CANADIAN CIVIL LIBERTIES ASSOCIATION
ASSOCIATION CANADIENNE DES LIBERTES CIVILES

Consultation response: Draft privacy guidance on facial recognition for police agencies

October 21, 2021

Brenda McPhail, Ph.D.
Privacy Director
Canadian Civil Liberties Association
90 Eglinton Ave. E., Suite 900
Toronto, ON M4P 2Y3
Phone: 416-646-1406
www.ccla.org

Lucie Audibert
Legal Officer
Privacy International
62 Britton Street
EC1M 5UY London
United Kingdom
www.privacyinternational.org

Introduction

The Canadian Civil Liberties Association ("CCLA") and Privacy International ("PI") welcome the opportunity to provide this response to the draft privacy guidance on facial recognition for police agencies.

CCLA is an independent, non-governmental, non-partisan, non-profit, national civil liberties organisation. Founded in 1964, CCLA and its membership promote respect for and recognition of fundamental human rights and civil liberties. For fifty years, CCLA has litigated public interest cases before appellate courts, assisted Canadian governments with developing legislation, and published expert commentary on the state of Canadian law. Facial recognition technology engages issues of privacy, surveillance, equality, and potentially other fundamental freedoms, including rights to free expression, assembly and association, which are all core to our mandate.

As a civil society organization, CCLA's perspective on facial recognition technology, or as we often refer to it, facial fingerprinting, is grounded in our mandate to protect the rights and freedoms of individuals. Our experience includes engagement via our international networks in the widespread debates taking place in jurisdictions around the world regarding the risks and benefits that might accrue because of the proliferation of facial recognition applications in law enforcement and national security applications.[1] We are pleased to have the opportunity to collaborate with colleagues from Privacy International in bringing this submission forward for this consultation.

Privacy International ("PI") is a London-based non-profit, non-governmental organization that researches, advocates and litigates globally against government and corporate abuses of data and technology. PI is frequently called upon to give expert evidence to Parliamentary and Governmental committees around the world on privacy issues and has advised and reported to, among others, the UK Parliament, the Council of Europe, the European Parliament, the OECD, and the UN. PI also regularly acts as claimant or intervener in cases involving the right to privacy, having previously acted in the courts of the UK, Colombia, Kenya, France, Germany, United States, as well as in the European Court of Human Rights.

PI regularly engages with authorities in the UK and abroad to warn of the risks of facial recognition technology, and to ensure that any use is lawful and adheres to fundamental rights.[2] Most recently, we filed legal complaints with data protection authorities in five European countries against web scraping and facial recognition company Clearview AI, and against the use of its technology by law enforcement authorities.[3] We welcome the Commissioner's efforts to strengthen the

[1] See, for example, a report published by the International Network of Civil Liberties Organisations, "In Focus: Facial recognition tech stories and rights harms from around the world," Available https://ccla.org/get-informed/inclo-reports/in-focus-facial-recognition-tech-stories-and-rights-harms-from-around-the-world/

[2] See, for example, PI, Submission to the Scottish Parliament's Justice Sub-Committee on Policing's inquiry into facial recognition policing (November 2019), https://privacyinternational.org/sites/default/files/2020-04/19.11.01_JusticeSC_FRT_Evidence_PI_FINAL_2%20%282%29.pdf.

[3] Privacy International (25 May 2021) Privacy International and others file legal complaints across Europe against controversial facial recognition company Clearview AI. Available at https://privacyinternational.org/press-release/4520/privacy-international-and-others-file-legal-complaints-across-europe-against.

framework around police use of facial recognition, and are very grateful to the Commissioner and to the CCLA for this opportunity to contribute our views.

Our responses selectively address questions posed in the notice of consultation.

Framing the Initiative

These guidelines present both opportunity and risk. Canadian law enforcement bodies have been somewhat more cautious in their adoption of facial recognition technology (FRT) than their peers in the United States or the United Kingdom, but as the Clearview AI debacle showed[4], there is significant interest in experimenting with, and integrating this technology into, a range of policing activities in forces across Canada. It is timely for the Office of the Privacy Commissioner of Canada and provincial colleagues to take the opportunity to issue guidance to ensure that the procurement, testing, and use of FRT by police services is compliant with privacy laws, upholds the *Charter of Rights and Freedoms*, and is only undertaken with careful attention to privacy best practice and principles. The risk of issuing such guidelines, however, is that the conversation then shifts to focus on "how" to use the technology in a rights-respecting manner, rather than "if" it is possible to do so. At CCLA and PI, we believe that the question of "if" should still be front and centre in public discussions about this controversial, risky, and often racist technology.[5] This is particularly the case given the Canadian reckoning with systemic racism that followed the murder of George Floyd, which had repercussions in Canada up to and including the revitalization of debates regarding re-tasking and de-funding police.[6]

Consequently, while we respond constructively in this submission to questions regarding the text of the draft guidelines, we wish to state from the outset that we believe there should be a moratorium on FRT for policing purposes in the absence of comprehensive and effective legislation that

- provides a clear legal framework for its use,
- includes rigorous accountability and transparency provisions,
- requires independent oversight, and
- creates effective means of enforcement for failure to comply.

We further take the position that the use of FRT for the purposes of mass surveillance, that is, facial recognition widely deployed in public or publicly accessible spaces to identify individuals,

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

[5] The literature in this area is extensive. A seminal piece is Buolamwini, J. & Gebru, T. Proceedings of Machine Learning Research 81, 77-91 (2018); data from the NIST Face Recognition Vendor Test on Demographic Effects is often cited and authoritative, Grother, P., Ngan, M. & Hanaoka, K. *Face Recognition Vendor Test Part 3: Demographic Effects* (NIST, 2019).

[6] A report entitled Rethinking Community Safety – A Step Forward for Toronto, in which CCLA participated with a range of partners under the leadership of the Toronto Neighborhood Centres, examines these issues in depth. Available: https://ccla.org/criminal-justice/ccla-partners-on-report-urging-toronto-to-detask-police/

poses such high potential for abuse, and creates such a serious risk to human rights, that there is no framework, either technical or legal, that could eradicate the threat.[7] We note that the European Parliament, as part of its deliberations around the proposal for an Artificial Intelligence Act[8], has recently voted to support a ban on biometric mass surveillance, and called for a ban on the use of private facial recognition databases.[9]

Responding to the Consultation Questions

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

This guidance may help by directing police bodies to consider a series of important factors and core privacy principles across the range of legal authorities relevant to use of FRT. It is rendered necessary yet insufficient by the reality that current Canadian legislation is woefully inadequate to address the potential privacy harms, and harms to rights and freedoms for which privacy serves as a threshold or gateway right, of this technology. And in that statement lies the rub; while the guidance can *help* ensure police agencies' use of FRT is lawful in the current legal landscape, mere legal compliance will be insufficient to fully mitigate the risks to rights, including privacy rights, posed by the full spectrum of potential uses for FR in policing.

This caveat became crystal clear when CCLA had the privilege of participating in a convening hosted by the Information and Privacy Commissioner of Ontario on September 16, 2021, along with representative from police bodies and the Ministries of the Attorney General and Solicitor General. While this blunt summary does something of a disservice to the constructive conversation that occurred, it is not unreasonable to describe a rough split between academic and civil society participants, who wondered if the guidelines went far enough, and those with more direct responsibility for policing who generally expressed concerns that the guidelines went farther in some respects than was warranted by current legislation.

[7] In this CCLA and PI are aligned with the 179 signatories to the "open letter calling for a global ban on biometric recognition technologies that enable mass and discriminatory surveillance." Available: https://www.accessnow.org/ban-biometric-surveillance/

[8] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS (COM/2021/206 final). Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[9] For the European Parliament's resolution, see European Parliament (6 October 2021) European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)). Available at https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_EN.html. For the report adopted by the European Parliament's resolution, see Committee on Civil Liberties, Justice and Home Affairs (13 July 2021) Report on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)). Available at https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_EN.pdf.

This is not a reason for reducing the aspirational aspects of the guidelines or the recommendations based on privacy best practice, including the importance of a necessity and proportionality analysis when considering invasive public surveillance. But it is an indication that practical implementation may be at best, inconsistent. This is particularly the case given that the advice for police bodies to navigate the genuinely complex set of legal authorities including statutory and common law authority for police powers, the relevant federal or provincial privacy laws, and the *Charter of Rights and Freedoms*, is to consult legal counsel. As a pragmatic step, this makes sense. As an effective mitigation strategy to risks to rights, it falls short for two reasons.

First, any such advice will be subject to solicitor-client privilege and as such, will be kept entirely outside the public view. Such advice may be good or great (or neither), it may be effective and strictly adhered to or ignored, it may rely on a rigorous assessment of protections afforded by each legal authority under analysis or come up against the underdeveloped jurisprudence in this area that seems likely to render legal certainty regarding the nuances of FRT use elusive for the foreseeable future. But the public will never know. At best, as with the Cadillac Fairview case, it will require an investigation by the OPC to reveal that there has been a questionable interpretation of privacy law on the part of a private sector actor.[10] At worst, there will be no complaint, no investigation, and no redress for an infringement based on such privileged interpretations. Indeed, the predicted opacity of the legal assessments the guidelines indicate should take place prior to use of FRT would leave the public with no insight into the ways police bodies have given human rights, including privacy rights, due consideration and no means of assessing whether such considerations did or did not carry through into the processes of technology acquisition and use.

Second, in all such cases, there is a genuine question regarding the consistency with which the guidance can be interpreted under such circumstances. In this regard CCLA commends the submission to the current consultation of Professors Lisa Austin and Andrea Slane, who elaborate on the complexity of the legal landscape relevant to FRT use by police.[11] People across Canada deserve equal, consistent, protections for their rights if police forces use FRT. A requirement to "ask your lawyer" in this uncertain legal environment, for this controversial and evolving technology, will not achieve it.

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

[10] While this was a private sector use of facial analytics, not a public sector use of FRT, the principle that permissive or simply incorrect interpretations of law may lead to privacy invasions is relevant in this context. See: Joint Investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia. PIPEDA Findings #2020-004, October 28, 2020. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/

[11] Lisa Austin and Andrea Slane (October 2021). Submission to consultation on privacy guidance on facial recognition for police agencies.

CCLA believes it is important to stress, firstly, that the guidelines are absolutely correct to place the onus on law enforcement bodies using FRT to ensure the tools they choose are compliant with all relevant Canadian laws. The Royal Canadian Mounted Police's (RCMP) resistance to accepting responsibility for ensuring third party vendors comply with privacy law, documented in the Investigation Findings regarding the RCMP's use of Clearview AI facial recognition technology, clearly highlights the necessity of this provision.[12] It must form a part of every procurement process, carry through to implementation, and continue for the full span of time the tool is in operation. Given the potential for technological changes in third party software, ongoing diligence regarding compliance is of particular importance. Lack of in-house expertise to make such assessments can and should be addressed by independent outside consultation with experts, including a comprehensive range of community stakeholders. In paragraph 69 of the guidance, last bullet point, we would ask that involvement of technical experts and stakeholder groups be considered mandatory instead of a mere option as currently suggested by the wording "may include"; we also suggest that police agencies should be required to demonstrate in their PIA report how they have engaged with such experts and community stakeholders. The guidance should also require that assessment of legal compliance and consultation with external stakeholders must be performed, completed and reported on prior to any trial involving members of the public, and of course prior to any actual contracting and deployment of a technology. The resources to fund such consultation must be considered part of the costs of acquisition and budgeted for accordingly. Bodies responsible for enforcing the law must be demonstrably compliant with the law in all of their dealings if public trust is to be achieved or deserved.

On this topic, PI would like to note that ensuring that third parties involved in facial recognition-related initiatives operate with lawful authority is not the only thing that police agencies should assure themselves of. In its work, PI observes that as authorities around the world seek to expand their surveillance capabilities and harness the power of data to deliver public services, they often have recourse to the services of private technology companies, through public-private partnerships ("PPPs").[13] These partnerships raise serious human rights questions regarding the involvement of private actors in the use of invasive surveillance technologies and the exercise of powers that have been traditionally understood as the state's prerogative.

Through its investigative work and the work of its partners around the world, PI has identified a number of issues common to PPPs that involve surveillance technology and/or the mass processing of data. To address these issues, PI have defined corresponding safeguards that they recommend for implementation by public authorities and companies who intend to enter into such partnerships. Classified between principles of Transparency, Proper Procurement, Legality, Necessity & Proportionality, Accountability, Oversight and Redress, together they seek to uphold human rights and restore trust in the state's public functions as these increasingly get outsourced to private hands. The safeguards intend to be jurisdiction-blind, so that they can apply as widely as possible across the globe. We humbly invite the Commissioner to review these proposed safeguards (and the examples of abuse they seek to remedy) and consider how they

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

[13] PI, Unmasking Policing, Inc., https://privacyinternational.org/campaigns/unmasking-policing-inc.

could be integrated and upheld in this guidance for the use of FRT by police agencies in Canada. The safeguards have not yet been officially launched and we are currently seeking feedback from some of the partners we work with around the world, but please find a near-final draft as **Exhibit 1** to this submission.

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

In our opening comments for this submission, we expressed a reservation that the mere publication of these guidelines, which address "how", more fully than "if", FRT has a role to play in rights-respecting law enforcement, might change the focus of public conversations towards finding the "best" way to enable FRT use by police.

This is particularly important to consider, because while these guidelines are appropriately addressed towards policing bodies, they also have an important role to play in educating members of the public about their rights in relation to FRT. When formally in place, the guidelines will be relied upon by members of the public to develop an understanding of the legal authorities under which police may use FRT, the factors police should be required to assess prior to acquiring FRT, and the safeguards they should put in place to ensure any use of the technology is lawful, ethical and fair.

But there is a serious risk that putting public focus on these "how" questions will forestall or supplant rigorous questioning of the "if" or "when" questions that still have received insufficient attention in Canada. And that matters, a lot, because FRT is genuinely dangerous. Its data source is our faces, the outward signifier of who we are. It can run hidden, behind camera infrastructures that have been in use long enough to be largely invisible by virtue of familiarity, or in conjunction with image databases, such as mugshots, whose collection is governed at least in part under laws that did not contemplate the quantitatively and qualitatively different abilities of FRT in relation to their use.[14] Again, this is particularly relevant in the context of the systemic over-policing of racialized peoples, who are subsequently more likely to be represented in such databases.[15]

FRT is sufficiently powerful that it has the potential to fundamentally change the relationship between residents and the state. It has implications that stretch beyond the confines of public sector privacy law into the social impacts of surveillance, the ethical morass surrounding artificial intelligence, the blurring (or artificially claimed but practically non-existent) boundaries between public and private sector information collection and use, and the interlinked relationships between big data, social sorting and profiling, and discrimination. A strict adherence to a technical, legal definition of privacy grounded in personally identifiable information is profoundly insufficient to address the interlocking risks to those rights which

[14] As, for example, the *Identification of Criminals Act* R.S.C., 1985, c. I-1.

[15] See, for example, Scot Wortley and Maria Jung, "Racial Disparity in Arrests and Charges: An analysis of arrest and charge data from the Toronto Police Service. Submitted to the Ontario Human Rights Commission, July 2020. Available: http://www.ohrc.on.ca/sites/default/files/Racial%20Disparity%20in%20Arrests%20and%20Charges%20TPS.pdf.

initially rely on an ability to move through the world without routine scrutiny by the state. Yet guidelines that stretch beyond those legal confines will predictably be resisted and will be difficult if not impossible to enforce.

We recognize that there is a rock on one side and a hard place on the other, and these guidelines fit between. The appetite for experimentation with Clearview AI (41 entities in Canada were listed in internal company data as having used the software) speaks to the reality that police forces across the country are interested in moving forward with some form of FRT.[16] In Toronto, the Police Services Board is considering AI policy that encompasses FRT and has used FRT since 2018. Calgary was the first force in Canada to adopt FRT in 2014. Other forces across Canada have allocated funds in their budget, expressed interest in the technology, or have recently finalized contracts with vendors.[17]

The risks of FRT should never be considered by looking only at the technology on its own (as the guidelines do), but always at the context in which it is deployed, and the numerous social goods it threatens. For example, Clearview AI's technology is not a mere searchable face database. It is a dystopian tool that unlocks the ability for anyone to identify anyone both online and in the physical world, and to combine online and physical world information to track, surveil and potentially stalk or harass in much more efficient ways.[18] We of course acknowledge and welcome the Commissioner's finding that RCMP's use of Clearview AI's technology was unlawful, but we worry that a slightly different technology deployed in better adherence to procedural safeguards may check all the boxes in the guidance, while having the same unacceptable effects on fundamental rights.

While careful and comprehensive guidelines, as these are, seem pragmatically better than no guidelines, the risk of their mere existence serving to preclude conversations about whether police should or should not be using FRT at all is real, and troubling. This is particularly the case because conversations in relation to a series of access to information requests submitted by CCLA regarding police use of FRT across the country have indicated that many forces are awaiting the arrival of these guidelines prior to moving forward with acquiring the technology.

[16] See Buzzfeed's release of Clearview AI company data, Ryan Mac, Caroline Haskins and Antonio Pequeño, "Police in at least 24 countries have used Clearview AI. Find out which ones here," August 25, 2021, available: https://www.buzzfeednews.com/article/ryanmac/clearview-ai-international-search-table.

[17] York Regional Police allocated 1.68 Million dollars for a "Facial Recognition and Automated Palm and Fingerprint Identification System", Regional Municipality of York Police Services Board, Revised Agenda Public Session, November 7, 2018, http://www.yrpsb.ca/usercontent/meetings/2018/nov/Merged_Agenda_Package_-_Public_Board_Meeting_Nov07_2018.pdf.; Alberta's IPC is on record encouraging Edmonton Police to seek a privacy review for their intended FRT program, see Jordan Omstead, "Caution urged as Edmonton police explore facial recognition technology," CBC News , February 5, 2020, https://www.cbc.ca/news/canada/edmonton/caution-urged-as-edmonton-police-explore-facial-recognition-technology-1.5451823; and the Sûrete du Québec finalized a contract with IDEMIA Identify and Security Canada for $4.4 million in August 2020, see Kevin Dougherty, "Quebec lawmakers raise the alarm over police use of facial recognition," iPolitics, September 22, 2020, https://ipolitics.ca/2020/09/22/quebec-lawmakers-raise-the-alarm-over-police-use-of-facial-recognition/

[18] Privacy International, Get out of our face, Clearview!, https://privacyinternational.org/campaigns/get-out-our-face-clearview.

There is the related risk that the guidelines, once implemented, will also serve to lessen the urgency for a badly needed new legal regime to govern the collection and use of biometric identifiers in Canada.

In this context, PI would like to draw the Commissioner's attention to the repercussions of a judgment from the Court of Appeal of England & Wales in the case of *Bridges v South Wales Police*.[19] The Court found in this case that the deployment of Automated Facial Recognition technology by the South Wales Police breached a number of data protection laws and equality laws, and that there were "fundamental deficiencies" [20] in the legal framework surrounding the use of the technology. While we welcomed this judgment, we have observed various police forces later rely on it as providing that their use of facial recognition technology can be lawful if they develop better policies, such as to "who" can be placed on a watchlist and "where" the technology can be deployed. Police forces in the UK have thereby not been deterred from using the technology and some are currently deploying live facial recognition technology.[21] We therefore worry that despite numerous strong statements about the dangers of FRT and need for necessity and proportionality in its use, "easy-to-fix" concerns and guidance on how to fix them actually detract from engaging in the more serious and fundamental questions about the place of such a technology in democratic societies.

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

The CCLA submits that police use of FRT is not appropriately regulated in Canada under existing law. The patchwork of legal instruments deemed relevant in the guidelines is insufficient in oversight provisions, insufficient in enforcement options, and insufficient to protect the fundamental rights threatened by biometric surveillance, including privacy, freedom of expression, freedom of association, and equality.

A cross-sector data protection law grounded broadly in a human rights framework would come closer to the mark, particularly in an environment where the private and public sector are using the same technologies (albeit often to different ends) but are now subject to different legal requirements. Targeted laws governing biometrics or more broadly, data-intensive algorithmically enabled or driven technologies could be even better fit for purpose, and there are a number of examples globally where such legislation has recently been enacted or is under consideration.[22] In Canada, we already have a specific statute governing police use of DNA, so

[19] *R (Bridges) v Chief Constable of South Wales Police* [2020] EWCA Civ 1058. Available at https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment-1.pdf.

[20] Ibid, para 91.

[21] See Metropolitan Police, Live Facial Recognition. Available at https://www.met.police.uk/advice/advice-and-information/facial-recognition/live-facial-recognition/.

[22] See for example the Illinois Biometric Privacy Act, 740 ILCS 14; New York Senate Bill S79; and Vermont S.124 (Act 166) An act relating to governmental structures protecting the public health, safety and welfare.

the precedent has been established with regards to a data of a highly sensitive and personal nature.[23]

Oversight

Accountable surveillance, a term used in a recent article by the UK Surveillance Camera Commissioner's Office (itself an example of a possible model), is increasingly necessary to enforce in a world where new options for tracking, monitoring, and identification proliferate.[24] There is a dearth of effective, independent oversight (not just review) and public transparency requirements in the current legal framework that leaves significant accountability gaps.

A key factor is a comprehensive oversight mechanism for police use of surveillance technologies that brings a range of perspectives, including from law enforcement and civilian stakeholders, to bear on the full suite of questions relevant to considering potential use of FRT and other invasive, data-driven surveillance technologies. In this regard the CCLA adopts the suggestions regarding "Crafting an Oversight Framework that would be Adequate" contained in the submission to this consultation by Professors Austin and Slane for the creation of an independent, external oversight body and correlated processes.[25]

Enforcement

Enforcement is an area amenable to improvement within current privacy laws. While policing is a provincial responsibility and most police forces are governed by provincial or municipal privacy laws, federal laws govern the RCMP. Here we address only required improvements to the relevant federal privacy legislation.

The Office of the Privacy Commissioner of Canada, alone and together with the provincial Commissioners, has recently engaged in three investigations regarding facial analytic and facial recognition technology, and made detailed findings. In each of these cases, there were provisions in our current federal public and private sector laws that applied and allowed for pointed findings, but no consequences beyond naming and shaming. In each case, those under investigation pushed back or disputed recommendations, and the lack of enforcement powers, including a lack of binding order-making powers, for the federal Commissioner meant no administrative penalties could be applied. Bill C-11 would not have solved this problem and it remains to be seen whether the next private sector privacy law proposed will be fit for this purpose.

The recent consultation regarding modernizing Canada's Privacy Act posed questions regarding the need to provide the Privacy Commissioner with the power to issue orders, expand the Federal Court's review jurisdiction to encompass matters relating to the collection, use, disclosure, retention and safeguarding of personal information, and adding new offences for serious

[23] DNA Identification Act (SC 1998, c. 37).

[24] Surveillance Camera Commissioner's Office, "What we talk about when we talk about biometrics…*", 12 October 2021. Available: https://videosurveillance.blog.gov.uk/2021/10/12/what-we-talk-about-when-we-talk-about-biometrics/.

[25] Austin and Slane (October 2021). P. 4

violations of the Act.[26] These measures are necessary for the OPC's review function of Canada's national police force, the RCMP, to gain in effectiveness.

Fundamental Rights Protections

There are risks to rights inherent in FRT, and more broadly speaking, algorithm-driven decision making, inferential algorithms, and a range of other potential biometric technologies that may be used to facilitate remote surveillance, and whose impacts go beyond privacy to potentially infringe a wide range of *Charter*-protected rights. A focus on regulating the use of individual, personally identifiable information cannot fully mitigate these risks, which may also adhere to groups who are socially sorted using a range of personal and inferred data, and subject to differential treatment as a result in ways that may be subtle and cumulative rather than direct and focused. The recommended range of perspectives necessary to consider when determining how to regulate the diffuse and socially corrosive impacts of unrestrained surveillance is well expressed by the current Surveillance Camera Commissioner in the UK:

1. The technologically possible (what can be done)
2. The legally permissible (what must/must not be done) and
3. The societally acceptable (what communities will tolerate and support).[27]

The need for a framework to support fundamental rights protections beyond the scope of privacy rights alone supports the call for an independent, external, multidisciplinary oversight body for police use of data-driven surveillance technologies including FRT, as per the recommendation above.

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

FRT should be unlawful if deployed in bulk/indiscriminately (i.e. taking a mass surveillance approach).

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

[26] Government of Canada. "Respect, Accountability, Adaptability: A discussion paper on the modernization of the *Privacy Act*. Available: https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/raa-rar.html#s1

[27] Fraser Sampson. *Response to the Government's Statutory Consultation on the Surveillance Camera Code under s. 29(5)(e)*. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1017674/Fraser_Sampson_s_response_to_SC_Code_Revision_FINAL_08.09.2021.pdf

One ‘no-go-zone’ would also be the use by police agencies of privately deployed FRT systems and watchlists. For example, PI last year denounced the partnerships between police forces in the UK and the company Facewatch, which sells FRT software to retail stores and other businesses and allows them to upload pictures of “subjects of interest” (“SOIs”) so they are alerted when these enter their premises.[28] Facewatch even centralizes the lists of SOIs that their subscribers upload and may share them with surrounding subscribing businesses. The issue with such a partnership is two-fold: (1) it puts policing powers in the hands of private actors, allowing them to decide who is a suspect or potential criminal; and (2) it expands the realms of surveillance in allowing the police to extend the reach of its surveillance to private spaces. We invite the Commissioner to warn about the use of such public-private partnerships which tend to skirt established procurement procedures and to operate outside the legal framework governing policing powers and refer in this regard to the proposed safeguards in **Exhibit 1** (as introduced above).

CCLA notes that this question, and the others which address specific permissions and protections for FRT uses (i.e. What protections should be granted to individuals whose biometric information is included in a faceprint database? Should police use of FR, including the collection of faceprints, be limited to a defined set of purposes (such as serious crimes or humanitarian reasons, e.g. missing persons)? Should they be able to use or retain faceprints beyond those of individuals who have been arrested or convicted?) are precisely the kinds of questions that Canada needs a multistakeholder, statutorily created, independent oversight authority to consider, as per our recommendations and those of Austin and Slane in the “oversight” section above. Drawing on inspiration from the recently legislatively created Vermont Criminal Justice Council with regards to FRT policy,[29] such questions require careful consideration by a multidisciplinary group with the dedicated time, resources, and specific mandate to engage with the full range of stakeholders to determine the correct answers, for people in Canada, now and for the future.

CCLA further recommends, as is the case in Vermont, a moratorium on facial recognition technology by law enforcement officers until such time as the suggested oversight body has had the chance to consider and answer these and other questions, and made its recommendations for a federal/provincial/territorial policy on law enforcement acquisition and use of FRT.

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

This includes, for example, emerging legal, ethical, or social issues in relation to

[28] Privacy International (15 October 2020) Facewatch: the Reality Behind the Marketing Discourse. Available at: https://privacyinternational.org/long-read/4216/facewatch-reality-behind-marketing-discourse.

[29] See Vermont S.124 (Act 166) An act relating to governmental structure protecting the public health, safety and welfare, s. . October 7, 2020. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1017674/Fraser_Sampson_s_response_to_SC_Code_Revision_FINAL_08.09.2021.pdf

the development and implementation of faceprint databases by the police. If so, what are these issues, and how do you recommend they should be addressed?

Felix Stalder, in an opinion piece aptly entitled "Privacy is not the antidote to surveillance" notes that surveillance is "a structural problem of political power."[30] We give our law enforcement agencies extraordinary powers, of investigation, arrest, and detention to enforce the rule of law. In turn, effective accountability and transparency must form a key part of the structure that upholds police in their powers. FRT and other data-intensive surveillance technologies have the potential to obliterate privacy, to render it impossible to move through public space unwatched, uncategorized, unidentified.

It is reasonable to note here, in a closing section on emerging issues in relation to the development of faceprint databases by police, Woodrow Hartzog and Evan Selinger's five distinguishing features of FRT that differentiate it from other biometrics, and other data-driven surveillance technologies. First, they note, faces are hard to hide, hard to change, cannot be encrypted and are remotely capturable covertly and from a distance. Second, there is an existing set of legacy databases containing images, including driver's licenses, passports, mugshots, social media profiles, all created for other purposes, legally authorized or consensual, all potentially able to be leveraged. Third, data inputs are images that are easily collected by current technology—CCTV cameras, body cams, dash cams—tools in the field right now. This can happen behind the camera technology the public sees and knows about, invisibly. Fourth, he identifies the risk of "tipping point creep" as a shift from static, after the fact analysis to live, precautionary analysis is technologically relatively simple and likely as social acculturation to the technology occurs. Finally, faces are part of our core identity, online and off, connecting what Hartzog and Selinger call our "real-name, anonymous, and pseudonymous activities."[31]

These five features put the potential structural power of FR technology, wielded by law enforcement, into stark relief. FRT uses our face against us in policing contexts. It can, and generally will, happen covertly. It builds on a range of legacy databases; mugshot databases in particular carry their own legacy due to the well-documented disproportionate arrest and charging of those who are Black and Indigenous.[32] It can be live or retroactive; if the latter, any image taken at any time in any circumstance could be used as a comparator in contexts where even if the acquisition was "lawful" at the time and in the circumstances, might have occurred without any public understanding or anticipation of such a use.

There is a disturbing trend in conversations regarding law enforcement use of FRT to talk about "uncontroversial" or even "common" uses such as comparisons of captured images with a mugshot database, as opposed to "controversial" uses such as using FRT live in public spaces. But current uses are not "uncontroversial," law enforcement bodies have simply gotten away with thus far. For example, in Toronto it began with a secretive pilot project that went public when a journalist noticed a report in a set of technically public, but practically obscure, Police

[30] Felix Stalder, (2002). "Opinion. Privacy is not the antidote to surveillance." Surveillance & Society. Available: https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/3397/3360

[31] Woodrow Hartzog (August 2, 2018). "Facial Recognition is the Perfect Tool for Oppression." Medium. Available: https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66

[32] Supra, note 7.

Board Minutes. By the time it came to light, The Toronto Police Service had already decided to proceed with a full implementation of the technology.[33] There may be a spectrum of uses, a concept that emerged at the previously mentioned Ontario IPC roundtable, but there is no part of that spectrum that is free of privacy risks or pressing social questions about discriminatory impacts.

Canada needs a public debate about FRT. The conversations around the guidelines that are the subject of this consultation have begun that process, but only among a small group of law enforcement groups, civil society actors, academics and privacy regulators, not our democratically elected representatives, and not the broader public. More is needed. As a next step to this consultation, CCLA believes the OPC is well positioned to initiate and lead some of those necessary public consultations, which must include a component of public education.

Both the CCLA and PI are grateful for the opportunity to make this submission and look forward to ongoing conversations on facial recognition technology and its appropriate constraint and regulation.

[33] See Kate Allen and Wendy Gillis, (May 28, 2019) Toronto police have been using facial recognition technology for more than a year. Available: https://www.thestar.com/news/gta/2019/05/28/toronto-police-chief-releases-report-on-use-of-facial-recognition-technology.html