 2021, 116 Members of the European Parliament (MEPs) have written to the European Commission's leaders in support of a civil society organization letter calling for greater restriction on uses of AI that compromise fundamental rights. [59]

X. In addition, some specific EU countries such as Germany,[60] are putting in place total bans on the use of FRT in public spaces, in advance of the negotiations of the EU AI Act.

Scotland

XI. In Feb 2020, Scottish parliament halted all live facial recognition use for police investigations after a parliamentary report from the Justice Sub-Committee on Policing[61] and a new Biometrics Commissioner Parliamentary Officer was appointed in 2021, to specifically provide oversight of biometric information use by police, draft legislation to guide this use, and establish a complaint mechanism. The Justice Secretary stated that "Given the explosion in biometric data technologies in recent years, it is all the more important that we have an independent commissioner who will lead a national conversation about rights, responsibilities and standards…I see that we have a golden opportunity for the new biometrics commissioner to link up with others, such as the Information Commissioner and the Scottish Human Rights Commission, to perhaps take forward a national campaign."[62]

58 Use of artificial intelligence by the police: MEPs oppose mass surveillance at www.europarl.europa.eu/news/en/press-room/20210930IPR13925/use-of-artificial-intelligence-by-the-police-meps-oppose-mass-surveillance

59 '116 MEPs Agree – We Need AI Red Lines to Put People over Profit', *European Digital Rights (EDRi)* at edri.org/our-work/meps-agree-we-need-ai-red-lines-to-put-people-over-profit/

60 www.politico.eu/article/german-coalition-backs-ban-on-facial-recognition-in-public-places/

61 'Facial Recognition: How Policing in Scotland Makes Use of This Technology', *Scottish Parliament Reports* at digitalpublications.parliament.scot/Committees/Report/JSP/2020/2/11/Facial-recognition--how-policing-in-Scotland-makes-use-of-this-technology

62 Meeting of the Parliament 09 January 2020 at archive2021.parliament.scot/parliamentarybusiness/report.aspx?r=12448