UNIVERSITY OF TORONTO

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

15 January 2021

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

Dear Members of the Information and Privacy Commissioner of Ontario,

Re: Consultation on the IPC's Strategic Priorities: Submission of the Citizen Lab in regards to the critical role of the IPC in modernizing Ontario's system of oversight of the use of algorithmic policing technology by law enforcement authorities

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.

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 legal reform recommendations are contained in a report jointly released 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.

We are pleased to see that findings discussed in our report concerning the constitutional and human rights impacts of algorithmic policing technology have been recognized in the *IPC Strategic Priority Setting Consultation Paper*, in the IPC's discussion of next-generation law enforcement as a potential strategic priority in the next five years. This submission does not seek to repeat the findings and conclusions set out in our report, particularly given the IPC's recognition of the connection between the IPC's mandate and the report's findings. Instead, in order to contribute to the IPC's deliberations in the triaging of its strategic priorities, this submission serves to provide particularized input with respect to the IPC's public interest mandate in the oversight of law enforcement authorities when it comes to the use of algorithmic policing technology in Ontario.[2] **Particularly given long overdue legislative responses to emerging threats to digital privacy in the 21st century, the Citizen Lab urges the IPC to prioritize a strategic role in this arena. With significant risks to Ontarians created by the growing emergence of an algorithmic policing technology ecosystem, and constitutional implications flowing from law enforcement authorities' access to personal information through their use of such technologies, the need for enhanced, urgent, and independent oversight by the IPC is pressing and substantial.**

This submission unfolds in three parts. **Part 1** provides a high-level summary of some of the complex and intersecting challenges presented by the use of algorithmic policing technology by law enforcement authorities. **Part 2** sets out some of the key reasons why confronting, regulating, and limiting the use of algorithmic policing technology by law enforcement authority must be an urgent strategic imperative to mitigate against serious potential harm to Ontarians, including some of the province's most vulnerable communities. Finally, **Part 3** outlines three key aspects of the IPC's crucial role within a comprehensive, multi-governmental approach to the oversight and regulation of emerging policing and surveillance technologies.

[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] We note that this submission to the IPC 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.

Part 1. Complex and intersecting challenges associated with the use of algorithmic policing technology by law enforcement authorities

Algorithmic policing technologies include a wide range of algorithm-driven or artificial intelligence-driven technologies intended for use in policing and law enforcement in the criminal justice context. They may be divided into two broad categories. The first is what is generally known as 'predictive policing' technology, which includes (a) location-focused predictive policing tools, which algorithmically process historical police data to purportedly predict when and where crime will next occur, before it occurs; and (b) person-focused predictive policing tools, which rely on algorithmic data analysis in order to attempt to identify people who are more likely to be involved in potential criminal activity or to assess an identified person for their purported risk of engaging in criminal activity in the future. The second broad category is algorithmic surveillance technologies, which do not necessarily include a predictive component but are used for general monitoring and surveillance on a level far beyond traditional policing methods, including facial recognition technology, automated license plate readers, social media surveillance, and social network analysis.

Algorithmic policing technologies—whether predictive policing software or algorithmic surveillance tools—raise complex questions for both constitutional and private sector privacy law that Canadian legislation and jurisprudence have yet to address directly. This deficit must be addressed with urgency in light of the rise of algorithmic policing technologies used, under development, or being considered by law enforcement agencies at the municipal, provincial, and federal levels across Canada.[3] Commercial vendors of such technologies play a major role in Canadian law enforcement where agencies purchase them as opposed to developing them in-house.[4] Our research has principally focused on the constitutional and human rights law implications in the context of criminal justice; however, over the course of this work, several significant issues concerning algorithmic policing technology vendors and private sector privacy law became apparent.

Today, police services in Canada have access to unprecedented and ever-growing amounts of data. The state's surveillance infrastructure and law enforcement's big data ecosystem

[3] See e.g., Miles Kenyon, "Algorithmic Policing in Canada Explained" (1 September 2020), Citizen Lab <https://citizenlab.ca/2020/09/algorithmic-policing-in-canada-explained/>; and Caroline Haskins, "Dozens of Cities Have Secretly Experimented With Predictive Policing Software," *Vice Motherboard* (6 February 2019) <https://www.vice.com/en_us/article/d3m7jq/dozens-of-cities-have-secretly-experimented-with-predictive-policing-software>.
[4] *To Surveil and Predict*, *supra*.

form the backdrop of, and fuel for, algorithmic policing technologies. In Ontario alone, the Toronto Police Service (TPS) has collaborated with the data broker and data analytics company Environics Analytics since 2016, to engage in "data-driven policing", and has expressed interest in potentially adopting certain forms of 'predictive policing' in the future.[5] The TPS has also used facial recognition technology for more than a year without public notice; it was only following media reports that brought the program to public attention in 2019 that the public was made aware that these technologies were being used.[6] It appears to remain uncertain what type of facial recognition system was procured by the Toronto Police Service. Also in 2019, the Ottawa Police Service (OPS) conducted a three-month pilot program with the facial recognition technology NeoFace Reveal. Both the TPS, OPS, and numerous other police services throughout Ontario admitted to informally using or testing the controversial facial recognition product Clearview AI, only after the New York Times revealed the connection.[7] In addition, the TPS, OPS, and RCMP have all engaged, or are engaging, in algorithmic social media surveillance, using products and services procured from commercial vendors.

Much of the data that are collected and processed through algorithmic policing results are made possible by way of surveillance technologies that are sold by commercial vendors, and which may remain involved in updating, running, or otherwise facilitating the surveillance even after selling the technology. As a result, these vendors can sometimes maintain at least some custody or control over collected data. Law enforcement actors may have access to smart city data, social media data, mobile device information (including location) obtained remotely, and private sector consumer data (e.g., surveillance cameras built into "smart home" devices), in addition to personal information collected through facial recognition technology, automated license plate readers, social network analysis, and social media

[5] *Ibid*, at page 45.
[6] Kate Allen & Wendy Gillis, "Toronto police have been using facial recognition technology for more than a year", *Toronto Star* (28 May 2019), <https://www.thestar.com/news/gta/2019/05/28/toronto-police-chief-releases-report-on-use-of-facial-recognition-technology.html>.
[7] "Toronto police admit using secretive facial recognition technology Clearview AI", *CBC News* (13 February 2020) <https://www.cbc.ca/ news/canada/toronto/toronto-police-clearview-ai-1.5462785>; Kelly Bennett, "Hamilton police tested controversial facial recognition technology Clearview AI", *CBC News* (20 February 2020), <https://www.cbc.ca/news/canada/hamilton/the-service-says-it-has-not-used-the-tool-for-anyinvestigative-purposes-1.5470359>; Shaamini Yogaretnam, "Ottawa police piloted controversial facial recognition software last year", Ottawa Citizen (13 February 2020), <https://ottawacitizen.com/news/local-news/ottawa-police-piloted-controversial-facial-recognition-software-lastyear>.

surveillance tools—all commercial technologies sold by private sector entities. The AI Now Institute has stated:

> AI raises the stakes in three areas: automation, scale of analysis, and predictive capacity. Specifically, AI systems allow automation of surveillance capabilities far beyond the limits of human review and hand-coded analytics. ... These systems also exponentially scale analysis and tracking across large quantities of data, attempting to make connections and inferences that would have been difficult or impossible before their introduction. Finally, they provide new predictive capabilities to make determinations about individual character and risk profiles, raising the possibility of granular population controls.[8]

Current Canadian privacy and data protection laws may no longer suffice to safeguard the right to privacy, in the face of algorithmic policing technologies' formidable reach and capabilities. We are concerned with the potential of algorithmic policing technologies, where obtained from, managed by, or operated in conjunction with commercial vendors, to result in uses by law enforcement that circumvent or undermine constitutional protections against unreasonable search and seizure under section 8 of the *Canadian Charter of Rights and Freedoms*.

Particularly given much needed legislative reform remains only on the horizon, we urge the IPC to prioritize a strategic role within this area. 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 need for enhanced, urgent, and independent oversight by the IPC is clear.

Part 2. Real and substantial human rights impacts upon the lives of Ontarians

Algorithmic policing technologies are not just fiction or imaginary potentialities. They 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

[8] AI Now Institute, *AI Now Report 2018* (December 2018) at 12 <https://ainowinstitute.org/AI_Now_2018_Report.pdf>.

privacy, liberty, and equality, expressive and associational freedoms, and others. The range of real and substantial human rights impacts associated with policing technologies warrant prioritization by the IPC as it defines its mandate.

The emergence of algorithmic policing technology within the law enforcement and commercial-sector ecosystems has taken place within the social and historical context of longstanding systemic bias and discrimination in society and in the criminal justice system. In developing legal and policy responses to the use of algorithmic policing technology by law enforcement authorities, priority consideration must be given the technology's potential impacts and risks, including the human and constitutional rights of individuals and communities that have been the subject of historic discrimination. When considering the adoption of new methods of policing, such as algorithmic policing technology, it is essential to ensure that these new methods do not aggravate or contribute to the historic disadvantage experienced by communities targeted as a result of systemic bias.

Preventing the perpetuation of systemic bias and discrimination includes asking questions such as whose personal information is being collected or used by the technology, and which individuals or communities will be most affected, and why? The use of police-generated data sets that are affected by bias may create negative feedback loops where individuals from historically disadvantaged communities are labelled by an algorithm as a heightened risk because of historic bias towards those communities.

For individuals and communities that are impacted by the criminal justice system in Canada, the adverse effects of being subjected to heightened police scrutiny, criminal litigation, and incarceration can be significant and long-lasting. The effects include heightened recidivism rates;[9] negative effects on health, poverty, and human dignity;[10] and renewed cycles of poverty and oppression that leave individuals vulnerable and in circumstances that can give rise to further police scrutiny. Even a non-custodial conviction and imposition of a criminal record can have lifelong consequences, including stigmatization, significant adverse effects on employment prospects or career, immigration consequences, and restricted travel.

[9] Paula Smith, Claire Goggin, & Paul Gendreau, "The Effects of Prison Sentences and Intermediate Sanctions on Recidivism: General Effects and Individual Differences" (January 2002), <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ffcts-prsn-sntncs/index-en.aspx>.
[10] Fiona Kouyoumdijian et al., "Health status of prisoners in Canada" (March 2016) 62 *Clinical Review* 215 <https://www.cfp.ca/content/cfp/62/3/215.full.pdf>.

Reliance on algorithmic predictions that use these inflated recidivism rates will likely exacerbate existing biases.

Adverse effects are also demonstrable when considering the impact of police stops and detentions on individuals who are the target of ongoing scrutiny. The Supreme Court of Canada recently described that the disproportionate policing of racial minorities through carding "takes a toll on a person's physical and mental health" and "impacts their ability to pursue employment and education opportunities."[11] The Court held that the "practice contributes to the continuing social exclusion of racial minorities, encourages a loss of trust in the fairness of our criminal justice system, and perpetuates criminalization."[12] Rights violations of racialized individuals also cause vicarious harm to their friends, family, and community members.[13] The historical ripple effects of the over-policing and excessive incarceration of Indigenous communities are only more severe.[14]

The lasting social and psychological impacts on individuals who have been involved with or subjected to the criminal justice system as suspects or defendants reinforce the importance of ensuring that algorithmic policing methods do not put individuals at risk of potential false positives (i.e., a mistake that misidentifies an individual or overrepresents an individual's perceived risk to the public) or of implicit discrimination that could result in biased arrests, detentions, or incarceration.

Algorithmic policing technologies also pose other imminent dangers to the human rights of all Ontarians. Algorithmic policing tools, such as algorithmic surveillance and person-focused

---

[11] *R v Le*, 2019 SCC 34 at para 95.
[12] *R v Le*, 2019 SCC 34 at paras 93-95 [citations omitted]. See also: The Honourable Roy McMurtry, *Review of the Roots of Youth Violence*, Volume 1 (2008) at 77-78, <http://www.children.gov.on.ca/htdocs/english/documents/youthandthelaw/rootsofyouthviolence-vol1.pdf>; Scot Wortley & Akwasi Owusu-Bempah, "The Usual Suspects: Police Stop and Search Practices in Canada" (2011) 21 *Policing and Society* 395 at 400-401, <https://www.researchgate.net/publication/238046161_The_Usual_Suspects_Police_Stop_and_Search_Practices_in_Canada>.
[13] Scot Wortley & Akwasi Owusu-Bempah, "The Usual Suspects: Police Stop and Search Practices in Canada" (2011) 21 *Policing and Society* 395 at 400-401, <https://www.researchgate.net/publication/238046161_The_Usual_Suspects_Police_Stop_and_Search_Practices_in_Canada>; see also: Sophie de Saussure, "Parents in prison: A public policy blind spot", Policy Options (12 July 2018), <https://policyoptions.irpp.org/magazines/may-2018/parents-in-prison-a-public-policy-blind-spot/>.
[14] Davinder Singh, Sarah Prowse and Marcia Anderson, "Overincarceration of Indigenous people: a health crisis" (2019) 191:18 CMAJ, <https://www.cmaj.ca/content/191/18/E487>.

predictions, engage the right to privacy as a result of the data collection, processing, and sharing methods that algorithmic tools inherently tend to rely on. The use of these technologies by law enforcement authorities expose Ontarians to risks of privacy harms occasioned by indiscriminate surveillance, eroding reasonable expectation of privacy in public and online spaces, unjustified and adverse effects caused by inaccurate or biased data inferences created by law enforcement's use of unreliable technology, and unjustified invasions of privacy created by unconstitutional or overbroad data-sharing between law enforcement and the private sector or other governmental agencies. Algorithmic policing technologies introduce a high risk of algorithmic discrimination as a result of relying on biased data that is derived from practices reflecting systemic discrimination against particular groups by the Canadian criminal justice system. These groups include, in particular, Black and Indigenous individuals and communities; the LGBTQ+ community; those who live with mental illnesses or disability; and those who live in poverty, rely on social welfare, or are unhoused.

Algorithmic policing technology also risks chilling the exercise of the fundamental freedoms of expression, peaceful assembly, and association. A growing body of empirical evidence has revealed the link between government online surveillance— including the mere prospect of such surveillance—and chilling effects on the freedom of expression.[15] Substantial chilling effects that may be caused by government surveillance include individuals being less likely to engage in certain legal activities or being more likely to exercise greater caution when they engage in such activities, including with respect to online speech, online search, and sharing personally created content on social media.[16]

The use of algorithmic social media mining tools to monitor online conversations about or among targeted subjects increases the risk that individuals will engage in self-censorship if they know or suspect that their speech is being monitored by government agencies. Similarly, individuals may avoid freely exercising their freedom of association if police algorithms are used to track social networks and group affiliations, or even if individuals only suspect that the police may be tracking such information. Such chilling effects may impact

[15] See Jonathon W Penney, "Internet surveillance, regulation, and chilling effects online: a comparative case study" (2017), 6:2 *Internet Policy Review* 22; Alex Marthews and Catherine E Tucker, "The Impact of Online Surveillance on Behavior" in David Gray and Stephen E Henderson, eds, *The Cambridge Handbook of Surveillance Law* (Cambridge, Cambridge University Press, 2017), at 437; and Margot E Kaminski and Shane Witnov, "The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech" (1 January 2015) 49 *University of Richmond Law Review*.

[16] Jonathon W Penney, "Internet surveillance, regulation, and chilling effects online: a comparative case study" (2017) 6:2 *Internet Policy Review* 22.

marginalized communities acutely. These communities include those who have been subjected to disproportionate surveillance by police services and other government agencies or who have reason to distrust Canadian law enforcement.

Part 3. Priority imperatives within the IPC's mandate to contribute to a comprehensive and effective system of independent oversight concerning law enforcement's use of algorithmic policing technology

In *To Surveil and Predict*, the Citizen Lab and IHRP identified twenty recommendations that we consider to be necessary to ensure that law enforcement agencies and governments uphold constitutional and human rights whenever they consider developing or adopting algorithmic policing technologies. These recommendations were also intended to be considered and applied retroactively to algorithmic policing technologies that have been developed, adopted, or otherwise already put into use by Canadian law enforcement.

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.[17] 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 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.

[17] 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.

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.

With much needed initiatives such as modernization of federal and provincial legislation still outstanding, it becomes that much more important that the IPC play a prominent role within the existing system of independent oversight in Ontario for law enforcement authorities. The remainder of this section will raise three specific issues and related recommendations for the IPC as it defines its mandate and strategic priorities for the next five years: i) proactive oversight to facilitate public disclosure and fact-finding regarding uses of algorithmic policing technologies in Ontario; ii) inter- and intra-governmental consultation in the reform and development of regulations; and, iii) oversight, audit, and review of law enforcement authorities' policies and discretionary decision-making in Ontario concerning the collection, use, and retention of personal biometric information.

i. Proactive oversight of law enforcement authorities to ensure fulsome disclosure is made to the public regarding the extent to which law enforcement authorities are using, procuring, or experimenting with algorithmic policing technology in Ontario

One of the short-term imperatives identified in *To Surveil and Predict* is that 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 in order to enable democratic dialogue and meaningful accountability and oversight. To this end, **the IPC should consult with law enforcement authorities and assist as needed in facilitating disclosure of the urgent information that is required with regards to the use of algorithmic policing technology in Ontario. Furthermore, the IPC should also act as a proactive and independent oversight body by relying on review, audit, and investigatory aspects of the IPC's mandate**. In doing so, the IPC can fulfill a critical fact-finding role in circumstances where voluntary disclosure by law enforcement authorities is otherwise deficient. This should include review and/or audit of law enforcement practices in Ontario in regards to any subsisting claims of secrecy surrounding undisclosed electronic surveillance methods.[18]

[18] *To Surveil and Predict*, *supra* at p. 67. By analogy, the Supreme Court of Canada has cautioned that in proceedings under the *Immigration and Refugee Protection Act*, "[t]he judge must be vigilant and skeptical with respect to the Minister's claims of confidentiality. Courts have commented on the government's tendency to exaggerate claims of national security confidentiality": *Canada (Citizenship and Immigration) v. Harkat*, 2014 SCC 37 at para 63.

Prioritizing the IPC's fact-finding functions within its mandate is 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. At present, without support from independent oversight bodies (e.g., privacy and human rights commissioners), the burden of unveiling electronic surveillance practices by law enforcement will too often fall on the shoulders of defendants in the criminal justice system. Allocating the burden of revealing and challenging potential rights-infringing uses of experimental technologies to individuals is unworkable, inequitable, and endangers the integrity of the justice system due to the tremendous individual and societal harms associated with wrongful convictions and unchecked human rights violations. These dangers are acute at present in Ontario'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 have led to a colloquial description of the justice system as a "guilty-plea-machine." For example, 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 and elsewhere: "factually innocent persons in Canada have sometimes, for a variety of reasons, pleaded guilty to crimes they did not commit."[19] 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.[20] 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."[21] 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.[22] Lack of legal aid funding has contributed to false guilty pleas

[19] 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>.
[20] *Ibid* at 179-180.
[21] Angela Bressan & Kyle Coady, "Guilty pleas among Indigenous people in Canada" (2017) at 9 <http://publications.gc.ca/site/eng/9.851369/publication.html>.
[22] *Ibid* at 6.

from those with socio-economic disadvantage.[23] The problem of false guilty pleas is further informed by disproportionate denials of bail and by the fact that the Canadian 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.[24]

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 rights violations. For example, in *To Surveil and Predict*, the report uncovered information suggesting that a particular form of controversial and (in all likelihood) unconstitutional surveillance practice has been in use and unchecked for approximately 10 years in Ontario without courts having an opportunity to rule on the legality of the practice. Our report revealed that the Ontario Provincial Police and Waterloo Regional Police Service (WRPS) appear to be unlawfully intercepting private communications in online private chat rooms through reliance on a form of social media surveillance technology known as the ICAC Child On-line Protection System (ICACCOPS). The ICACCOPS software is a technology that was designed by the OPP that is used to scan, scrape, and store the contents of online chat room conversations into a searchable database that is accessible to law enforcement authorities. The technology also reportedly enables law enforcement authorities to gain access to particularly private chat conversations, such as chat conversations involving only two participants (or a very small number of participants), or chat rooms that are password-protected. In at least one criminal case that was before the courts in Ontario (where the use of the ICACCOPS technology by the OPP and the WRPS ultimately became known), the Court became aware that this surveillance technology was

[23] 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>.

[24] 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>.

used by the WRPS on a warrantless basis. The Crown prosecutor reportedly conceded that the investigative technique did constitute an "interception" within the meaning of *Criminal Code* provisions that relate to intercepting private communications, though the Crown planned to argue that prior judicial authorization might not be required on the theory that it is open source material.[25] The case was discontinued by the Crown at a later date, so did not result in further litigation or any judicial decisions on that point of law.

After the Citizen Lab and IHRP's report was published in September 2020, the WRPS responded to media inquiries about the matter by advising that they began using this technology approximately 10 years ago, and that the police service plans to continue using the technology. It is still not understood why the WRPS considered itself to have the legal authority to conduct this form of warrantless surveillance. It is concerning that the automated nature of the surveillance technique tends to suggest that untold numbers of individuals have had their private conversations intercepted, monitored, and/or collected through this technique. The Citizen Lab is not aware of any instance where disclosure of the ICACCOPS technology was previously made to the public, or in a case that resulted in any judicial decision on the legality of the technique.

Given this context 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 in Ontario. Information can assist policymakers and justice-system participants (including courts, prosecutors, and defence counsel), to have context to identify gaps in existing access to justice mechanisms, and to support and enhance their respective roles. The IPC is well-situated to perform this important function.

ii. Consultation and collaboration in a multi-governmental approach to the regulation of algorithmic policing technology

Throughout 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

[25] It does not appear that the Crown's position is correct that the chat room conversations are truly "open source" materials, given the tool appears to scrape even password-protected conversations, including conversations in chat rooms that may have as few as only two people in them: see *R v Mills*, 2019 SCC 22 at para 24; *R v Marakah*, 2017 SCC 59 at paras 28 and 55.

governing the use of algorithmic technologies in Canada's justice system.[26] 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. To that end, we were pleased to see that the IPC likewise recognizes the overarching need for modernization of privacy legislation in Ontario, as reflected in its recent submission to the Ministry of Government and Consumer Services in 2020.[27] **The Citizen Lab recommends that the IPC should continue to play an ongoing role consulting and collaborating with law enforcement agencies and federal, provincial, and municipal government entities in the development and implementation of much needed legislative and regulatory reform.**

In particular, Recommendation 14 set out in *To Surveil and Predict* is a priority recommendation to provincial governments to enact Ministerial directives regarding the use and procurement of algorithmic policing technologies. By way of example, these directives should include 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.

As an independent body with important subject-matter expertise in the privacy impacts of digital technologies, the IPC should provide contributions to the development of ministerial directives in Ontario in regards to algorithmic policing technology. The IPC is well-situated to contribute to this objective by consulting with members of government and providing expert input towards the establishment of such directives. For example, as noted, Ontario presently lacks a regulatory framework that mandates the completion of algorithmic impact assessments prior to the development or use of any algorithmic policing technology. Algorithmic accountability experts in the United States have proposed that governments and public agencies use algorithmic impact assessments (AIAs) to facilitate

[26] See *To Surveil and Predict*, Part 6, Recommendations 1, 3, 4, 5, 7, 9, 14, and 15.
[27] Information and Privacy Commissioner of Ontario, Submission to the Ministry of Government and Consumer Services re: *Ontario Private Sector Privacy Reform* Discussion Paper, October 16, 2020, <https://www.ipc.on.ca/wp-content/uploads/2020/12/ipc-strategic-priority-setting-consultation.pdf>.

transparency, accountability, and human rights compliance when deploying algorithmic technologies.[28] Incorporating an AIA requirement early in the process of considering any algorithmic policing technology provides policy-makers with a framework to think through—and demonstrate to the public and independent experts—the potential consequences of using such a technology. This framework would also provide opportunity for policymakers to design appropriate mechanisms for oversight and redress in the event the technology is still deployed after completing the AIA. A properly done AIA would include meaningful public consultation that allows impacted communities, external researchers, human rights experts, and civil society to understand how technologies are being used, to identify potential issues, and to provide feedback or recommendations to relevant authorities,[29] and to challenge the proposed or continued use of a technology where it risks infringing upon constitutional or human rights.[30]

On April 1, 2019, the Treasury Board of Canada Secretariat ("Treasury Board") implemented the binding Directive on Automated Decision-Making ("the Directive"). Among other requirements such as system testing before deployment, the Directive requires federal government departments to conduct a prescribed AIA in the form of a questionnaire prior to putting into "production" (i.e., deploying outside of an internal test environment) any automated decision-making technology that is intended to supplement or replace the judgment of human decision-makers. It must be noted that the Treasury Board's Directive does not include a specific focus on the use of algorithmic technology in the criminal justice system, thus it may lack considerations appropriate to that context. The Directive also does not apply outside of federal institutions, yet many algorithmic policing technologies are adopted and implemented on a provincial or municipal level. Notwithstanding, at present, to the extent that provincial governments may consider adopting a regulatory framework concerning algorithmic technologies, there is a risk that the Treasury Board's Directive is too quickly adopted as a model for an AIA in the criminal law context.

In *To Surveil and Predict*, we identify serious deficiencies in the impact assessment template adopted by the Treasury Board that warrant careful attention and scrutiny before

[28] See Andrew D Selbst, "Disparate Impact in Big Data Policing" (2017) 52 Georgia Law Review 109; and Dillon Reisman, Jason Schultz, Kate Crawford & Meredith Whittaker, "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability" (April 2018) AI Now Institute.
[29] Andrew D Selbst, "Disparate Impact in Big Data Policing" (2017) 52 *Georgia Law Review* 109 at 178-179.
[30] Dillon Reisman, Jason Schultz, Kate Crawford, and Meredith Whittaker, "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability", AI Now (April 2018), <https://ainowinstitute.org/aiareport2018.pdf> at 5.

transplanting that model to the criminal justice setting.[31] While the questionnaire in the Treasury Board's Directive may provide a helpful preliminary internal assessment tool to test ideas before investing further resources in them, the tool in its current form is unlikely to fulfill the function of what has generally been understood to constitute a meaningful AIA, such as that proposed by Andrew Selbst and the AI Now Institute.[32] Any AIA adopted in Canada should follow the latter model, which would require more of government agencies or law enforcement authorities who wish to use algorithmic policing technologies on members of the public. **The Citizen Lab recommends that the IPC consult with the Government of Ontario in the enactment of its own directives (including an AIA requirement), with robust transparency, accountability, and oversight mechanisms**.

iii. Oversight, audit, and review of law enforcement authorities' policies and discretionary decision-making in Ontario concerning the collection and retention of personal biometric information

The collection and retention of personal information, such as fingerprints, mug shots, and DNA, by law enforcement authorities is protected by section 8 of the *Charter* and privacy legislation. However, individual police services have differing policies with respect to the retention or destruction of biometric data (e.g., fingerprints, mug-shot photos) after an individual's court case comes to a conclusion. In most cases, destruction 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.

Similarly, the collection and retention practices of facial images by law enforcement authorities is not an area that has historically been the target of focused regulation and oversight. When considering the privacy implications of facial recognition technology, two components of the systems must be evaluated: the algorithm that processes images and the image database. The creation of image databases carries privacy ramifications as it involves the collection and retention of personal information from individuals, and due to the

[31] For more details, see *To Surveil and Predict*, "In Focus #8: Algorithmic Impact Assessments", in Section 5.6.3. Concluding Comments: Algorithmic Policing Technology and Due Process.
[32] Dillon Reisman, Jason Schultz, Kate Crawford, and Meredith Whittaker, "Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability", AI Now (April 2018), <https://ainowinstitute.org/aiareport2018.pdf>; Andrew D Selbst, "Disparate Impact in Big Data Policing" (2017) 52 *Georgia Law Review* 109.

emergence of new facial recognition technology, the privacy interests associated with facial images are heightened. Facial recognition systems raise new questions, and re-emphasize older questions: Who should be permitted to put up video cameras and for what purposes? When should law enforcement be required to obtain prior judicial authorization before collecting images, such as from private companies and online platforms? Are the existing practices surrounding retention of images that were previously collected by law enforcement authorities appropriate and sufficient?

Police mug-shots databases can serve to focus the aforementioned questions. Mug-shot photographs are obtained through police arrest powers,[33] and law enforcement authorities are even authorized to use force if it is needed to obtain the photograph.[34] It is not a consent-driven process. Multiple law enforcement agencies in Canada report using (or are planning to use) facial recognition technology against their mug-shot databases. However, mug-shot databases can contain photos of individuals who have never been charged with a criminal offence, who have had their charges withdrawn, or who have been found innocent of allegations. Individuals have a constitutionally protected right to privacy in relation to their fingerprints and mug-shot images. In particular, the unauthorized retention of images is unconstitutional, but judicial guidance (usually obtained from court case litigation) is sparse and largely out of date in this area given technological developments have rapidly increased the privacy interests that are at stake in biometric information such as DNA and facial images. [35] In practice, however, each police service has its own internal policies with respect to the destruction of biometric data, and those policies typically entail a discretionary, request-based, or even fee-based process.[36]

Similar concerns exist in regards to the need for heightened and modernized regulations surrounding the collection, use, and retention of DNA information by law enforcement and forensic laboratories. This includes a need for transparency and clear limits surrounding the relationship between law enforcement authorities and private sector companies offering AI-based forensic services or genealogical tracing. Greater public access to information is required to enable independent review of the use of probabilistic genotyping technology in

[33] *Identification of Criminals Act*, RSC, 1985, c I-1.
[34] *Identification of Criminals Act*, RSC, 1985, c I-1, at s 2(2).
[35] *R v Strickland*, 2017 BCPC 1, and 2017 BCPC 211; *R v Dore*, [2002] OJ No 2845 at paras 64-71 (CA).
[36] 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>.

Ontario,[37] including publication of the Centre for Forensic Studies' validation study of the use of a privately-developed AI-based tool (called STRmix), that is used to conduct probabilistic genotyping for the purposes of criminal investigations and prosecutions. Given the above mentioned access to justice created by imbalances of power, resources, and knowledge between individual litigants and AI vendors and developers, independent academic researchers and human rights watchdogs must have public access to full information regarding the circumstances in which biometric information is being used in AI-generated forensic methods for the purposes of criminal proceedings.

By way of historical comparison to some of these ongoing issues, prior to the enactment of the *Police Record Checks Reform Act* (PRCRA),[38] 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.[39] **The Citizen Lab recommends that the IPC direct its oversight, review, and audit powers towards the prevention of similarly unjustified human rights impacts caused by the unjustified collection, use, and retention of personal and biometric information by law enforcement agencies**. Given the emerging range of policing technologies that may continue to make new uses of personal and biometric information, the need for legislative review and reform (including an expansion of the regulatory model set out in the PRCRA to biometric information) is significant. In the meantime, with the existing prevalence of discretionary authority exercised by law enforcement authorities in this area, there is a pressing need to prioritize the IPC's mandate in the review of policies and practices surrounding personal and biometric information.

Conclusion

Ontarians are increasingly concerned about their privacy, and in how law enforcement authorities (and adjacent private companies) collect, retain, process, and disclose their personal information. Unfortunately, successive governments have failed to table, and pass, meaningful and comprehensive privacy reform over the past decade. The Ontario

[37] Probabilistic genotyping is the use of algorithms to analyze trace or degraded DNA samples, or complex DNA mixtures involving multiple human contributors.
[38] 2015, S.O. 2015, c. 30.
[39] No doubt, continued vigilance in the oversight of law enforcement authorities' compliance with the PRCRA is crucial given continued on-the-ground experiences within the defence bar representing clients who have had continued adverse impacts caused by unjustified disclosures on criminal record checks in Ontario.

government now has the opportunity to assess what it can do to better protect the interests of its residents. The points raised above are neither exhaustive nor comprehensively explored here, but instead are issues that emerged in the course of our work that warrant flagging for the Information and Privacy Commissioner's attention as it charts its strategic course for the next five years. The relevant provincial ministries and the IPC should work with other provincial privacy commissioners and the federal privacy commissioner in a coordinated effort to establish robust oversight and accountability measures to protect the privacy rights of those subjected to algorithmic policing technologies.

We appreciate the efforts that are being undertaken through the IPC's strategic priority setting and consultation process, and the attention being paid to the issues identified in *To Surveil and Predict*. The Citizen Lab looks forward to seeing the consultation unfold, and would be pleased to discuss our recommendations in more depth as the consultation progresses, at the IPC's convenience.

Thank you for this opportunity to comment.

Signed:

Kate Robertson, lawyer at Markson Law in Toronto and Research Fellow at the Citizen Lab

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.