UNIVERSITY OF TORONTO

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

22 October 2021

Office of the Privacy Commissioner of Canada
30, Victoria Street
Gatineau, Quebec
K1A 1H3

Information and Privacy Commissioner of Ontario
2 Bloor Street East
Suite 1400
Toronto, ON M4W 1A8

Dear Members of the Office of the Privacy Commissioner of Canada and the Information and Privacy Commissioner of Ontario,

Re: Consultation on draft guidance for police services to clarify their privacy obligations with respect to their use of facial recognition ("FR") technology

The Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto ("Citizen Lab"), is an interdisciplinary laboratory which focuses on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security. Our work relies on a "mixed methods" approach to research combining practices from political science, law, computer science, and area studies. Citizen Lab research has included, among other work: investigating digital espionage against civil society; documenting Internet filtering and other technologies and practices that impact freedom of expression online; analyzing privacy, security, and information controls of popular applications; and examining transparency and accountability mechanisms related to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Our submission is based on research that we have conducted at the Citizen Lab, and is submitted in our individual capacities as fellows of the Citizen Lab.

Part 1. Overview of the Citizen Lab's research on algorithmic policing technologies

Over the past several years, we have conducted in-depth analysis of the human rights impacts of emerging technologies in the area of predictive policing and algorithmic surveillance, as well as the relevant law and policy issues that are engaged by such issues. Our findings and law reform recommendations are contained in a report jointly released in 2020 by the Citizen Lab (Munk School of Global Affairs & Public Policy, University of Toronto) and the International Human Rights Program (IHRP) (University of Toronto's Faculty of Law), titled *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada* ("*To Surveil and Predict*").[1] A copy of our report is appended to this letter.

Algorithmic policing technologies, like facial recognition technology ("FRT"), have arrived or are coming to Canadian cities and provinces, and they are doing so quickly. In *To Surveil and Predict*, we identified a number of significant policy, practice, and legal deficits related to the use of algorithmic policing technologies in Canada, including imminent or foreseeable impacts to human rights and fundamental freedoms including the rights to privacy, liberty, and equality, expressive and associational freedoms, and others.

Among those recommendations, we identified a subset of priority recommendations that governments and law enforcement authorities must act upon with particular urgency. These priority recommendations, if implemented, are the most likely to mitigate some of the worst human rights and *Charter* violations that could occur as a result of Canadian government and law enforcement agencies using algorithmic policing technologies.[2] This shortlist of priority recommendations is set out again here for ease of reference:

a. **Governments must place moratoriums** on law enforcement agencies' use of technology that relies on algorithmic processing of historic mass police data sets, pending completion of a comprehensive review through a judicial inquiry, and on use

[1] Kate Robertson, Cynthia Khoo, and Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (September 2020), Citizen Lab and International Human Rights Program, University of Toronto ("*To Surveil and Predict*").

[2] If heeded, these priority recommendations may result in bans or severe limitations on some forms or uses of algorithmic policing technology in circumstances where nothing less would sufficiently protect constitutional or human rights. In that context, subsequent recommendations become moot, inapplicable, or of lesser importance, as they come into effect only where an algorithmic policing technology would, in fact, be used. See *To Surveil and Predict*, *supra* at p 151-152.

of algorithmic policing technology that does not meet prerequisite conditions of reliability, necessity, and proportionality.

b. **The federal government should convene a judicial inquiry** to conduct a comprehensive review regarding law enforcement agencies' potential repurposing of historic police data sets for use in algorithmic policing technologies.

c. **Governments must make reliability, necessity, and proportionality prerequisite conditions** for the use of algorithmic policing technologies, and moratoriums should be placed on every algorithmic policing technology that does not meet these established prerequisites.

d. **Law enforcement agencies must be fully transparent** with the public and with privacy commissioners, immediately disclosing whether and what algorithmic policing technologies are currently being used, developed, or procured, to enable democratic dialogue and meaningful accountability and oversight.

e. **Provincial governments should enact directives regarding the use and procurement of algorithmic policing technologies**, including requirements that law enforcement authorities must conduct algorithmic impact assessments prior to the development or use of any algorithmic policing technology; publish annual public reports that disclose details about how algorithmic policing technologies are being used, including information about any associated data, such as sources of training data, potential data biases, and input and output data where applicable; and facilitate and publish independent peer reviews and scientific validation of any such technology prior to use.

f. **Law enforcement authorities must not have unchecked use of algorithmic policing technologies in public spaces**: police services should prohibit reliance on algorithmic predictions to justify interference with individual liberty, and must obtain prior judicial authorization before deploying algorithmic surveillance tools at public gatherings and in online environments.

g. **Governments and law enforcement authorities must engage external expertise, including from historically marginalized communities that are disproportionately**

impacted by the criminal justice system, when developing regulation and oversight mechanisms for algorithmic policing technologies, as part of completing algorithmic impact assessments, and in monitoring the effects of algorithmic policing technologies that have been put into use.

This submission does not seek to repeat the findings and conclusions set out in our report that accompany the above priority recommendations. Instead, in order to contribute to the OPC's and IPC's development of guidance for police services on FRT, this submission serves to provide further particularized input in two areas.[3] **Part 2** responds to the Commissioners' request for feedback in regards to the legal and policy framework concerning the use of FRT. It makes recommendations regarding the need to require independent, comprehensive oversight in any legal framework that purports to regulate the use of FRT. **Part 3** details a recommendation to expand the public disclosure obligation set out in paragraph 107 of the *Draft privacy guidance.*

Part 2. Lawful Authority and the Importance of Independent, Comprehensive Oversight

Part 2 of this submission responds to the Commissioners' request for feedback in regards to the legal and policy framework concerning the use of FRT. The Citizen Lab urges the Commissioners to affirm the importance of requiring independent, comprehensive oversight in any legal framework that purports to restrain police conduct that intrudes upon protected zones of privacy through the use of FRT.

In the landmark decision in *Hunter v. Southam Inc.*, the Supreme Court of Court determined that a warrantless search is presumptively unreasonable. The presumed constitutional standard for searches or seizures in the criminal sphere is judicial pre-authorization: a prior determination by a neutral and impartial arbiter, acting judicially, that the search or seizure is supported by reasonable grounds, established on oath.[4] The *Draft privacy guidance*

[3] We note that this submission is written entirely by members of the Citizen Lab; assertions and positions provided in this submission may not wholly reflect those of the International Human Rights Program and, as such, should not be attributed to them unless they have explicitly indicated so elsewhere.

[4] *Hunter v Southam Inc.*, [1984] 2 SCR 145; *R v Tse*, 2012 SCC 16.

acknowledges the availability of judicial authorizations to obtain lawful authority to collect and use faceprints in circumstances that merit such action.

Failures by police agencies to obtain prior judicial authorization in respect of privacy-impacting police activity are unlawful and unconstitutional.[5] Even in statutory frameworks applicable to police activity carried out in exigent circumstances,[6] the absence of mandatory, independent oversight mechanisms can be constitutionally fatal to a statutory scheme. For example, in *R v Tse*,[7] the Supreme Court of Canada struck down a provision of the *Criminal Code* that purported to authorize the warrantless interception of private communications in exigent circumstances involving an apprehension of imminent serious harm. The Court held that even though the exigent circumstances requirement provided justification for a warrantless interception, the statutory provision still violated section 8 of the *Charter*. Parliament had failed to "provide any mechanism to permit oversight of the police use of this power."[8] The Court wrote that it was "[o]f particular concern, [that] it does not require that notice be given to persons whose private communications have been intercepted."[9] The statutory power was also unjustifiably exempted from the Parliamentary reporting requirements that are applicable to other wiretap authorizations under the *Criminal Code*.

With the growing emergence of an algorithmic policing technology ecosystem and corresponding privacy threats associated with law enforcement authorities' access to personal information through their use of such technologies, the urgent need for enhanced, comprehensive, and independent oversight of police services is clear. Prior judicial oversight is critical to the protection of the public interests at stake when law enforcement seeks to rely on algorithmic surveillance technologies such as FRT.[10] The UN High Commissioner for Human Rights has called for the involvement of all branches of government in the oversight of surveillance programs to supplement judicial oversight as well as for the establishment of

[5] This requirement has of course been modified in the context of exigent circumstances.
[6] Such as an apprehension of the occurrence of imminent serious harm.
[7] *R v Tse*, 2012 SCC 16.
[8] *R v Tse*, 2012 SCC 16 at para 11.
[9] *R v Tse*, 2012 SCC 16 at para 11.
[10] See Hunter v Southam, [1984] 2 SCR 145; R v Duarte, [1990] 1 SCR 30; R v Tse, 2012 SCC 16; R v Jones, [2017] 2 SCR 696, at para 74; UN Human Rights Council, "The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights" (30 June 2014) A/HRC/27/37 <https://undocs.org/A/HRC/27/37>, at para 37.

independent civilian oversight agencies.[11] Robust oversight of the use of algorithmic surveillance technologies, at minimum, is required to enable public confidence that law enforcement agencies' use of algorithmic tools is reasonably justified, necessary, and proportionate. Where law enforcement authorities seek to engage in preemptive data collection practices, the practice contravenes this long-established principle that police action that intrudes into protected freedoms be subject to meaningful oversight.

Current Canadian privacy and data protection laws governing police services are not sufficient safeguards of the right to privacy given the formidable reach and dangers associated with algorithmic policing technologies. Through a series of related recommendations in the report, *To Surveil and Predict*, the Citizen Lab and IHRP recommended a revitalization of Canada's system of oversight governing the use of algorithmic technologies in Canada's justice system.[12] Canada has a complex network of regulatory actors that share partially overlapping roles in governing and overseeing law enforcement agencies. No doubt, making this system effective in respect of 21st century technologies will require reform of numerous areas of legislation at multiple levels of governments.

Pervasive inadequacies in the manner in which police services apply the existing regulatory framework governing the collection and retention of biometric information demonstrate the dangers created by a failure to require a mandatory, independent system of oversight in the statutory schemes. The creation and/or use of biometric databases by police services has significant privacy implications associated with the collection and retention of personal information from individuals. Two factors in particular contribute to the heightened privacy risks associated with police use of FRT: the nature of the biometric data captured, and the nature of FRT itself.

Biometric data such as faceprints is a form of particularly sensitive data, warranting rigorous protections that go beyond previous privacy regulations and safeguards, in order to maintain the baseline standard of privacy rights to which everyone in Canada is constitutionally entitled. Regulators and lawmakers in Canada and around the world have recognized the

[11] UN Human Rights Council, "The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights" (30 June 2014) A/HRC/27/37 <https://undocs.org/A/HRC/27/37>, at para 37. Additional oversight was adopted, for example, in legislative amendments to the *Criminal Code* in the 1970s, which regulate interceptions of private communications. To reinforce accountability measures, the Minister of Public Safety and Emergency Preparedness is statutorily obliged to prepare and present to Parliament with an annual report regarding the use of intercepts and wiretap surveillance: Criminal Code, s. 195.
[12] See *To Surveil and Predict*, Part 6, Recommendations 1, 3, 4, 5, 7, 9, 14, and 15.

special status of biometric data relative to other forms of personal data, due to its sensitivity and immutability.[13] While one may—albeit at great inconvenience and potential hardship—opt not to share the kinds of personal data collected through social media websites, or refrain from sharing personal information with a brick-and-mortar store, for example, it is not similarly possible to simply leave one's face at home when going out in public. Further, faceprints raise unique concerns even relative to other types of biometric data. For instance, while it is possible to obtain an individual's fingerprints without their knowledge in certain circumstances, the ease of remotely obtaining and storing faceprints of individuals from afar is incomparable to the challenge that would be posed by attempting to collect fingerprints from members of the public *en masse* without their knowledge.[14] It would be trivial, however, for FRT to capture individuals' faces in opaque databases with them being none the wiser—whether they are crossing the street, attending a protest, doing on-site news reporting, or visiting with friends in a different neighbourhood.

Due to the emergence of FRT, the privacy interests associated with faceprints are even more heightened. FRT takes a category of personal data that is already especially sensitive, and subjects it to an especially powerful and far-reaching form of privacy-threatening technology. Additionally, FRT heightens the privacy implications of pervasive use and access to CCTV cameras in cities, and the collection of faceprints by police from private companies or online platforms. However, the collection and retention practices of faceprints by law enforcement authorities is not an area that has historically benefited from adequate independent oversight mechanisms. Individual police services have differing policies with respect to the collection, retention, disclosure, or destruction of biometric data.[15]

---

[13] See e.g., Els Kindt, "A First Attempt at Regulating Biometric Data in the European Union" in *Regulating Biometrics: Global Approaches and Urgent Questions*, ed Amba Kak, AI Now Institute (September 2020), <https://ainowinstitute.org/regulatingbiometrics-kindt.pdf>; "Biometric Information Privacy Act (BIPA)", ACLU Illinois, <https://www.aclu-il.org/en/campaigns/biometric-information-privacy-act-bipa>; and "What is special category data?", United Kingdom Information Commissioner's Office, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/special-category-data/what-is-special-category-data/#scd4>.

[14] Clare Garvie, Alvaro M Bedoya and Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Center on Privacy & Technology at Georgetown Law (2016), at 10 <https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf>.

[15] By way of historical comparison to these ongoing issues, prior to the enactment of the *Police Record Checks Reform Act* (PRCRA), 2015, S.O. 2015, c. 30, law enforcement authorities likewise wielded an excessive amount of discretion in the area of criminal record checks in Ontario. The absence of clear regulatory limits on law enforcement's handling of criminal record checks caused significant harm to Ontarians who came into contact with the criminal justice system. The PRCRA limited the disclosure of non-conviction information, given the

By way of example, arrest photographs ('mugshot' photographs) are obtained through police arrest powers,[16] and law enforcement authorities are even authorized to use force if it is needed to obtain the photograph.[17] It is not a consent-driven process. Multiple law enforcement agencies in Canada report using (or are planning to use) FRT against their arrest photograph databases. However, arrest photograph databases contain photos of individuals who have never been charged with criminal offences, who have had their charges withdrawn, or who have been found innocent of allegations. Individuals have a constitutionally-protected right to privacy in relation to their faceprint, and the unauthorized retention of biometric data such as faceprints is unconstitutional. However, jurisprudential guidance (obtained from court case litigation) is sparse and largely out of date in this area. Technological developments have rapidly increased the privacy interests that are at stake in biometric information such as DNA and facial images.[18]

In practice, each police service has its own internal policies with respect to the destruction of arrest photographs. In many police services, the destruction of biometric information is a request-based system (i.e., individuals must request their data be destroyed, as opposed to data being regularly destroyed automatically and in accordance with justified limits). Current processes through which a person can request the destruction of records after their case is dealt with are likewise inconsistent, fee-based, vague, and/or overly discretionary.[19]

Conclusion in respect of Part 2

As noted above, the Citizen Lab has **recommended that governments place moratoriums** on law enforcement agencies' uses of algorithmic policing technology that do not meet prerequisite conditions of reliability, necessity, and proportionality. If heeded, this priority recommendation may result in bans or severe limitations on some forms or uses of algorithmic policing technology in circumstances where nothing less would sufficiently protect constitutional or human rights. Given the demonstrable human rights risks of FRT, in addition to their unreliability, police services should halt any further use or adoption

pre-existing, discretionary regulations led to unjustified, discriminatory, and arbitrary practices with the disclosure of non-conviction information in the employment and education contexts, to the detriment of individuals' livelihoods, dignity, and personal/family wellbeing.

[16] *Identification of Criminals Act*, RSC, 1985, c I-1.

[17] *Identification of Criminals Act*, RSC, 1985, c I-1, at s 2(2).

[18] *R v Strickland*, 2017 BCPC 1, and 2017 BCPC 211; *R v Dore*, [2002] OJ No 2845 at paras 64-71 (CA).

[19] See for example *Lin v Toronto Police Services Board*, [2004] OJ No 170 (SCJ); Information and Privacy Commissioner of Ontario, Privacy Complaint No. MC-060020-1 (21 December 2007), <https://decisions.ipc.on.ca/ipc-cipvp/privacy/en/135086/1/document.do>.

of FRT until and unless appropriate laws and regulations are in place and such tools have been shown to meet prerequisite conditions of reliability, necessity, and proportionality.

Assuming the preconditions to the use of FRT could be satisfied, an appropriate legal framework restraining the use of the technology would then be critical. Part 2 of this submission has urged the Commissioners to incorporate throughout the ongoing work and guidance for police services an acknowledgement that it is not enough to be following the right kind of rules. Police services also need to be subject to the right kind of oversight to provide public confidence that those rules are respected.

Judicial authorization in respect of investigative uses of FRT ("1:N" matching[20]) is one necessary and critical component of a comprehensive system of oversight. However, it is not alone sufficient. Any legal framework that is prospectively considered in the regulation of police use of FRT must include comprehensive oversight, including, for example:

- Judicial authorization in respect of the collection of faceprints;
- Mandatory independent auditing of data management practices and policies associated with faceprints;
- The replacement of discretionary regulations with mandatory, knowable, standardized limits restraining the collection, use, and retention of faceprints by police;
- The prohibition of reverse-onus policies by police services that, in practice, limit the police services' adherence to privacy obligations to only cases where the individual makes assertive requests for the destruction of faceprints. Instead, presumptive rules should mandate the automatic destruction of images in defined circumstances;
- A prohibition of the practice of police services to charges fees in order to process a request for the destruction of biometric information;
- Mandatory and meaningful notice requirements, including requirements that notice be provided to all individuals whose faceprint is collected by police services (including the purpose thereof and the source(s) of their faceprint), as well as notice to individuals whose photograph is in 'mugshot' databases. Notice should include notice of what lawful authority the police agency was relying upon when the photograph was collected or retained, and how to challenge the retention;

[20] As noted in the *Draft Guidance*, the term 1:N matching refers to inputting a specific image into the FRT system and comparing it against all other images in a database of pre-enrolled faces in an attempt to learn the individual's identity.

- Mandatory and robust reporting requirements to governments and the public (detailed further below).

Part 3. Recommended amendment to *Draft privacy guidance* regarding transparency

One of the priority imperatives identified in *To Surveil and Predict* is that law enforcement agencies must be fully transparent with the public and with privacy commissioners. Such transparency will involve immediately disclosing whether and what algorithmic policing technologies are currently being used, developed, or procured in order to enable democratic dialogue and meaningful accountability and oversight. Further detail pertaining to the Citizen Lab's recommendations in regards to accountability and transparency are set out in Recommendations 12, 14, and 20 of *To Surveil and Predict*.

Paragraph 107 of the *Draft privacy guidance* sets out recommendations regarding the publication of information surrounding the planning, development, and implementation of FRT systems. The *Draft privacy guidance* recommends ongoing publication of the existence and development of the initiative, a link to the Privacy Impact Assessment summary, information about statistics regarding use of FRT, the purpose of using FRT, its effectiveness, the results of testing for accuracy and bias, and a requirement to make data available for oversight purposes. We are pleased to see these features included in the *Draft privacy guidance*. **We recommend that the public disclosure obligation be expanded** to include, at a minimum:

- Inclusion of information about what training and development methods occurred in respect of the FRT;
- In publishing statistics and purposes in regards to the use of FRT, police agencies should also be disclosing what source(s) of legal authority the police agency relied upon;
- Disclosure of the results (or a summary of the results) of all audits and period reviews of program activity, including the results of the assessment of compliance with privacy requirements;
- Publication of a complete copy of all information sharing agreements and service agreements that may be put in place with third parties;

- Disclosure of all policies and procedures in place for handling personal information that is collected, used, created, disclosed and retained over the course of an FRT initiative. This should include disclosure of the following documents referred to elsewhere in the *Draft privacy guidance*:
    - standard operating procedures for performing a FR search (paragraph 89 of the *Draft privacy guidance*);
    - the protocol that specifies the circumstances under which officers are authorized to perform a FR search (paragraph 89 of the *Draft privacy guidance*);
    - Disclosure of retention periods in place for different forms of personal information (paragraph 101 of the *Draft privacy guidance*); and,
    - the policy framework that is supported by mechanisms to systematically verify that data collected by the initiative falls within the initiative's lawful authority to collect (paragraph 85 of the *Draft privacy guidance*);
- Disclosure of any appropriate threshold that may be determined in accordance with the recommendation referred to in paragraph 82 of the *Draft privacy guidance*;
- When disclosing "the results of any accuracy or bias testing performed by the police agency, with justification for any variations across groups", police agencies should also disclose the results of any independent external testing that it is in the possession of the police agency, as well as the results of any testing described in paragraph 82 of the *Draft privacy guidance*; and,
- Making training data available for oversight and review purposes (i.e., judicial approval, analysis by privacy commissioner or other independent body) in addition to search data.

We also recommend that the guidance in paragraph 107 be framed as an obligation ("must" instead of "should"), particularly given the earlier acknowledgement in the *Draft* that "[w]herever possible, individuals and the public must be informed of the purpose of the collection of their personal information, including how the information may be used or disclosed."

Requiring fulsome public disclosure—including advance public notice prior to adoption—pertaining to the use of FRT is particularly vital, given the vulnerability of the communities who are most likely to be adversely affected by the human rights harms associated with algorithmic policing technology. In the past, the burden of unveiling electronic surveillance practices by law enforcement has too often fallen on the shoulders of defendants in the criminal justice system. Allocating the burden of obtaining information

about potential rights-infringing uses of experimental technologies to individuals is unworkable, inequitable, and endangers the integrity of the justice system. Wrongful convictions and unchecked human rights violations pose unjustified and tremendous societal harm and cost.

These dangers are acute at present in Canada's justice system, due to the systemically under-resourced legal aid system and the substantial likelihood that individuals who are affected by algorithmic technologies will be unable to obtain any legal representation or legal aid assistance at all. These existing problems in Ontario's justice system, for example, have led to a colloquial description of the justice system as a "guilty-plea-machine." The vast majority of criminal cases do not go to trial and are instead dealt with through resolutions, including guilty plea resolutions. Consequently, statistics about criminal conviction rates in Canada are largely made up of guilty plea convictions. However, the 2018 Report of the Federal/Provincial/Territorial Heads of Prosecutions Subcommittee on the Prevention of Wrongful Convictions called attention to how the phenomenon of false guilty pleas has become an issue of growing concern among experts in Canada: "factually innocent persons in Canada have sometimes, for a variety of reasons, pleaded guilty to crimes they did not commit."[21] Innocent individuals who have been denied bail or who believe that they are unlikely to be granted bail may be incentivized to plead guilty in order to obtain an earlier release from custody.[22] In 2017, Department of Justice researchers found that Indigenous individuals "sometimes plead guilty even if they are innocent…, have a valid defence, or have grounds to raise *Charter* issues."[23] Research has also suggested that other marginalized groups, including youth, individuals with cognitive deficits, individuals experiencing mental health or addictions issues, individuals in poverty, and racialized individuals may also be particularly at risk of entering false guilty pleas.[24] Lack of legal aid funding has contributed to false guilty pleas from those with socio-economic disadvantage.[25] The problem of false guilty pleas is further informed by disproportionate denials of bail and by the fact that the Canadian

[21] Federal/Provincial/Territorial Heads of Prosecutions Subcommittee on the Prevention of Wrongful Convictions, *Innocence at Stake: The Need for Continued Vigilance to prevent Wrongful Convictions in Canada* (2018) at 169 <https://www.ppsc-sppc.gc.ca/eng/pub/is-ip/is-ip-eng.pdf>.
[22] *Ibid* at 179-180.
[23] Angela Bressan & Kyle Coady, "Guilty pleas among Indigenous people in Canada" (2017) at 9 <http://publications.gc.ca/site/eng/9.851369/publication.html>.
[24] *Ibid* at 6.
[25] See, e.g., Dough Schmidt, "Windsor lawyers worry that funding cuts mean more jail for poor, vulnerable" (20 June 2019) *Windsor Star*, <https://windsorstar.com/news/local-news/windsor-lawyers-worry-that-funding-cuts-mean-more-jail-for-poor-vulnerable>.

justice system does not accommodate Indigenous cultural conceptions of justice, which differ in critical ways from how criminal justice is understood and approached in Canadian law.[26]

The errors, biases, wrongful convictions, and false guilty pleas endemic within the Canadian criminal justice system may only increase when combined with the errors and biases which FRT propagates.[27] Already, police use of FRT has repeatedly led to serious cases of mistaken identity and false arrests of Black men.[28] Such consequences cannot be considered an acceptable trade-off for whatever "efficiencies" police claim are gained through FRT use. Regulators and lawmakers must accordingly implement sufficiently stringent oversight and accountability regimes—if not ban FRT altogether—to prevent such outcomes.

Due process and access to justice concerns are acute where AI-generated evidence and algorithmic surveillance techniques are involved, given the significant imbalance of power, knowledge, and resources between individual litigants and AI-developers and vendors from the private and public sectors. Lack of funding (to cover costly litigation), technological illiteracy, lack of access to expert resources, and barriers to fulsome disclosure (e.g., assertions of trace secrecy by private vendors) will also limit the ability even of individuals who are represented by counsel from accessing remedies for rights violations.

Moreover, case-by-case litigation in courtrooms is a slow and sometimes non-responsive mechanism of revealing and remedying low-visibility, yet high-impact, rights violations.

Where transparency and effective remedies to rights violations can be elusive, public access to information about the ecosystem of electronic surveillance practices and other uses of algorithmic technology by law enforcement authorities is a critical safeguard to support individuals and communities. Information can assist policymakers and justice-system participants (including courts, prosecutors, and defence counsel), to have context to identify

[26] Angela Bressan & Kyle Coady, "Guilty pleas among Indigenous people in Canada" (2017) at 6 <http://publications.gc.ca/site/eng/9.851369/publication.html>; Abby Deshman & Nicole Myers, "Set Up to Fail: Bail and the Revolving Door of Pre-trial Detention", Canadian Civil Liberties Association and Education Trust (July 2014), <https://ccla.org/cclanewsite/wp-content/uploads/2015/02/Set-up-to-fail-FINAL.pdf>.
[27] See e.g., Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, Center on Privacy & Technology at Georgetown Law (2019), <https://www.flawedfacedata.com>.
[28] See e.g., Drew Harwell, "Wrongfully arrested man sues Detroit police over false facial recognition match" (13 April 2021) *Washington Post*, <https://www.washingtonpost.com/technology/2021/04/13/facial-recognition-false-arrest-lawsuit/>; and Kashmir Hill, "Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match" (29 December 2020) *New York Times*, <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>.

gaps in existing access to justice mechanisms, and to support and enhance their respective roles.

Conclusion

The recommendations set out above are intended to provide focused commentary in respect of the central importance of oversight, accountability, and transparency in respect of the use of FRT. However, as set out above, we have identified in *To Surveil and Predict* priority recommendations that governments and law enforcement authorities must act upon with particular urgency, including the recommendation that governments act now to make reliability, necessity, and proportionality prerequisite conditions for the use of algorithmic policing technologies. The above submission does not seek to modify or replace those recommendations. We have appended a copy of the report to this submission for further detail regarding the range of legal reforms that are necessary for governments and police services in Canada to act upon in respect of the use of algorithmic policing technology.

Thank you for this opportunity to comment. We appreciate the efforts that are being undertaken through the *Draft privacy guidance* and consultation, and the attention being paid to the issues identified in *To Surveil and Predict*.

Signed:

Kate Robertson, Research Fellow at the Citizen Lab and criminal and constitutional lawyer in Toronto

Cynthia Khoo, Research Fellow at the Citizen Lab and technology and human rights lawyer

Primary contact: Kate Robertson <kate@citizenlab.ca>

Encl. *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada* (September 2020), Citizen Lab and International Human Rights Program, University of Toronto.