# TO SURVEIL AND PREDICT

## A HUMAN RIGHTS ANALYSIS OF ALGORITHMIC POLICING IN CANADA


THECITIZENLAB

UNIVERSITY OF TORONTO
FACULTY OF LAW

INTERNATIONAL
HUMAN RIGHTS
PROGRAM

This publication is the result of an investigation by the University of Toronto's International Human Rights Program (IHRP) at the Faculty of Law and the Citizen Lab at the Munk School of Global Affairs & Public Policy.

**Authors: Kate Robertson, Cynthia Khoo, and Yolanda Song**
**Research Principals: Yolanda Song and Cynthia Khoo**
**Design and Illustrations: Ryookyung Kim**

# Copyright



Document Version: 1.0



Electronic version first published by the International Human Rights Program and the Citizen Lab in September, 2020. This work can be accessed through **https://ihrp.law.utoronto.ca/** and **https://citizenlab.ca**.

# Acknowledgements

The International Human Rights Program and the Citizen Lab wish to express their sincere gratitude for the support from many people who made this work possible.

This report was researched and written by **Kate Robertson**, criminal defence lawyer and Citizen Lab research fellow, **Cynthia Khoo**, Citizen Lab research fellow and technology and human rights lawyer, and **Yolanda Song**, lawyer at Stevenson Whelton LLP and *pro bono* research associate at the IHRP.

Primary data collection governed by the research protocol for this report was carried out by **Yolanda Song** and **Cynthia Khoo**.

This report was undertaken under the supervision of Professor **Ronald J. Deibert**.

The report was reviewed by **Ronald J. Deibert**, Professor of Political Science and Director of the Citizen Lab; **Christopher Parsons**, Senior Research Associate at the Citizen Lab; **Petra Molnar**, acting Director of the IHRP; and **Samer Muscati**, former Director of the IHRP.

The authors of this report are grateful to have received further detailed input, guidance, and support from **Christopher Parsons**.

The authors owe a significant debt of gratitude for, and deeply appreciate, the invaluable insights and advice from the following external reviewers (presented alphabetically by last name): **Vincent Chiao**, Associate Professor at the University of Toronto Faculty of Law; **Lex Gill**, Associate at Trudel Johnston & Lespérance and Research Fellow at the Citizen Lab; **Tamir Israel**, Staff Lawyer at Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC) at the University of Ottawa, Faculty of Law; **Emily Lam**, Partner, Kastner Law; **Brenda McPhail**, Director of the Privacy, Technology & Surveillance Project at the Canadian Civil Liberties Association; **Noa Mendelsohn Aviv**, Director of the Equality Program at the Canadian Civil Liberties Association; **Jill Presser**, Principal, Presser Barristers, and Osgoode Hall Law School, Adjunct Professor; **Rashida Richardson**, Director of Policy Research, AI Now Institute at New York University; **Teresa Scassa**, Professor and Canada Research Chair in Information Law and Policy at the University of Ottawa, Faculty of Law; and **Valerie Steeves**, Professor at the University of Ottawa Faculty of Social Sciences, Department of Criminology.

This report was copy-edited by **Joyce Parsons**, Principal of Stone Pillars Editing and Consulting, and fact-checked by **Mashoka Maimona**, a law student at the University of Toronto.

The cover art and design for the report was completed by **Ryookyung Kim**.

The authors would particularly like to thank University of Toronto law students **Julie Lowenstein** and **Solomon McKenzie** for their valuable research assistance throughout this project, and they are grateful to law student **India Annamanthadoo** for her contributions as well.

The authors further extend gratitude to the numerous subject matter specialists and expert stakeholders who provided their insight, feedback, and time in the development of this report through informal consultations with the authors and formal research interviews. The authors are also greatly appreciative of the participants of the March 2019 symposium, "Automated Decision-Making in the Criminal Justice System," co-hosted by the Law Commission of Ontario, the Citizen Lab, the IHRP, and the Criminal Lawyers' Association, for their engagement and views on the issues raised in this report.

The Citizen Lab would like to thank the following funders for supporting this research: the John D. and Catherine T. MacArthur Foundation, the Sigrid Rausing Trust, the Ford Foundation, and the Oak Foundation. This research was also supported in part by a grant from the Open Society Foundation.

The International Human Rights Program (IHRP) would like to thank the Law Foundation of Ontario for supporting this research.

# About the Authors

**Kate Roberson** is a criminal defence lawyer at Markson Law in Toronto and a Citizen Lab Research Fellow. Her criminal defence practice includes both trial and appellate work, focusing on a range of criminal law cases, including white-collar crime, sexual offences, and computer-based investigations and crime. She previously acted as a provincial Crown prosecutor in Ontario and as a Law Clerk at the Supreme Court of Canada. She holds a J.D from the University of Toronto, Faculty of Law.

**Cynthia Khoo** is a Research Fellow at the Citizen Lab and a technology and human rights lawyer. She holds an LL.M. (Concentration in Law and Technology) from the University of Ottawa and interned as a research student and junior counsel at the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic. Her work spans across key areas of digital rights law and policy, including privacy, surveillance, intermediary liability, freedom of expression, equality, and technology-facilitated abuse.

**Yolanda Song** is a civil litigation lawyer at Stevenson Whelton LLP in Toronto. Her practice includes government litigation and general administrative and constitutional law. Yolanda worked as the William Graham Research Fellow at the International Human Rights Program at the University of Toronto, Faculty of Law, and she continues to work as a *pro bono* research associate for the IHRP. She holds a J.D. from the University of Toronto, Faculty of Law.

# About the International Human Rights Program

The International Human Rights Program (IHRP) at the University of Toronto Faculty of Law addresses the most pressing human rights issues through two avenues: The Program shines a light on egregious human rights abuses through reports, publications, and public outreach activities, and offers students unparalleled opportunities to refine their legal research and advocacy skills through legal clinic projects and global fellowships. The IHRP's fundamental priority is impact: The Program strives to

equip students and recent graduates with the skills, the knowledge, and the professional network to become effective human rights advocates. The Program also seeks to address human rights violations in Canada and abroad by engaging in comprehensive research and advocacy that aims to reform law, policy, and practice.

# About the Citizen Lab

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security. The Citizen Lab uses a "mixed methods" approach to research, combining practices from political science, law, computer science, and area studies. Our research includes: 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 relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

# Corrections and Questions

Please send all questions and corrections to the authors directly at:
**kate@citizenlab.ca**
**cynthia@citizenlab.ca**
**yolanda.song@utoronto.ca**

# Suggested Citation

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.

# Table of Contents

# Table of Contents

# Table of Contents

# List of Acronyms

| | |
|---|---|
| **AI** | Artificial Intelligence |
| **AIA** | Algorithmic Impact Assessment |
| **ALPR** | Automated Licence Plate Reader |
| **CCTV** | Closed-Circuit Television |
| **COMPAS** | Correctional Offender Management Profiling for Alternative Sanctions |
| **CPIC** | Canadian Police Information Centre |
| **CPD** | Chicago Police Department |
| **CPS** | Calgary Police Service |
| **CRIME** | Consolidated Records and Intelligence Mining Environment (Vancouver, BC) |
| **CSC** | Correctional Service Canada |
| **DAS** | Domain Awareness System (New York City, NY) |
| **DRN** | Digital Recognition Network |
| **DTES** | Downtown Eastside (Vancouver, BC) |
| **EPS** | Edmonton Police Service |
| **FAT(E)** | Fairness, Accountability, Transparency (and Ethics) |
| **FNDGI** | First Nations Data Governance Initiative |
| **FOI** | Freedom of Information |
| **GDPR** | General Data Protection Regulation (European Union) |
| **GeoDASH** | Geographic Data Analysis and Statistics Hub (Vancouver, BC) |
| **GeoDASH APS** | GeoDASH Algorithmic Policing System (Vancouver, BC) |
| **GPS** | Global Positioning System |
| **HART** | Harm Assessment Risk Tool (Durham, United Kingdom) |
| **HRIA** | Human Rights Impact Assessment |
| **IACHR** | Inter-American Commission on Human Rights |
| **ICCPR** | International Covenant on Civil and Political Rights |
| **IMSI** | International Mobile Subscriber Identity |
| **LAPD** | Los Angeles Police Department |
| **LASER** | Los Angeles' Strategic Extraction and Restoration |
| **LSI-OR** | Level Service Inventory - Ontario Revised |
| **ML** | Machine Learning |
| **OHCHR** | Office of the Commissioner of Human Rights (United Nations) |
| **OPSOC** | Ottawa Police Strategic Operations Centre |
| **PIA** | Privacy Impact Assessment |
| **PIPEDA** | *Personal Information Protection and Electronic Documents Act* |
| **POI** | Person of Interest |
| **PRIME-BC** | Police Records Information Management Environment - British Columbia |
| **RCMP** | Royal Canadian Mounted Police |
| **RMS** | Records Management System |
| **RTD** | Risk-driven Tracking Database |

# List of Acronyms

| | |
|---|---|
| **SNA** | Social Network Analysis |
| **SPPAL** | Saskatchewan Police Predictive Analytics Lab |
| **SPS** | Saskatoon Police Service |
| **SPSS** | Statistical Package for the Social Sciences |
| **SSL** | Strategic Subjects List (Chicago, IL) |
| **TPS** | Toronto Police Service |
| **VPD** | Vancouver Police Department |

# Executive Summary

This report examines algorithmic technologies that are designed for use in criminal law enforcement systems. **Algorithmic policing** is an area of technological development that, in theory, is designed to enable law enforcement agencies to either automate surveillance or to draw inferences through the use of mass data processing in the hopes of predicting potential criminal activity. The latter type of technology and the policing methods built upon it are often referred to as **predictive policing**. Algorithmic policing methods often rely on the aggregation and analysis of massive volumes of data, such as personal information, communications data, biometric data, geolocation data, images, social media content, and policing data (such as statistics based on police arrests or criminal records).

In order to guide public dialogue and the development of law and policy in Canada, the report focuses on the human rights and constitutional law implications of the use of algorithmic policing technologies by law enforcement authorities. This report first outlines the methodology and scope of analysis in Part 1. In Part 2, the report provides critical social and historical contexts regarding the criminal justice system in Canada, including issues regarding systemic discrimination in the criminal justice system and bias in policing data sets. This social and historical context is important to understand how algorithmic policing technologies present heightened risks of harm to civil liberties and related concerns under human rights and constitutional law for certain individuals and communities. The use of police-generated data sets that are affected by systemic 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. Part 3 of the report then provides a few conceptual building blocks to situate the discussion surrounding algorithmic policing technology, and it outlines how algorithmic policing technology differs from traditional policing methods.

In Part 4, the report sets out and summarizes findings on how law enforcement agencies across Canada have started to use, procure, develop, or test a variety of algorithmic policing methods. The report compiles original research with existing research to provide a comprehensive overview of what is known about the algorithmic policing landscape in Canada to date. In the overview of the use of algorithmic policing technology in Canada, the report classifies algorithmic policing technologies into the following three categories:

- **Location-focused algorithmic policing technologies** are a subset of what has generally been known as 'predictive policing' technologies. This category of algorithmic policing technologies purports to identify where and when potential criminal activity might occur. The algorithms driving these systems examine correlations in historical police data in order to attempt to make predictions about a given set of geographical areas.
- **Person-focused algorithmic policing technologies** are also a subset of predictive policing technologies. Person-focused algorithmic policing technologies rely on 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.

- **Algorithmic surveillance policing technologies**, as termed in this report, do not inherently include any predictive element and are thus distinguished from the two categories above (location-focused and person-focused algorithmic policing). Rather, algorithmic surveillance technologies provide police services with sophisticated, but general, surveillance and monitoring functions. These technologies automate the systematic collection and processing of data (such as data collected online or images taken from physical outdoor spaces). Some of these technologies (such as facial recognition technology that processes photos from mug-shot databases) may process data that is already stored in law enforcement police files in a new way. For ease of reference, this set of technologies will be referred to as simply **algorithmic surveillance technologies** throughout the rest of this report. The term should be understood to be confined to the context of policing (thus excluding other forms of algorithmic surveillance technologies that are more closely tied to other contexts, such as tax compliance or surveilling recipients of social welfare).

The primary research findings of this report show that technologies have been procured, developed, or used in Canada in all three categories. For example, at least two agencies, the Vancouver Police Department and the Saskatoon Police Service, have confirmed that they are using or are developing 'predictive' algorithmic technologies for the purposes of guiding police action and intervention. Other police services, such as in Calgary and Toronto, have acquired technologies that include algorithmic policing capabilities or that jurisdictions outside of Canada have leveraged to build predictive policing systems. The Calgary Police Service engages in algorithmic social network analysis, which is a form of technology that may also be deployed by law enforcement to engage in person-focused algorithmic policing. Numerous law enforcement agencies across the country also now rely on a range of other algorithmic surveillance technologies (e.g., automated licence plate readers, facial recognition, and social media surveillance algorithms), or they are developing or considering adopting such technologies. This report also uncovers information suggesting that the Ontario Provincial Police and Waterloo Regional Police Service may be unlawfully intercepting private communications in online private chat rooms through reliance on an algorithmic social media surveillance technology known as the ICAC Child On-line Protection System (ICACCOPS). Other police services throughout Canada may also be using or developing additional predictive policing or algorithmic surveillance technologies outside of public awareness. Many of the freedom of information (FOI) requests submitted for this report were met with responses from law enforcement authorities that claimed privilege as justification for non-disclosure; in other cases, law enforcement agencies did not provide any records in response to the submitted FOI request, or requested exorbitant fees in order to process the request.

Building on the findings about the current state of algorithmic policing in Canada, Part 5 of the report presents a human rights and constitutional law analysis of the potential use of algorithmic policing technologies. The legal analysis applies established legal principles to these technologies and

demonstrates that their use by law enforcement agencies has the potential to violate fundamental human rights and freedoms that are protected under the *Canadian Charter of Rights and Freedoms* ("the *Charter*") and international human rights law. Specifically, the authors analyze the potential impacts of algorithmic policing technologies on the following rights: the right to privacy; the right to freedoms of expression, peaceful assembly, and association; the right to equality and freedom from discrimination; the right to liberty and to be free from arbitrary detention; the right to due process; and the right to a remedy. The major findings of this analysis are presented as follows:

- **Implications for the Right to Privacy and the Right to Freedom of Expression, Peaceful Assembly, and Association:** The increasing use of algorithmic surveillance technologies in Canada threatens privacy and the fundamental freedoms of expression, peaceful assembly, and association that are protected under the *Charter* and international human rights law. The advanced capabilities and heightened data requirements of algorithmic policing technologies introduces new threats to privacy and these fundamental freedoms, such as in the repurposing of historic police data, constitutionally questionable data sharing arrangements, or in algorithmically surveilling public gatherings or online expression, raising significant risks of violations. The Canadian legal system currently lacks sufficiently clear and robust safeguards to ensure that use of algorithmic surveillance methods—if any—occurs within constitutional boundaries and is subject to necessary regulatory, judicial, and legislative oversight mechanisms. Given the potential damage that the unrestricted use of algorithmic surveillance by law enforcement may cause to fundamental freedoms and a free society, the use of such technology in the absence of oversight and compliance with limits defined by necessity and proportionality is unjustified.
- **Implications for the Right to Equality and Freedom from Discrimination:** Systemic racism in the Canadian criminal justice system must inform any analysis of algorithmic policing, particularly its impacts on marginalized communities. The seemingly 'neutral' application of algorithmic policing tools masks the reality that they can disproportionately impact marginalized communities in a protected category under equality law (i.e., communities based on characteristics such as race, ethnicity, sexual orientation, or disability). The social and historical context of systemic discrimination influences the reliability of data sets that are already held by law enforcement authorities (such as data about arrests and criminal records). Numerous inaccuracies, biases, and other sources of unreliability are present in most of the common sources of police data in Canada. As a result, drawing unbiased and reliable inferences based on historic police data is, in all likelihood, impossible. Extreme caution must be exercised before law enforcement authorities are permitted, if at all, to use algorithmic policing technologies that process mass police data sets. Otherwise, these technologies may exacerbate the already unconstitutional and devastating impact of systemic targeting of marginalized communities.

- **Implications for the Right to Liberty and to Freedom from Arbitrary Detention:** It is incompatible with constitutional and human rights law to rely on algorithmic forecasting to justify interfering with an individual's liberty. By definition, algorithmic policing methods tend to produce generalized inferences. Under human rights law and the *Charter*, loss of liberty (such as detention, arrest, denial of bail, and punishment through sentencing) cannot be justified based on generalized or stereotypical assumptions, such as suspicion based on beliefs about an ethnic group or on the location where an individual was found. Reliance on algorithmic policing technologies to justify interference with liberty may violate *Charter* rights where the purported grounds for interfering with liberty are based on algorithmic predictions drawn from statistical trends, as opposed to being particularized to a specific individual. Violations may include instances where an individual would not have been detained or arrested *but* for the presence of an algorithmic prediction based on statistical trends, all other circumstances remaining the same.

In addition to these major findings, the report documents problems that are likely to arise with respect to meaningful access to justice and the rights to due process and remedy, given that impactful accountability mechanisms for algorithmic policing technology are often lacking, and in light of the systemic challenges faced by individuals and communities seeking meaningful redress for rights violations that do not result in charges in Canadian courts. The absence of much needed transparency in the Canadian algorithmic policing landscape animates many of the core recommendations in this report. The authors hope that this report provides insight into the critical need for transparency and accountability regarding what types of technologies are currently in use or under development and how these technologies are being used in practice. With clarified information regarding what is currently in use and under development, policy- and lawmakers can enable the public and the government to chart an informed path going forward.

In response to conclusions drawn from the legal analysis, the report ends with a range of recommendations for governments and law enforcement authorities with a view to developing law and oversight that would establish necessary limitations on the use of algorithmic policing technologies. Part 6 provides a list of these recommendations, each of which is accompanied by contextual information to explain the purpose of the recommendation and offer potential guidance for implementation. The recommendations are divided into **priority recommendations**, which must be implemented now, with urgency, and **ancillary recommendations**, which may be inapplicable where certain algorithmic policing technologies are banned but must be implemented if any such technologies are to be developed or adopted. The following is a condensed summary of those recommendations:

A. Priority recommendations for governments and law enforcement authorities that must be acted upon urgently in order to mitigate the likelihood of human rights and *Charter* violations associated with the use of algorithmic policing technology in Canada:

1. **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.

2. **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.

3. **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.

4. **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.

5. **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.

6. **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.

7. **Governments and law enforcement authorities must engage external expertise, including from historically marginalized communities that are disproportionately impacted by the criminal justice system**, before and when considering, developing, or adopting algorithmic policing technologies, when developing related regulation

and oversight mechanisms, as part of completing algorithmic impact assessments, and in monitoring the effects of algorithmic policing technologies that have been put into use if any.

B. Ancillary recommendations for law enforcement authorities:

1. **Law enforcement authorities should enhance police database integrity and management practices**, including strengthening the ability of individuals to verify and correct the accuracy of personal information stored in police databases.

2. **Law enforcement authorities must exercise extreme caution to prevent unconstitutional data-sharing practices** with the private sector and other non-police government actors.

3. **Law enforcement authorities should undertake the following best practices** whenever an algorithmic policing technology has been or will be adopted or put into use, with respect to that technology:

    i. Implement ongoing tracking mechanisms to monitor the potential for bias in the use of any algorithmic policing technology;

    ii. Engage external expertise ongoingly, including consulting with communities and individuals who are systemically marginalized by the criminal justice system, about the potential or demonstrated impacts of the algorithmic policing technology on them;

    iii. Formally document written policies surrounding the use of algorithmic policing technology; and

    iv. Adopt audit mechanisms within police services to reinforce and identify best practices and areas for improvement over time.

C. Ancillary recommendations for law reform and related measures by federal, provincial, territorial, and municipal governments:

1. **The federal government should reform the judicial warrant provisions of the *Criminal Code*** to specifically address the use of algorithmic policing technology by law enforcement authorities.

2. **Federal and provincial legislatures should review and modernize privacy legislation** with particular attention to reevaluating current safeguards to account for the advanced capabilities of algorithmic policing technologies and to the retention and destruction of biometric data by law enforcement authorities.

3. **The federal government should expand the Parliamentary reporting provisions under the *Criminal Code*** that currently only apply to certain electronic surveillance methods to specifically address police powers in relation to the use of algorithmic policing technology by law enforcement authorities.

4. **Governments must ensure that privacy and human rights commissioners are empowered and have sufficient resources** to initiate and conduct investigations into law enforcements' use of algorithmic policing technology.

D. Ancillary recommendations for government to enable access to justice in relation to the human rights impacts of algorithmic policing technology:

1. **Governments should make funding available for research** to develop the availability of independent expertise.

2. **Governments must ensure adequate assistance is available for low-income and unrepresented defendants** in order that they might to retain expert witnesses in criminal proceedings.

3. **Governments and law enforcement agencies must make the source code of algorithmic policing technologies publicly available** or, where appropriate, confidentially available to public bodies and independent experts for the purposes of algorithmic impact assessments, pre-procurement review, security testing, auditing, investigations, and judicial proceedings.

# 1. Overview and Background

## 1.1. Introduction

Algorithmic policing is an area of technological development that, in theory, is designed to enable law enforcement agencies to automate surveillance or to draw inferences through mass data processing in the hopes of predicting potential criminal activity. The latter type of technology and policing methods built upon it are often referred to as 'predictive policing' technology. Generally speaking, the purpose of algorithmic policing technology is to complement traditional police investigative methods and to enable law enforcement agencies to prioritize the deployment of resources in a manner that will more effectively prevent or detect crime.

The extent to which Canadian law enforcement agencies have begun to use algorithmic policing technologies is poorly understood. This report, first, sets out research findings about how law enforcement agencies in Canada have begun to use algorithmic policing technologies, and second, it examines the human rights and constitutional law implications of the use of algorithms in the Canadian criminal justice system. The use of algorithmic technologies by policing agencies is the focus of this report, but the human rights and constitutional law analysis is also applicable to algorithmic technology that may be used in other stages of the criminal justice system.

Due to the relatively limited public use of algorithmic policing technology in Canada, this report, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada," takes a forward-looking approach. In addition to analyzing algorithmic policing technologies that Canadian police services are known to be using, the authors address technologies that they consider to be on the horizon, based on findings regarding such activities known to date, statements made publicly or in research interviews by law enforcement representatives, and the implementation of algorithmic policing technologies in peer jurisdictions such as the United States and the United Kingdom.

This report contributes to public decision-making regarding the potential use of algorithmic policing technologies in Canada by considering the human rights and constitutional implications of adopting such technologies for criminal law enforcement purposes. Algorithmic policing raises issues that go beyond questions relating to whether the technology involved is useful, cost-effective, or reliable, even if such questions were not themselves difficult to answer with clarity. The vulnerability of populations who are disproportionately and significantly impacted by the criminal justice system warrants a careful approach to the adoption of new technologies (such as technologies that may influence the frequency or form of street detentions, arrests, and surveillance) that law enforcement agencies may use in ways that materially affect the lives of often already marginalized individuals. Further, state action taken in the investigation of crime must be constrained within constitutional parameters (even though law enforcement agencies often fall short of this obligation in practice).[1] As a result, it is critical that state actors and decision-makers at all levels of government and the criminal justice system critically

1 The history of criminal law litigation in Canada is replete with examples of recognized violations of constitutionally protected rights of individuals by law enforcement agencies (see, e.g., *R v Grant*, 2009 SCC 32; *R v Le*, 2019 SCC 34; *R v Evans*, [1996] 1 SCR 8; *R v Nasogaluak*, 2010 SCC 6; *R v Cole*, 2012 SCC 53).

evaluate the potential of algorithmic policing technologies to violate rights under the *Canadian Charter of Rights and Freedoms* ("the *Charter*"),[2] in order to comply with constitutional obligations as well as their obligations under international human rights law. Algorithmic policing initiatives engage a panoply of civil liberties concerns relating to due process, equality, privacy, liberty, and other fundamental freedoms such as the freedom of expression.

The Canadian government has recognized the need for a rights-centred approach to considering whether or how to integrate algorithmic technologies into public sector services. Legislative and policy developments have emerged in Canada to address the intersection between artificial intelligence and human rights, though, as of writing, none have specifically addressed algorithmic policing.[3] International institutions have also been engaging with the human rights implications of states' use of artificial intelligence.[4] At the same time, civil society and non-governmental organizations have called urgent attention to civil liberties issues relating to Fairness, Accountability, Transparency, and Ethics (referred to as FATE) that are engaged by a range of algorithmic technologies as well as the need to affirm clear limits on the uses of the technology that are necessary to uphold *Charter* and human rights.[5] Governmental initiatives in peer jurisdictions have begun to investigate or regulate algorithmic technologies in their criminal justice systems given the human rights implications at stake.[6]

2 *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution* Act, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11.

3 The most prominent initiative from the federal government has been the work of the Treasury Board of Canada Secretariat (TBSC), and includes the Directive on Automated Decision-Making, an Algorithmic Impact Assessment tool, and a white paper, "Responsible Artificial Intelligence in the Government of Canada": Government of Canada, "Directive on Automated Decision-Making" (5 February 2019) <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592>; Government of Canada, "Algorithmic Impact Assessment (AIA)" (31 May 2019) <https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/responsible-use-ai/algorithmic-impact-assessment.html>; Government of Canada, "Responsible Artificial Intelligence in the Government of Canada: Digital Disruption White Paper Series" (10 April 2018).

4 See, e.g., UN Human Rights Council, *The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights*, A/HRC/39/29 (3 Aug 2018) <https://undocs.org/A/HRC/39/29>; UN General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/73/348 (29 Aug 2018) <https://undocs.org/A/73/348>; United Nations Office of the High Commissioner of Human Rights, "Expert Seminar on Artificial Intelligence and the Right to Privacy" (May 2020) <https://www.ohchr.org/EN/Issues/DigitalAge/Pages/SeminarArtificialIntelligence.aspx>.

5 See, e.g., Montréal Declaration Responsible AI, "Montreal Declaration for a responsible development of artificial intelligence" (2018) <https://www.montrealdeclaration-responsibleai.com>; Access Now, "The Toronto Declaration: Protecting the rights to equality and non-discrimination in machine learning systems" (16 May 2018) <https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems/>. Generally, the FATE approach has been critiqued due to its propensity to focus on soft governance through ethics, as opposed to regulating hard and necessary limits: see, for example, Campolo, A, Sanflippo, M, Whittaker, M, & Crawford, K, "AI Now Report 2017" (2017), <https://ainowinstitute.org/AI_Now_2017_Report.pdf>, at p 34.

6 See e.g., United Kingdom Government, "Investigation launched into potential for bias in algorithmic decision-making in society" (20 March 2019) <https://www.gov.uk/government/news/investigation-launched-into-potential-for-bias-in-algorithmic-decision-making-in-society>; *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision* 2008/977/JHA (2016) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02016L0680-20160504>; US Executive Office of the President, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights* (May 2016) <https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf>; Adi Robertson, "A new bill would force companies to check their algorithms for bias", *The Verge* (10 April 2019) <https://www.theverge.com/2019/4/10/18304960/congress-algorithmic-accountability-act-wyden-clarke-booker-bill-introduced-house-senate>; City of New York, "Mayor de Blasio Announces First-In-Nation Task Force to Examine Automated Decision Systems Used by the City" (16 May 2018) <https://www1.nyc.gov/office-of-the-mayor/news/251-18/mayor-de-blasio-first-in-nation-task-force-examine-automated-decision-systems-used-by>; April Glaser, "San Francisco is about to be the first US city to ban police from using facial recognition tech", *Slate* (6 May 2019) <https://slate.com/technology/2019/05/san-francisco-first-city-ban-facial-recognition.html>; Andy Rosen, "Somerville moves to ban facial recognition surveillance", *The Boston Globe* (10 May 2019) <https://www.bostonglobe.com/metro/2019/05/10/somerville-moves-ban-

Against this backdrop, Canadian policy-makers and governing entities have an opportunity to lead in the development of algorithmic policing technology laws, policies, and practices that respect domestically and internationally protected human rights. Based on the findings and analysis in this report, decision-makers in Canada have an obligation to approach algorithmic policing technology with caution, by thoroughly assessing the potential human rights impacts and constitutional implications of algorithmic policing technology *before* any adoption of such by law enforcement agencies in Canada. Such assessments could enable appropriate interventions to mitigate or prevent huma rights violations and harms to individuals and communities that would otherwise be caused by the continued use or deployment of new, untested, or flawed technology.

To inform and guide public dialogue, the law, and policy-making, this report provides the public and state actors with an overview of the human rights and constitutional law implications of integrating algorithmic policing technologies into the criminal law enforcement system. The research findings and analysis in this report therefore answer two main questions:

1. **Are Canadian law enforcement agencies currently using, developing, or considering adopting algorithmic policing technologies, and, if so, what are the details of such initiatives?** The research conducted for this report found that multiple law enforcement agencies across Canada have started to use, procure, develop, or test a variety of algorithmic policing methods. These programs include using and developing 'predictive policing' technologies—one location-focused and one person-focused—and using algorithmic surveillance tools, such as facial recognition technology and social network analysis. Additionally, some law enforcement agencies have acquired tools with the capability of algorithmic policing technology, but they are not currently using that capability for lack of interest at time of writing or lack of resources to pursue such initiatives. The full research findings in answer to this question are set out in Part 4 ("Algorithmic Policing in Canada: The Current Landscape") of this report.

2. **What are the human rights and constitutional law implications of using algorithmic policing technologies, and does this use risk violating constitutional or human rights?** The legal and policy analysis conducted for this report found that the use of algorithmic policing technologies by law enforcement can raise a myriad of potential constitutional and civil liberties violations under the *Canadian Charter of Rights and Freedoms* and under international human rights law. In particular, the analysis identified a number of issues related to the use of personal data and mass data, algorithmic and systemic bias, lack of transparency, and due process concerns, pointing to a fundamental incompatibility between certain uses of algorithmic policing

---

facial-recognition-surveillance/ebhl0qcX6k14O1H78yrpiI/story.html>. These initiatives have not all been without criticism, however; see e.g., Rashida Richardson, ed, "Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force", *AI Now Institute* (December 2019) <https://ainowinstitute.org/ads-shadowreport-2019.pdf>.

technology and constitutional and human rights protections, particularly concerning rights relating to liberty, equality, and privacy. In Part 5 ("International Human Rights and *Charter* Rights Implications of Algorithmic Policing"), this report applies established legal principles in human rights and constitutional law to existing or potential uses of algorithmic policing technologies in the Canadian criminal justice system, based on the research findings in Part 4.

Parts 1-3 of this report provide background context to set the stage for the research findings and analysis in Parts 4 and 5. Section 1.2 outlines the methodology that the authors adopted in the course of researching and writing this report. Part 2 ("Social and Historical Context") provides social and historical context regarding the impact of systemic discrimination in the Canadian criminal justice system and an overview of the ways in which systemic bias can permeate police data. It is this systemic discrimination and systemic bias that informs many human rights issues that are linked to algorithmic policing. Part 3 ("What Is Algorithmic Policing?") provides an introduction to algorithmic policing, including an explanation of its key concepts and technological terms and an explanation of how algorithmic policing differs from conventional policing and surveillance methods.

## 1.2. Methodology

This report uses a mixed-methods approach to investigate the use of algorithmic policing technologies in Canada and the ways in which such technologies may raise human rights and *Charter* issues. The two core phases of research for this report—how algorithmic policing technologies are used by Canadian police services (Part 4) and a human rights and constitutional law assessment of existing or future algorithmic policing technology (Part 5)—often relied on discrete sets of methods. Broadly, these phases relied on desk research, legal and policy research, filing access-to-information and freedom-of-information (FOI) requests, informal consultations with subject matter experts, formal research interviews with a variety of expert stakeholders, and a multidisciplinary full-day symposium that included collaborative workshops. This report applies an interdisciplinary and critical intersectional lens, combining human rights, criminal law, constitutional law, technology law and policy, science and technology studies, and social sciences literature. Integrating these interdisciplinary and intersectional perspectives enables an assessment of the potential implications for vulnerable communities who may be particularly impacted by the use of algorithmic policing methods.

The remainder of this section describes the research and analysis methods in more detail.

### 1.2.1. Data Collection

Desk research drew on primary and secondary sources. Primary sources included government and police agency documents that were publicly available online, such as police service board reports, meeting minutes, procurement notices, presentation slide decks, and records from other parties' past access-to-information and freedom-of-information requests. Secondary sources included media coverage of algorithmic policing technologies and related initiatives as well as numerous legal, policy, investigative, and research reports at the cross-section of algorithms, artificial intelligence,

criminal justice, and human rights. These reports were produced by governmental bodies, non-governmental organizations, professional associations (e.g., law societies or law foundations), research institutions, and advocacy groups in Canada and similar jurisdictions such as the United States, United Kingdom, and European Union.

Access-to-information and freedom-of-information requests ("FOI requests")[7] were filed to various federal, provincial, and municipal bodies. All of the bodies were directly associated with law enforcement functions in the Canadian justice system.[8] Response rates to these requests varied. In November 2018, the authors submitted FOI requests to the following government bodies:

**Municipal Police Services**

- Calgary Police Service
- Edmonton Police Service
- Ottawa Police Service
- Saskatoon Police Service
- Toronto Police Service
- Vancouver Police Department
- Durham Regional Police Service
- Hamilton Police Service
- London Police Service
- Peel Regional Police

**Provincial Ministries**

- Alberta Ministry of Justice and Solicitor General
- British Columbia Ministry of Attorney General
- British Columbia Ministry of Public Safety & Solicitor General
- Ontario Ministry of the Attorney General
- Ontario Ministry of Community Safety and Correctional Service (renamed Ministry of the Solicitor General in 2019)
- Saskatchewan Ministry of Justice and Attorney General
- Saskatchewan Ministry of Corrections and Policing

**Federal Departments and Agencies**

- Ministry of Public Safety and Emergency Preparedness
- Department of Justice
- Canadian Security Intelligence Service
- Royal Canadian Mounted Police
- Correctional Service Canada
- Parole Board of Canada
- Public Prosecution Service of Canada

7 Federal requests for information by the public are governed by the *Access to Information Act*, RSC 1985 cA-1, while provincial and municipal requests are governed by some variant of a *Freedom of Information and Protection of Privacy Act*. For ease of reference, both forms of requests are referred to as FOI requests.

8 Other public sector agencies tasked with other governmental functions or the enforcement of other laws in Canada, which may make referrals to criminal law enforcement agencies, are beyond the scope of this report, as such agencies are engaged with a different set of public interests and legislative contexts than those engaged in the criminal justice system. This would include counter-intelligence and national security agencies, a host of regulatory agencies such as the Canada Revenue Agency and financial regulators, as well as other investigative agencies tasked with the investigation of non-criminal provincial offences.

Appendix A provides a copy of the template text used for all the initial FOI requests. Nearly every request resulted in ongoing negotiations with an assigned FOI officer or analyst. Such officers or analysts regularly sought to narrow the scope of requests, to clarify the kind of records the authors were seeking, or to seek—often exorbitant—fees for processing the request. Follow-up negotiations were pursued to address these responses where possible. Several requests received responses that asserted privilege in respect of the requested records. Obtaining records also necessitated numerous follow-up emails and phone calls, and significant time extensions were needed to fulfill the requests. In some cases, miscommunication led to the premature closing of the files, while in others, the authors would have been required to apply for fee waivers or appeal unsatisfactory responses to the relevant regulator. The authors obtained records across multiple jurisdictions and levels of government following such negotiations and payment of some of the smaller fees. Responses to these requests have been incorporated throughout the report where relevant.[9]

The authors conducted eight formal research interviews (including one joint interview) for this project, in the format of semi-structured interviews, with a total of nine individuals: five legal practitioners, human rights advocates, community service providers, and/or racial justice advocates and four law enforcement representatives across Canada. All research interviews were conducted under a research protocol approved by the University of Toronto Research Ethics Board. The responses and findings from these interviews have been integrated throughout the report with the person interviewed identified or pseudonymized according to their consent and in accordance with the adopted research ethics protocol.

Data collection through research interviews was limited to interviewing professionals and recognized experts under the project's research ethics protocol, as the authors were not in a position to responsibly engage in a full, front-line community consultative process with vulnerable individuals. However, the lawyers, human rights and racial justice advocates, and community members who were interviewed represent, work with, and are from and are embedded within their respective communities on a day-to-day basis. Additionally, they are familiar with and possess expertise regarding how the criminal justice system impacts and interacts with the circumstances and experiences of racialized and Indigenous individuals and groups in Canada.

A multidisciplinary symposium, "Automated Decision-Making in the Criminal Justice System", was co-hosted by the Law Commission of Ontario, the IHRP, the Citizen Lab, and the Criminal Lawyers' Association on March 22, 2019. The symposium followed the Chatham House Rule.[10] This symposium was a closed event that fostered candid, cross-disciplinary discussions among over 60 attendees about the challenges that arise with the use of automated decision-making tools at different stages of the criminal justice system, including policing, pretrial detention, sentencing, risk assessment, and corrections. Participants were informed of, and consented to, the discussions and workshops

9 Several of the FOI requests sent for this report in November 2018 remain outstanding as of time of writing.

10 Background materials from the symposium are available at <https://www.lco-cdo.org/wp-content/uploads/2019/03/Background-Info-Package-1.pdf>. The Chatham House Rule reads that "participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed." See Chatham House: The Royal Institute of International Affairs, "Chatham House Rule," Accessed 10 August 2018, <https://www.chathamhouse.org/chatham-house-rule>.

informing research and publications such as this report. Insights from the symposium have informed some of the analyses in this report.

### 1.2.2. Legal Analysis of Collected Data

The human rights and legal analysis in this report draws on international human rights law and Canadian human rights, criminal, and constitutional law. This report predominantly focuses on jurisprudence under the *Canadian Charter of Rights and Freedoms*. While Canadian constitutional law provides a robust framework of rights for individuals that regulate the use of police investigative powers, emerging technologies and their novel uses often pose legal issues that have not previously been the subject of constitutional litigation. As a result, this report also analyzes Canada's relevant international human rights law obligations on the basis that they inform the interpretation of *Charter* rights while also providing a parallel legal regime that imposes human rights obligations on the Canadian government. Such obligations are complementary to Canadian human rights law.

# 2. Social and Historical Context

This report is written in the broader context of issues that relate to systemic bias and discrimination in society and in the criminal justice system. Algorithmic policing technology must be situated in this context to adequately consider the technology's potential impacts and risks, particularly with respect to human and constitutional rights. Section 2.1 provides context related to governmental and judicial findings that call attention to systemic bias and racism in the criminal justice system in Canada and considers the impact of systemic discrimination on individuals and communities. Section 2.2 provides an overview of the ways in which systemic bias can permeate police data. For individuals and communities that are impacted by the criminal justice system in Canada, the adverse effects can be significant and long-lasting. If systemic biases permeate data sets that are produced in Canada's criminal justice system, these biases may become embedded in and perpetuated by algorithmic policing technology to the further detriment of individuals and communities that have been the subject of historic discrimination.

## 2.1. Criminal Justice and Systemic Discrimination in Canada

The existence of systemic bias and racism in the criminal justice system is well recognized in Canada and has had the effect of disproportionately affecting Black, Indigenous, low-income, LGBTQ, racialized, and other marginalized communities. Justice system actors, researchers, investigative journalists, government bodies, and human rights bodies have documented and called attention to over-policing and excessive incarceration of Black and Indigenous individuals in the Canadian criminal justice system.[11]

Over-policing includes disproportionate scrutiny by law enforcement of racialized and Indigenous individuals in circumstances where the individuals are found to be doing no wrong and being subjected to harsher treatment by law enforcement authorities. For example, research indicates that racialized persons may be more likely to be arrested for minor offences than non-racialized individuals, resulting in overly harsh treatment for offences that are not public safety concerns.[12] Other data shows that despite similar cannabis use across different racial groups, Black and Indigenous individuals are overrepresented in cannabis possession arrests in Canada and are more likely to be held in custody and brought to bail court as opposed to being released from the police station.[13] Such over-policing has disturbing implications and consequences, including the disproportionate stopping, questioning, and searching of racialized individuals. While such activities may find a few individuals with illegal substances or other contraband—as would be the case if non-racialized individuals were disproportionately stopped and

13 Rachel Browne, "Black and Indigenous people are overrepresented in Canada's weed arrests" (18 April 2018) *Vice* <https://www.vice.com/en_ca/article/d35eyq/black-and-indigenous-people-are-overrepresented-in-canadas-weed-arrests>; Jim Rankin & Sandro Contenta, "Toronto marijuana arrests reveal 'startling' racial divide", *Toronto Star* (6 July 2017), <https://www.thestar.com/news/insight/2017/07/06/toronto-marijuana-arrests-reveal-startling-racial-divide.html>; Alex Luscombe and Akwasi Owusu-Bempah, "Why legalization won't change racial disparities in cannabis arrests", *VICE* (19 April 2018), <https://www.vice.com/en_ca/article/gymnym/why-legalization-wont-change-racial-disparities-in-cannabis-arrests>.

searched—it also often unnecessarily and unfairly targets the vast majority who are doing no wrong, and this practice generates biased statistics about targeted groups.

The Supreme Court of Canada recognized the overrepresentation of Indigenous persons in all aspects of criminal justice processing as "a crisis in the Canadian criminal justice system ... [that] reveals a sad and pressing social problem."[14] Justice system participants and lawmakers continue to struggle with, and ostensibly work towards, redressing the effects of this historic and continuing legacy. As of January 2020, Indigenous individuals represented just 5% of the Canadian population while now, for the first time in history, they surpass 30% of the total population in federal custody.[15] As cited by the Supreme Court of Canada, Professor Michael Jackson has written that, "placed in an historical context, the prison has become for many young native people the contemporary equivalent of what the Indian residential school represented for their parents."[16] The final report of the Truth and Reconciliation Commission of Canada called on all levels of government to address the grossly disproportionate imprisonment of Indigenous people, which continues to grow.[17]

Researchers and judicial inquiries also call attention to the over-policing and racial profiling of racialized individuals, particularly members of Black and Indigenous communities.[18] In a 2018 report of the Independent Street Checks Review, Justice Michael H. Tulloch found that data from police services across Ontario indicated disproportionate rates of police stops and detentions involving Indigenous, Black, and other racialized communities, as well as youth and people from underprivileged socio-economic groups.[19] When stopping and detaining individuals on the street, police have had a controversial and long condemned[20] practice of regularly asking individuals for identification information, which is then recorded in police databases along with other information gleaned from the encounter, about

14 *R v Gladue*, [1999] 1 SCR 688 at para 64.

15 Government of Canada, Office of the Correctional Investigator, "Indigenous People in Federal Custody Surpasses 30%: Correctional Investigator Issues Statement and Challenge", News Release (21 January 2020), <https://www.oci-bec.gc.ca/cnt/comm/press/press20200121-eng.aspx>.

16 *R v Gladue*, [1999] 1 SCR 688 at para 60.

17 Truth and Reconciliation Commission of Canada, *Honouring the Truth, Reconciling for the Future: Summary of the Final Report of the Truth and Reconciliation Commission of Canada* (December 2015) <http://nctr.ca/assets/reports/Final%20Reports/Executive_Summary_English_Web.pdf>.

18 See generally, David Tanovich, *The Colour of Justice* (Toronto: Irwin Law, 2006); Ontario Human Rights Commission, *Under Suspicion: Research and consultation report on racial profiling in Ontario* (April 2017) <http://www.ohrc.on.ca/en/under-suspicion-research-and-consultation-report-racial-profiling-ontario>; Ontario Human Rights Commission, *A Collective Impact: Interim report on the inquiry into racial profiling and racial discrimination of Black persons by the Toronto Police Service* (November 2018) <http://www.ohrc.on.ca/en/public-interest-inquiry-racial-profiling-and-discrimination-toronto-police-service/collective-impact-interim-report-inquiry-racial-profiling-and-racial-discrimination-black>; LogicalOutcomes, "'This Issue Has Been with Us for Ages': A Community-Based Assessment of Police Contact Carding in 31 Division" (November 2014).

19 The Honourable Michael H. Tulloch, *Report of the Independent Street Checks Review* (2018) at page 44 <https://www.mcscs.jus.gov.on.ca/sites/default/files/content/mcscs/docs/StreetChecks.pdf>

20 "Ontario report finds carding has little to no value for law enforcement, should be sharply curtailed", *The Globe and Mail* (2 January 2019), <https://www.theglobeandmail.com/canada/article-ontario-report-finds-little-to-no-evidence-that-controversial-practice/>; The Honourable Michael H. Tulloch, *Report of the Independent Street Checks Review* (2018) at page 44 <https://www.mcscs.jus.gov.on.ca/sites/default/files/content/mcscs/docs/StreetChecks.pdf>; Ontario Human Rights Commission, "Policy on eliminating racial profiling in law enforcement" at 4.2.6.2, <http://www.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement>; Scot Wortley, *Halifax, Nova Scotia: Street Checks Report* (March 2019) <https://humanrights.novascotia.ca/streetchecks>.

the individual's location, activity, and social associations.[21] Findings of disproportionate policing of racialized communities and racial profiling have surfaced across Canada, including in Montreal,[22] Halifax,[23] Edmonton,[24] Calgary,[25] and Vancouver.[26] The *Toronto Star* reported that from 2008 to mid-2011, "the number of young black and brown males aged 15 to 24 documented in each of the city's 72 patrol zones is greater than the actual number of young men of colour living in those areas."[27] Police-civilian encounters on the street are only one example of police techniques that disproportionately impact racialized and marginalized communities. Reports have likewise highlighted other forms of state surveillance targeted at racialized, marginalized, and political communities.[28]

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

21 Identity information is also generally used to conduct CPIC searches relating to the individual in the police encounter. A CPIC search is considered a search under section 8 of the *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11, s 8; *R v Walters*, 2018 ONSC 4194, at para 125. Members of racialized, low-income, or otherwise over-policed communities who are disproportionately targeted by this practice are thus susceptible to being captured in police databases without having engaged in any wrongdoing, and their personal information is thereafter available to law enforcement agencies and other federal departments in Canada, or even in some cases law enforcement agencies in the United States. Graeme Norton, *Presumption of Guilt? The Disclosure of Non-Conviction Records in Police Background Checks*, Canadian Civil Liberties Association (May 2012) <https://ccla.org/cclanewsite/wp-content/uploads/2015/02/Presumption-of-Guilt.pdf> at 7.

22 Toula Drimonis, "Racial profiling a systemic problem for Montreal police", *National Observer* (24 April 2018), <https://www.nationalobserver.com/2018/04/24/opinion/racial-profiling-systemic-problem-montreal-police>.

23 Scot Wortley, *Halifax, Nova Scotia: Street Checks Report* (March 2019) <https://humanrights.novascotia.ca/streetchecks>.

24 Andrea Huncar, "Indigenous women nearly 10 times more likely to be street checked by Edmonton police, new data shows", *CBC News* (27 June 2017), <https://www.cbc.ca/news/canada/edmonton/street-checks-edmonton-police-aboriginal-black-carding-1.4178843>.

25 Rocky Mountain Civil Liberties Association, "Calgary Police data suggests Police Carding is Greatest in Diverse Neighbourhoods" (9 May 2016), <http://www.rmcla.ca/blog/?p=394>.

26 Globe and Mail, "Vancouver Police Department's use of carding disproportionately targets Indigenous people" (4 June 2018), <https://www.theglobeandmail.com/canada/british-columbia/article-vancouver-police-departments-use-of-carding-disproportionately/>.

27 Jim Rankin & Patty Winsa, "Known to police: Toronto police stop and document black and brown people far more than whites", *The Toronto Star* (9 March 2012) <https://www.thestar.com/news/insight/2012/03/09/known_to_police_toronto_police_stop_and_document_black_and_brown_people_far_more_than_whites.html?li_source=LI&li_medium=star_web_ymbii>.

28 Reg Whitaker, Gregory S. Kealey & Andrew Parnaby, *Secret Service: Political Policing in Canada From the Fenians to Fortress America* (Toronto: University of Toronto Press, Scholarly Publishing Division, 2012). For example, numerous reports of targeting of Muslim individuals in Canada have been uncovered. See Colton Praill, "Muslim students in Saskatchewan receiving calls from CSIS, say university students", *Global News* (20 November 2018) <https://globalnews.ca/news/4683333/muslim-students-saskatchewan-calls-csis/>; Benjamin Shiller, "Activists launch 'don't talk' campaign to denounce CSIS 'intimidation tactics'", *The Toronto Star* (30 January 2012), <https://www.thestar.com/news/canada/2012/01/30/activists_launch_dont_talk_campaign_to_denounce_csis_intimidation_tactics.html>. The RCMP have also been reported to target Indigenous rights activists: see Andrew Nikiforuk, "When Indigenous Assert Rights, Canada Sends Militarized Police", *The Tyee* (17 January 2019), <https://thetyee.ca/Analysis/2019/01/17/Indigenous-Rights-Canada-Militarized-Police/>; Miles Howe & Jeffrey Monaghan, "Strategic Incapacitation of Indigenous Dissent: Crowd Theories, Risk Management, and Settler Colonial Policing" (2018) 43:4 Canadian Journal of Sociology 325, <https://journals.library.ualberta.ca/cjs/index.php/CJS/article/view/29397/21432?fbclid=IwAR0gOWPQ6ZE6Om8Tq4u0vO1rF2ndSSfvbtjLOeM4U_B2F_YzYeqRNuipHQw>; "Snooping on First Nations activist went too far, privacy commissioner says", *CBC News* (29 May 2013), <https://www.cbc.ca/news/canada/snooping-on-first-nations-activist-went-too-far-privacy-commissioner-says-1.1364426>. In 2017, investigative reporting by the *Toronto Star* also brought to light the RCMP's controversial use of a racial profiling screening tool at a border crossing between the United States and Canada. This practice reportedly ended a controversial practice that was reportedly brought to an end after it was brought to the public's attention: Michelle Shephard, "RCMP will redact more than 5,000 records collected using questionnaire targeting Muslim asylum seekers", *The Toronto Star* (27 November 2017) <https://www.thestar.com/news/canada/2017/11/27/rcmp-will-redact-more-than-5000-records-collected-using-questionnaire-targeting-muslim-asylum-seekers.html>.

can be significant and long-lasting. The effects include heightened recidivism rates[29] and negative effects on health, poverty, and human dignity,[30] 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. 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 (and their communities and families) who are the target of ongoing scrutiny.[31] 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."[32] 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."[33] 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.

## 2.2. Bias and Inaccuracies in Police Data

Algorithmic policing technologies[34] routinely depend on processing massive quantities of data from a wide-ranging set of sources. This data is used to train algorithms or as input data to generate forecasts about people or locations, forecasts which law enforcement authorities then act upon. Data sources might include criminal survey statistics, social media posts, geolocation data, crisis centre call logs,

29 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>.

30 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>.

31 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/>.

32 *R v Le*, 2019 SCC 34 at para 95.

33 *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>.

34 Algorithmic policing technologies will be defined and introduced in greater detail in Part 3 ("What is 'Algorithmic Policing'?").

hospital injury data, or criminal activity data collected by non-police security personnel such as transit, campus, or mall cops, or private security.[35]

For the purposes of this report, **police data** refers to statistical and biographical data that is collected and recorded by police services (e.g., police stop data and reported crimes) and to data that may form part of a person's criminal record (e.g., arrests, convictions).[36] Many sources of police data may not be objective or accurate measures of criminal activity, but the data is recorded in municipal, provincial, and federal police databases, which, in turn, influence future interactions between the affected individual and police or the criminal justice system. Wherever this report refers to algorithmic processing of data from police databases, such data sets are referred to as **historic mass police data** or **historic police data sets**. These terms are used to emphasize the 'big data' nature of algorithmic policing and focus on circumstances where large volumes of pre-existing police data is used to train police algorithms or is otherwise mass processed by such algorithms. Historic mass police data is to be distinguished from piecemeal data processed on an individual basis, for instance, using a police officer's written notes in the case of a specific individual (as opposed to digitizing all of every officer's written notes and feeding that data set to an algorithm).

This section briefly surveys some key problems with different types of police data that may be used to train or that may inject bias and distortions into other data sets that are used to train policing algorithms or to derive an automated criminal justice decision about an individual.

**Police stop data:** The use of data gleaned from police stops poses a particular problem in light of the long-standing and widespread reports of discriminatory practices and patterns throughout Canada. A 2019 report on street checks in Halifax found that police were six times more likely to target Black individuals than white individuals.[37] In Ontario, police stops and traffic stops have long been reported to disproportionately affect Black, Indigenous, and other racialized individuals.[38] Although the controversial practice of "carding" came under some limited regulation in Ontario in 2017,[39] carding data that was gathered prior to 2017 is still accessible by police services in Ontario, and access is only partially restricted with respect to some carding data collected since 2017.[40] Many police

35 With thanks to Teresa Scassa for pointing these out. Specific types of algorithmic policing technologies and data sources are discussed in greater detail in Part 4 ("Algorithmic Policing in Canada: The Current Landscape").

36 For ease of reference throughout the report, the term "police data" will be used as a general term to describe these broad classes of data that are accessible to police and stored in police databases. Some aspects of the data, such as criminal convictions, are influenced by what happens in the later stages of criminal justice processes in criminal courts, but the data is nevertheless influenced substantially by law enforcement activity (as law enforcement, for example, chooses which cases to bring to court through its charging decisions), and is maintained in databases by law enforcement agencies.

37 Scot Wortley, *Halifax, Nova Scotia: Street Checks Report* (March 2019) at 105 <https://humanrights.novascotia.ca/streetchecks>.

38 See The Honourable Michael H. Tulloch, *Report of the Independent Street Checks Review* (2018) at 44 <https://www.mcscs.jus.gov.on.ca/sites/default/files/content/mcscs/docs/StreetChecks.pdf>.

39 In the report of the Independent Street Checks Review, Justice Tulloch defines "street check" as any incident where "information is obtained by a police officer concerning an individual, outside of a police station, that is not part of an investigation." "Carding" refers to a subset of street checks "in which a police officer randomly asks an individual to provide identifying information when the individual is not suspected of any crime, nor is there any reason to believe that the individual has information about any crime." *Ibid* at 2.

40 *Ibid* at 143; *Collection of Identifying Information in Certain Circumstances - Prohibition and Duties*, O. Reg. 58/16, s 2 and 9.

services have also not complied with transparency reporting requirements about police stop practices that are required by the regulation.[41] Data from police services across the country have revealed similar patterns in which Black and Indigenous individuals are overrepresented in police data.[42] The result is that police have access to vastly disproportionate amounts of information about racialized and Indigenous individuals and about certain neighbourhoods, which may then be used in policing algorithms.

**Gang databases:** Membership in a gang or association with gang members is often considered a risk factor by law enforcement agencies, and information stored in "gang databases" may be used to inform algorithmic policing technology.[43] The use of information about gang association gives rise to serious concerns about accuracy, as law enforcement agencies' determinations of gang involvement can often be problematic.[44] For example, in Surrey, British Columbia, a program that partners police and school staff to identify students at risk of gang activity examined factors such as whether the student's peer group is "uni- or multi-ethnic," whether they had "violent tendencies," and whether they were "hanging out with the wrong crowd."[45] According to a researcher at a Toronto-based community service organization that is focused on crime reduction, young people are routinely entered into police databases as being in a gang based on unverified information or incorrect assumptions from school staff, local service providers, or police officers.[46] Dr. Scot Wortley, a criminology professor at the University of Toronto, has raised concerns about the vagueness, imprecision, and manipulability of

41 Danielle, McNabb, Dennis Baker & Troy Riddell, "Mandatory police carding data severely lacking across Ontario", *Toronto Star* (14 August 2019), <https://www.thestar.com/opinion/contributors/2019/08/14/mandatory-police-carding-data-severely-lacking-across-ontario.html>.

42 Sunny Dhillon, "Vancouver Police Department's use of carding disproportionately targets Indigenous people", *The Globe and Mail* (4 June 2018) <https://www.theglobeandmail.com/canada/british-columbia/article-vancouver-police-departments-use-of-carding-disproportionately/>; Rocky Mountain Civil Liberties Association, "Calgary Police data suggests Police Carding is Greatest in Diverse Neighbourhoods" (9 May 2016), <http://www.rmcla.ca/blog/?p=394>; Andrea Huncar, "Indigenous women nearly 10 times more likely to be street checked by Edmonton police, new data shows", *CBC News* (27 June 2017) <https://www.cbc.ca/news/canada/edmonton/street-checks-edmonton-police-aboriginal-black-carding-1.4178843>.

43 For example, the Los Angeles Police Department considered gang membership in its person-focused predictive policing strategy known as the Chronic Offender Bulletin. See Issie Lapowsky, "How the LAPD Uses Data to Predict Crime", *Wired* (22 May 2018) <https://www.wired.com/story/los-angeles-police-department-predictive-policing/>.

44 Andrew Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (New York: NYU Press, 2017) at 58; Scot Wortley, "Identifying Street Gangs: Definitional Dilemmas and Their Policy Implications" (2010), <http://publications.gc.ca/collections/collection_2012/sp-ps/PS4-115-2011-eng.pdf>.

45 Nathan Munn, "This B.C. city is tackling gang violence by profiling high school students", *Vice* (7 January 2019) <https://www.vice.com/en_ca/article/59vv8x/this-bc-city-is-tackling-gang-violence-by-profiling-high-school-students>; Similarly, in the United States, researchers who claimed to develop an algorithm that identified gang members based on their Twitter posts—in particular, based on their use of "tough talk", certain words and emojis, and links to rap music videos—were criticized for the potentially discriminatory assumptions underlying the tool: Jordan Pearson, "Researchers Claim AI Can Identify Gang Members on Twitter", *Vice* (1 November 2016), <https://www.vice.com/en_us/article/mg7kgx/researchers-claim-ai-can-identify-gang-members-on-twitter>.

46 "As someone who evaluates gang programs, a lot of kids are labelled as involved or in a gang, whether it's by a school, local service provider, police officer, etc. That information just doesn't stay on the police's mental psyche, it gets fed into some other information database that this kid is in a gang. [...] Inside Corrections they have informants—some of that information, probably good. But when you get something from a school principal, and even when kids don't refer to themselves as a gang, they're labelled as a gang because they stole some kids' lunch money. There is more of an external imposition of labels. Then that is fed into other agencies with little validity, as opposed to what's actually confirmed." Interview of a researcher at a Toronto-based community service provider involved in criminal justice issues, by Yolanda Song & Cynthia Khoo (8 May 2019).

gang member criteria used by Canadian police services. He has also noted that flagging "gang association" can cause law-abiding friends and family members to be classified as "gang-involved."[47]

> *Kids may be not in a gang but gang-affiliated, because they're homeless or hanging around with them due to a dynamic lifestyle of need. A police officer would go, "Yup, that kid's been in a gang" because they're associated [...] But it could just be a homeless kid with addiction issues.*
>
> *- Researcher at Toronto-based community service provider*[48]

**Reports by members of the public:** Some police services may rely on crime reports initiated by members of the public to address the concerns associated with data generated by the police.[49] The reliability of reports by the public as a source of data is questionable, as demonstrated in a Statistics Canada report indicating that "[m]ost incidents of victimization, both violent and non-violent, never came to the attention of the police in 2014. Just under one-third (31%) were reported to the police, either by the victim directly (21%) or in some other way (10%)."[50] Even property crimes such as break-and-enters and motor vehicle thefts are only reported to the police about half the time.[51] These large gaps in reports of crime generated by the public may significantly undermine the accuracy of any crime forecasts that depend on this data source.

**Under-reported crimes:** Certain racialized communities are less likely to report crime due to pre-existing tensions, language or cultural barriers, fear of being deported, fear of law enforcement, prior bad experiences with the police, or mistrust of policing institutions due to discriminatory practices and history.[52] Transgender individuals and communities may also not report crimes "as a result of their own

47 Scot Wortley, "Identifying Street Gangs: Definitional Dilemmas and Their Policy Implications" (2010) at 13, <http://publications.gc.ca/collections/collection_2012/sp-ps/PS4-115-2011-eng.pdf>. Additionally, a 2019 review of the Chicago Police Department's gang database found that the Department was unable to confirm the accuracy of its gang designations, among other data quality and transparency issues. Sanjana Karanth, "Inspector General Finds Chicago Gang Database Outdated, Inaccurate and Damaging", *Huffington Post* (11 April 2019) <https://www.huff ingtonpost.ca/entry/chicago-inspector-general-police-gang-database_n_5cafd2b2e4b082aab0831bf7>.

48 Interview of a researcher at a Toronto-based community service provider involved in criminal justice issues, by Yolanda Song & Cynthia Khoo (8 May 2019).

49 See, for example, the Vancouver Police Department using only public-generated reports of property crime in its predictive policing algorithm, discussed in Section 4.1 ("Location-Focused Algorithmic Policing").

50 Samuel Perreault, "Criminal victimization in Canada, 2014" (23 November 2015) *Juristat Catalogue* no. 85-002-X at 23 <https://www150.statcan.gc.ca/n1/en/pub/85-002-x/2015001/article/14241-eng.pdf?st=RDyLQpoX>.

51 *Ibid* at 25. See also Teresa Scassa's critique of the reliability of public call data: "A person who reports a theft from their vehicle may realize some days later that the item they supposed to have been stolen was merely lost. Simply because something is reported to police does not mean that a crime occurred. If the maps simply reflect call data and are not updated as more information about the incidents becomes available, this decreases the reliability of the information." Teresa Scassa, "Police Service Crime Mapping as Civic Technology: A Critical Assessment" (2016) 5:3 International Journal of E-Planning Research 13 at 19.

52 The Honourable Michael H. Tulloch, *Report of the Independent Street Checks Review* (2018) at 45-46 <https://www.mcscs.jus.gov.on.ca/

or their community's experiences of victimization or discrimination at the hands of law enforcement."[53] Violence against women and sexual assault are also vastly underreported crimes, due to fear of stigma, re-victimization by law enforcement, and distrust that the victim's case will be respected or treated seriously.[54] Policing algorithms that purport to predict victimization may thus only reflect the circumstances of demographic groups that are more likely to report crime to police.

**Underdocumented crimes:** Compounding under-reported crime is crime that is reported, but ignored, whether as a result of error, mishandling, or discriminatory assumptions and stereotypes.[55] For instance, sexual assault is one of the most under-reported crimes in Canada,[56] due to punitive societal and institutional barriers that discourage victims and survivors from coming forward.[57] Despite this, a 2017 investigative report found that Canadian police have dismissed approximately 20% of reports of sexual assault as "baseless and thus unfounded."[58] Underdocumented crime may increase the disparity between sexual assault convictions and the actual prevalence of sexual assault in Canada—an issue that systemically harms women and girls and violates their human rights.[59] Using such data to train a policing algorithm may implicitly entrench into the model biases and assumptions that give rise to both under-reporting and overdismissal of sexual assault crime.

---

sites/default/files/content/mcscs/docs/StreetChecks.pdf>; Community Oriented Policing Services & Vera Institute of Justice, "How to Serve Diverse Communities" (2016) *Police Perspectives: Building Trust in a Diverse Nation*, No. 2 at 6 <https://www.securitepublique.gc.ca/lbrr/archives/cnmcs-plcng/cn96061923-eng.pdf>. Deportation fears may also be a contributing factor to under-reporting: Cecilia Benoit, "Issue Brief: Sexual Violence Against Women in Canada", commissioned by the Federal-Provincial-Territorial Senior Officials for the Status of Women (December 2015), <https://cfc-swc.gc.ca/svawc-vcsfc/index-en.html>.

53 Community Oriented Policing Services & Vera Institute of Justice, "How to Serve Diverse Communities" (2016) *Police Perspectives: Building Trust in a Diverse Nation*, No. 2 at 27 <https://www.securitepublique.gc.ca/lbrr/archives/cnmcs-plcng/cn96061923-eng.pdf>.

54 See e.g., "[Underreporting] may be a factor for certain types of crime (such as, for example, sexual assault or domestic violence) (Johnson, 2012) or for certain types of victims who may seek to minimize their contact with police (e.g. street involved persons). Underreporting may also be an issue in communities where there is a distrust of police or where there is a fear of retribution for reporting crimes to police." Teresa Scassa, "Police Service Crime Mapping as Civic Technology: A Critical Assessment" (2016) 5:3 International Journal of E-Planning Research 13 at 21.

55 "Policing is not the passive collection of information, nor the identification of every violation of the law. Every action—or refusal to act—on the part of a police officer, and every similar decision made by a police department, is also a decision about how and whether to generate data. … police decision-making shapes the very reality we perceive about crime and law breaking. We know about the crimes the police pay attention to. With others, we often don't." In Elizabeth E Joh, "Feeding the Machine: Policing, Crime Data, & Algorithms" (2017) 26:2 William & Mary Bill of Rights Journal 287 at 289-90 (footnotes omitted).

56 Shana Conroy & Adam Cotter, "Self-reported sexual assault in Canada, 2014" (11 July 2017) *Juristat, Catalogue no. 85-002-X* at 4 <https://www150.statcan.gc.ca/n1/pub/85-002-x/2017001/article/14842-eng.pdf>.

57 See generally Alana Prochuk, "We Are Here: Women's Experiences of the Barriers to Reporting Sexual Assault" (November 2018) West Coast *LEAF* <http://www.westcoastleaf.org/wp-content/uploads/2018/10/West-Coast-Leaf-dismantling-web-final.pdf>. According to one survey, in 2014, 83% of sexual assaults in Canada were not reported to police, while only 5% were: Department of Justice, "Just Facts: Sexual Assault" (May 2017) at 1 <https://www.justice.gc.ca/eng/rp-pr/jr/jf-pf/2017/may02.html>.

58 Robyn Doolittle, "Why police dismiss 1 in 5 sexual assault claims as baseless" (3 February 2017) *The Globe and Mail* <https://www.theglobeandmail.com/news/investigations/unfounded-sexual-assault-canada-main/article33891309/>.

59 Cristine Rotenberg, "From arrest to conviction: Court outcomes of police-reported sexual assaults in Canada, 2009 to 2014" (26 October 2017) *Juristat, Catalogue no. 85-002-X*, at 4, <https://www150.statcan.gc.ca/n1/pub/85-002-x/2017001/article/54870-eng.pdf>. Men and non-binary individuals are also systematically unlikely to report instances of sexual assault.

**Arrests:** While arrest data is frequently used in algorithmic policing technologies,[60] arrests are not factually or legally accurate representations of criminal activity. Individuals who are arrested may be released, have charges against them withdrawn, or be eventually acquitted. Furthermore, while relatively few Canadian studies of this issue exist, particularly since authorities are not required to collect or disclose data about race, some data and reporting has shown that racialized and Indigenous individuals are disproportionately more likely to be arrested for cannabis possession offences (despite similar rates of cannabis use amongst the general population) or subjected to overly harsh treatment for minor offences relative to white individuals.[61] In addition, arrests for administration of justice offences, which made up more than one in five of all adult criminal cases completed in 2015-2016,[62] may have a particular impact on marginalized groups. Administration of justice offences include failure to appear in court, breach of a probation order, being unlawfully at large, and failure to comply with an order. Some of these arrests result from the imposition of unjustified or inappropriate conditions that place unreasonable restrictions on vulnerable individuals. For example, individuals struggling with addiction may be more likely to be arrested for breaching bail conditions that require them to abstain from drugs or alcohol, while precariously housed individuals may face arrest for breaching bail conditions that require them to obey a curfew or remain at a fixed address.

**Convictions and Guilty Pleas:** Unlike arrests, convictions are legally considered to be proof that a person has committed a crime. However, conviction data is also unreliable for a number of reasons. As noted above, conviction data will also be permeated by the effects of systemic bias and over-policing, as convictions can arise only out of the cases that are brought to court by law enforcement. Further, individuals may be wrongfully convicted.[63] Certain groups, such as women and Indigenous individuals, are particularly vulnerable to wrongful convictions.[64] A subset of convictions come from cases where individuals have pleaded guilty and waived their right to a trial. The vast majority of criminal cases do not go to trial and are instead dealt with through resolutions, including guilty plea resolutions.[65] Consequently, statistics about criminal conviction rates in Canada are largely made up of guilty plea convictions even though "factually innocent persons in Canada have sometimes, for a variety of reasons,

60 See, for example, predictive policing strategies in Chicago, New Orleans, and Kansas City, Missouri, as described in Andrew Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (New York: NYU Press, 2017) at 44-51.

61 Rachel Browne, "Black and Indigenous people are overrepresented in Canada's weed arrests" (18 April 2018) *Vice* <https://www.vice.com/en_ca/article/d35eyq/black-and-indigenous-people-are-overrepresented-in-canadas-weed-arrests>; Jim Rankin & Sandro Contenta, "Toronto marijuana arrests reveal 'startling' racial divide", *Toronto Star* (6 July 2017), <https://www.thestar.com/news/insight/2017/07/06/toronto-marijuana-arrests-reveal-startling-racial-divide.html>. Akwasi Owusu-Bempah, "Race, Crime, and Criminal Justice in Canada", in *The Oxford Handbook of Ethnicity, Crime, and Immigration* (Oxford: Oxford University Press, 2014) at 15 <https://www.researchgate.net/publication/274314275_Race_Crime_and_Criminal_Justice_in_Canada>.

62 Department of Justice, "The Canadian Criminal Justice System: Overall Trends and Key Pressure Points" (23 November 2017) <https://www.justice.gc.ca/eng/rp-pr/jr/press/>.

63 Innocence Canada has been involved in the exonerations of 23 individuals since 1993: Innocence Canada, "Exonerations" <https://www.innocencecanada.com/exonerations/>. It is unknown how many wrongful convictions go undetected; see 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 1 <https://www.ppsc-sppc.gc.ca/eng/pub/is-ip/is-ip-eng.pdf>.

64 *Ibid* at 221.

65 Although there are no Canadian national statistics on guilty pleas, researchers have estimated that approximately 90% of criminal cases are resolved by guilty pleas. See Angela Bressan & Kyle Coady, "Guilty pleas among Indigenous people in Canada" (2017) at 6 <http://publications.gc.ca/site/eng/9.851369/publication.html>.

pleaded guilty to crimes they did not commit."[66] 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.[67] 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."[68] Research has also suggested that other marginalized groups, including youth, individuals with cognitive difficulties, individuals experiencing mental health or addictions issues, individuals in poverty, and racialized individuals may also be particularly at risk of entering false guilty pleas.[69] Lack of legal aid funding has contributed to false guilty pleas from those with socio-economic disadvantage.[70] 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.[71]

The above is not an exhaustive list of all the forms of data that may determine how a policing algorithm works, nor are all of the types of police data reviewed necessarily used as training data or input data for policing algorithms in Canada.[72] However, the fact that all of the most common sources of police data are affected by problems that may distort the reliability of those sources should give rise to significant questions and apprehension about using big data-driven policing techniques such as algorithmic policing. Specific issues with data inaccuracies and data bias are discussed throughout the legal analysis provided in Part 5 ("International Human Rights and *Charter* Rights Implications of Algorithmic Policing") of this report.

In summary, the discussion of social and historical context just presented in this part of the report—Part 2 ("Social and Historical Context")—highlights that when considering the adoption of new methods of policing, such as algorithmic policing technology, it is essential to ensure that these new methods

66 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>.

67 *Ibid* at 179-180.

68 Angela Bressan & Kyle Coady, "Guilty pleas among Indigenous people in Canada" (2017) at 9 <http://publications.gc.ca/site/eng/9.851369/publication.html>.

69 *Ibid* at 6.

70 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>.

71 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>.

72 The problems associated with the use of police-generated data are not unique to criminal justice policy and have led to the call for the need for democratic accountability in relation to data governance and policy in Canada. The context of systemic bias and historical oppression in government data collection practices has been recognized, for example, by the BC First Nations Data Governance Initiative (BC FNDGI). The BC FNDGI and Indigenous scholars and advocates have called for Indigenous sovereignty and participation regarding data collection practices. Respecting such calls is of particular importance in light of how non-Indigenous data collection and sharing practices in Canada have "reinforced systemic oppression, barriers and unequal power relations": Open North & British Columbia First Nations Data Governance Initiative, "Decolonizing Data: Indigenous Data Sovereignty Primer" (April 2017) at 3; Marcia Nickerson, "First Nations' Data Governance: Measuring the Nation-to-Nation Relationship" (May 2017). Both papers are available at <https://www.bcfndgi.com/>.

do not aggravate or contribute to the historic disadvantage experienced by communities targeted by 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.[73] If law enforcement agencies seek to justify heightened surveillance or interferences with liberty and privacy based on algorithmic predictions derived from implicitly biased data, it puts historically disadvantaged and targeted groups at risk of ongoing discrimination through "math-washing."[74] Math-washing describes how inflated or false trust in seemingly neutral mathematical processes that underlie a decision-making process or method tends to obscure biases embedded in such decision-making. The human rights and *Charter* implications of these risks of bias are discussed in full in Part 5 ("International Human Rights and *Charter* Rights Implications of Algorithmic Policing").

Before turning to a more fulsome explanation of what algorithmic policing technologies are and how they work, the following spotlighted discussion, **In Focus #1: Community Perspectives on Algorithmic Policing**, provides a summary of the authors' findings with respect to the views of communities that are likely to be most impacted by the adoption of such technologies.

73 Data bias can occur in more than one way. For example, generally speaking, crime is more likely to be detected within communities that are the focus of police attention. Further, criminologists have called attention to problematic effects of disproportionate police attention and the criminal justice system that can, itself, breed environmental factors that lead to further police targeting and criminalization. Finally, socio-economic disparities and cycles of poverty render individuals vulnerable to heightened scrutiny and over-policing, while they are less able to access outcomes in criminal courts that focus on rehabilitation as opposed to punishment due to shortages in legal aid funding.

74 See, e.g., Elizabeth E Joh, "Feeding the Machine: Policing, Crime Data, & Algorithms" (2017) 26:2 William & Mary Bill of Rights Journal 287 at 292 <https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1835&context=wmborj> and Chelsea Barabas (26 February 2019), *Beyond Accuracy and Bias: The Pursuit of "Ethical AI" in Criminal Law*, lecture presented at the University of Toronto Centre for Ethics, <https://c4ejournal.net/2019/03/01/chelsea-barabas-beyond-accuracy-and-bias-the-pursuit-of-ethical-ai-in-criminal-law-2019-c4ej-9/>. The impacts of algorithmic policing on the right to equality, and the right to freedom from discrimination, of historically oppressed communities is further discussed below in Section 5.4 ("Right to Equality and Freedom from Discrimination").

# Community Perspectives on Algorithmic Policing

Community representatives from groups disproportionately impacted by over-criminalization, such as Black and Indigenous communities, were interviewed for this report.[75] These representatives included: Jonathan Rudin, the Program Director at Aboriginal Legal Services, author of *Indigenous People and the Criminal Justice System: A Practitioner's Handbook*, and a lawyer, speaking on behalf of himself in a personal capacity; Desmond Cole, a Canadian journalist, racial justice activist, and author of *The Skin We're In: A Year of Black Resistance and Power*; the Black Legal Action Centre (BLAC); and a researcher at a Toronto-based community service provider involved in criminal justice issues.

The research interviews covered a range of community perspectives on algorithmic policing and how such technologies could impact the respective communities of those interviewed. These individuals raised several concerns that closely overlap with the human rights issues associated with algorithmic policing as examined in this report, including algorithmic bias, the problems with police data, feedback loops entrenching systemic discrimination, data privacy, the chilling effect on racial justice and Indigenous rights activism, and exacerbating community distrust of law enforcement. Their comments on these points are incorporated throughout Part 5 ("International Human Rights and *Charter* Rights Implications of Algorithmic Policing") of this report.

Above all, community representatives expressed the overriding concern that algorithmic policing tools would perpetuate systemic discrimination against marginalized communities while simultaneously masking the underlying systemic issues and root problems in the criminal justice system that cannot be fixed through technology. According to Desmond Cole, "Offering a more fantastic method of police profiling is not a solution; it is actually a strategy to continue profiling Black people, Indigenous people, and other racialized groups. I would include in that the historical targeting of queer and trans people, people living with mental health issues, and people living with disabilities."[76] Responding to the notion that algorithms may decrease bias, the Black Legal Action Centre (BLAC) stated, "The solution isn't 'go to an algorithm,' the solution is to have your officers and have your employees not be racist. Before we go down this road, some of that money or all of it could be invested in things that reports and studies have said forever are important—the social determinants of health—a properly funded education system, public health, those kinds of things. Affordable housing. Community centres, grocery stores. Engaging the community in common sense ways as opposed to going to a computer to tell you there's a problem and have a private company benefit off of that."[77]

Community representatives also viewed the use of algorithmic policing tools as inseparable from Canada's history of colonialism and systemic discrimination against Indigenous, racialized, and other marginalized groups. Interview responses often turned towards the role of this history and its continuing

75 See Section 1.2 ("Methodology") for details regarding the research protocol followed for these interviews.

76 Interview of Desmond Cole by Cynthia Khoo & Yolanda Song (31 May 2019).

77 Interview of Black Legal Action Centre by Cynthia Khoo (12 July 2019).

impacts today, including the historical function of law enforcement and associated implications for algorithmic policing. For example, Rudin shared the following personal view, speaking on behalf of himself only: "Historically, when Indigenous people assert rights, they're seen to be breaking the law. Police are used historically—and by historically I'm going back to the Riel rebellion, but also Oka and Burnt Church and Ipperwash and what's going on in BC now—when Indigenous people assert rights, that isn't a legal question for courts. It's a policing question, and police work on the assumption that Indigenous people have no rights and arrest on various charges. Indigenous people are vulnerable to that surveillance and data collection when, in fact, they're engaged in legitimate activity."[78] In his interview, Cole stated, "The legacy of our origins on this territory, for me, mean that we understand being Black in Canada through a continuous story that is four centuries old of being racialized, being othered, being treated as a commodity [...] Everything that flows from that, every algorithm, every pattern recognition technology, simply flows out of the idea that there are limits to our freedoms as Black and Indigenous and other racialized peoples, and these algorithms are actually helping to enforce the limits."[79]

Community representatives involved in racial justice advocacy further shared the view that algorithmic policing tools are merely continuations of pre-existing policing tools that have been used to justify state violence. New policing technologies are seen as, in the words of BLAC, "allow[ing] for a scientific way to justify things that are already happening [...] Police being in schools, or police being on that corner. Data justifying more exclusion, more surveillance, more police interaction. And we know for Black folks, the more they interact with police, the more likely they are to die."[80] According to Cole, "Being able to create a social network that tells you that a 13-year-old is part of a gang will justify when you roll up on him and beat the crap out of him. I draw a straight line because it is only through the technology that the police are attempting to justify the violence that they have been committing. Thirty years ago when you just had paper notes, your paper notes would have told you to go after the young man anyhow. I don't actually separate these technologies from police engaging in direct forms of violence against Black communities."[81]

Those interviewed expressed doubt that algorithmic policing could benefit marginalized communities, with Rudin citing missing and murdered Indigenous women and girls as an example: "If I think about missing and murdered Indigenous women, I don't know what predictive policing does. They're seen as either not worthy of looking at, or they're just missing—so what is technology going to do?"[82] Similarly, a researcher at a Toronto-based community service provider involved in criminal justice issues stated,

78 Interview of Jonathan Rudin by Cynthia Khoo & Yolanda Song (8 May 2019). Rudin also noted, with respect to police discretion: "In Toronto, Indigenous protest is generally well-tolerated. You let the police know in advance, we're going to shut down an intersection, and people don't react immediately by arrest, generally. But they could. You could see it as legitimate protest or as breaking the law. And the determination of that is not an analytic discussion; it's a policing perspective discussion".

79 Interview of Desmond Cole by Cynthia Khoo & Yolanda Song (31 May 2019).

80 Interview of Black Legal Action Centre by Cynthia Khoo (12 July 2019).

81 Interview of Desmond Cole by Cynthia Khoo & Yolanda Song (31 May 2019).

82 Interview of Jonathan Rudin by Cynthia Khoo & Yolanda Song (8 May 2019).

"I've never seen a dot map in my life for intimate partner violence. Was there a dot map for missing Indigenous women?"[83]

Lastly, community representatives expressed concern regarding their lack of familiarity with emerging algorithmic policing techniques and, in doing so, raised issues of information asymmetry between policed communities on the one hand, and law enforcement and police technology vendors on the other.[84] Overall, the research interviews demonstrated a significant informational and perspectives gap between community representatives and law enforcement representatives, with respect to algorithmic policing technologies.

83 Interview of a researcher at a Toronto-based community service provider involved in criminal justice issues, by Yolanda Song & Cynthia Khoo (8 May 2019).

84 A researcher at a Toronto-based community service provider involved in criminal justice issues shared, "There would be very few, if any, community service providers [CSPs] that have familiarity with things like hotspot policing or automated decision-making tools in general." The researcher expressed particular concern about "how unprepared and uninformed most people like myself and other CSPs are on these things. We're really just not ready." Interview of a researcher at a Toronto-based community service provider involved in criminal justice issues, by Yolanda Song & Cynthia Khoo (8 May 2019).

# 3. What Is Algorithmic Policing?

Algorithmic policing technology refers to a variety of algorithm-driven technologies that purportedly enable law enforcement agencies in drawing inferences from mass data processing with the goal of predicting potential unlawful activity ('predictive policing' technologies) or, alternatively, in collecting and analyzing data through automated surveillance and algorithmic analysis ('algorithmic surveillance technology'). Section 3.1 introduces technological concepts that are involved in algorithmic policing and that are raised throughout the report. Section 3.2 explains how algorithmic policing, as defined in this report, differs from both conventional and 'big data' policing and surveillance methods.

## 3.1. A Technical Primer

This section provides a basic explanation of technological concepts that are key to algorithmic policing and discussed throughout the report.

**Algorithmic policing** describes the use of algorithms by police services for the pre-emptive monitoring and forecasting of potential crime before any crime has occurred. The term encompasses surveillance tools, such as facial recognition and automated licence plate readers, that rely on algorithmic technologies to operate. It also includes algorithmic technologies that draw inferences through mass data processing in the hopes of predicting potential criminal activity. The latter type of technology is often referred to as **predictive policing** technology.[85] However, this report predominantly uses the term algorithmic policing technology, since "predictive policing" is somewhat of a misnomer: using algorithms to draw inferences about potential criminal activity results in generalized statistical guesses rather than concrete predictions.[86] Thus, the authors use "algorithmic policing" to encompass both algorithmic surveillance tools and what has popularly been known as "predictive policing". The latter term will be used later in this report where a given discussion concerns "predictive policing" technologies specifically. This use recognizes that, for the public, predictive policing remains the most popular and familiar term to describe the types of technologies under consideration. This use also distinguishes algorithmic policing technologies with purported predictive capabilities from algorithmic policing technologies that are used for general surveillance.

85 This report uses the term "predictive policing" where relevant, to denote those technologies that attempt to generate statistical guesses through mass data processing.

86 "Predictive policing is a marketing term — popularized by vendors in the public safety industry — for computer systems that use data to automatically forecast where crime will happen or who will be involved." Upturn, *Stuck in a Pattern: Early evidence on "predictive policing" and civil rights* (August 2016), at 2 <https://www.upturn.org/static/reports/2016/stuck-in-a-pattern/files/Upturn_-_Stuck_In_a_Pattern_v.1.01.pdf>. S/Constable Ryan Prox of the Vancouver Police Department, in a research interview, was also critical of the term 'predictive policing': "I think it's a marketing ploy by a lot of vendors that say they can do all these other things. But a lot of it is black box stuff where there's no true evaluative metric on whether they're delivering on any crime prevention outcomes. I don't believe they are." Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019).

An **algorithm** is a "technologically automated mathematical formula"[87] that instructs a computer to process given inputs in a particular way so as to result in certain outputs. Where an algorithm is relied upon to assist or substitute human decision-making, this application is known as **algorithmic decision-making**, or sometimes **automated decision-making**. Algorithms are central to **artificial intelligence**, which refers to the ability of a computer to perform tasks that are normally considered to require human intelligence.[88]

Some algorithms, such as **machine-learning** algorithms, autonomously 'learn'[89] how to perform tasks. The algorithms generate a set of rules that are based on large **training data** sets, and the algorithm autonomously updates those rules as more data is provided in order to optimize the algorithmic outputs towards a particular goal.[90] Machine learning relies in part on **data mining**, which is the "practice of searching through large amounts of computerized data to find useful patterns and trends."[91] The algorithms extrapolate patterns from the training set examples to derive **output data (outputs)** from new **input data (inputs)**. As more data is provided, the algorithms may change to fit the new data.[92] Computer vision (identifying visual images), natural language processing (interpreting and simulating human language), and speech recognition (converting spoken words into text) are common examples of machine learning technology.[93]

87 Royal United Services Institute, M*achine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges* (September 2018) at 2. <https://rusi.org/sites/default/files/201809_whr_3-18_machine_learning_algorithms.pdf.pdf>.

88 Computers that complete specific discrete tasks, such as playing chess, unlocking car doors, or autocompleting search terms display **artificial narrow intelligence**. On the other hand, **artificial general intelligence** refers to "a system that displays intelligence across multiple domains, with the ability to learn new skills, and which mimic or even surpass human intelligence": Privacy International, "Privacy and Freedom of Expression In the Age of Artificial Intelligence" (April 2018), at 6 <https://privacyinternational.org/sites/default/files/2018-04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf>. The policing and criminal justice technologies examined in this report are artificial narrow intelligence systems.

89 To be clear, "the idea that the computers are 'learning' is largely a metaphor and does not imply that computers systems are artificially replicating the advanced cognitive systems thought to be involved in human learning." Harry Surden, "Machine Learning and Law" (2014) 89:1 Washington Law Review 87 at 89.

90 The Royal Society, *Machine learning: the power and promise of computers that learn by example* (April 2017) at 19 <https://royalsociety.org/~/media/policy/projects/machine-learning/publications/machine-learning-report.pdf>. "Learning" is used metaphorically to represent the process of the computer adjusting its algorithm as more data is provided.

91 Walter L Perry et al, "Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations" (2013) at 34 <https://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf>, citing the Merriam-Webster online dictionary. Note that while machine learning involves data mining, it is possible to engage in data mining without the use of machine learning.

92 Machine learning algorithms may be combined and integrated with each other in hundreds of layers of algorithmic data processing, forming **neural networks**. A neural network is a form of machine learning architecture that consists of numerous layers of interconnected computational processing units. Each layer processes the input data it receives, and the output data that layer provides becomes the input data for the next layer of processing units. Thus, every initial input in a neural network goes through dozens to hundreds of layers of algorithmic processing before the final output emerges. This process is known as **deep learning**. Access Now, "Human Rights in the Age of Artificial Intelligence", at 9; "What is a neural network and how does its operation differ from that of a digital computer? (In other words, is the brain like a computer?)", *Scientific American* (14 May 2007) <https://www.scientificamerican.com/article/experts-neural-networks-like-brain/>; and Hannah Couchman, "Policing by Machine: Predictive policing and the threat to our rights," (January 2019) Liberty, at 11 <https://www.libertyhumanrights.org.uk/sites/default/files/LIB%2011%20Predictive%20Policing%20Report%20WEB.pdf>.

93 Access Now, *Human Rights in the Age of Artificial Intelligence* (November 2018) at 10 <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf>.

There are two kinds of machine learning: supervised and unsupervised. In **supervised machine learning**, the training data set is labelled.[94] For example, an algorithm may be instructed to analyze thousands of animal photos already labelled "dog" or "cat", in order to train it to distinguish between the two. The algorithm determines what factors distinguish photos of dogs from photos of cats, and it applies those rules to new, unlabelled photos (inputs) in order to categorize them (outputs). In **unsupervised machine learning**, the system looks for patterns in unlabelled training data (e.g., unlabelled photos), based on variables that it determines to be the most relevant and subsequently generates rules based on those patterns.[95]

The inner workings of machine-learning algorithms are not always intelligible to human understanding, or their source code may be kept from public view for reasons of trade secrets in intellectual property, or due to free trade agreements. This opacity results in what is commonly known as the **black box**[96] problem: one may see the input and output data, but little to no information is available as to how or why a given input leads to a particular output. This lack of explainability can be problematic where it impairs the ability to assess the reliability of a given algorithm, including discovering if the algorithm is operating in a flawed or unintended way. For example, in one study, a neural network that had purportedly learned how to distinguish between dogs and wolves was classifying photos accurately, but based on whether or not there was snow in the background, and not based on the animals' features.[97]

To be effective, algorithms must be trained on data that is accurate and representative of the subject matter being studied. When the training data set is inaccurate or biased, those flaws are reflected in the algorithm's outputs (even if flaws are not obvious when appraising the algorithm's outputs). This principle is commonly referred to as "**garbage in, garbage out**." For example, if training photos of cats and dogs are labelled improperly, the algorithm will classify input photos less accurately. Additionally, if the algorithm is trained on thousands of photos of cats and only ten photos of dogs, the algorithm will be able to classify cat photos more accurately than dog photos. This is an example of **statistical bias**, which refers to gaps or other problems in a data set that cause it to be unrepresentative of reality. Statistical bias is a major source of concern in real-world training data sets.[98] A prominent example is seen in facial recognition algorithms that are trained on data sets in which certain genders, ages, or

94 Royal United Services Institute, *Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges* (September 2018) at 18 <https://rusi.org/sites/default/files/201809_whr_3-18_machine_learning_algorithms.pdf.pdf>.

95 *Ibid*, at 18-19.

96 Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, Massachusetts: Harvard University Press, 2015) at 3.

97 Marco Tulio Ribeiro, Sameer Singh & Garlos Guestrin, "'Why Should I Trust You?' Explaining the Predictions of Any Classifier" (Paper delivered at KDD '16: Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, August 2016). For additional examples of artificial intelligence technically following developers' instructions but in ways that "subverted their expectations or intentions", see Joel Lehman, Jeff Clune & Dusan Misevic, "The Surprising Creativity of Digital Evolution: A Collection of Anecdotes from the Evolutionary Computation and Artificial Life Research Communities" (2020) Artificial Life 1.

98 Upturn, *Stuck in a Pattern: Early evidence on "predictive policing" and civil rights* (August 2016) at 6 <https://www.upturn.org/static/reports/2016/stuck-in-a-pattern/files/Upturn_-_Stuck_In_a_Pattern_v.1.01.pdf>.

racial groups are under-represented or absent. Such models will make more errors in recognizing the faces of individuals from those under-represented groups.[99]

Algorithmic policing technologies whose underlying algorithms are trained on historical data will attempt to forecast future outcomes based on this data, and thus, they will generate inferences that are based on past patterns. The underlying assumption is that patterns found in past data will continue to be applicable in the future. However, where historical data is distorted by wrongful overrepresentation and systemic discrimination, the resultant models will reproduce those distortions. This is particularly so because algorithms are able to detect only correlation, not causation. Where a policing algorithm has been contaminated by corrupted, distorted, incomplete, or biased data (whether inadvertently or intentionally), it has been trained on **dirty data**.[100]

When developing and applying machine-learning algorithms, ensuring that training data is accurate and unbiased is only one component of an ongoing process that must be in place to properly evaluate the accuracy and reliability of the algorithm and to ensure that it is applied in a manner that does not result in adverse results or bias against individuals subjected to the algorithm. The evaluation and operation of a machine-learning mechanism can be just as fraught as the training process. Testing and evaluation must occur based on the input data that will be used in real-time operational situations. An algorithm that may appear to be accurate and unbiased can still produce adverse results if new and untested types of data are given as input during operation. Operational input data must also be accurate; otherwise, adverse results can occur even if the algorithm itself appears to be generally sound. For this reason, testing and evaluation must also continue past the implementation phase.

Section 3.1 has introduced central concepts that are used throughout the subsequent parts of this report. These explanations help to facilitate understanding of the research findings and legal analysis relating to algorithmic policing technology, set out in Part 4 ("Algorithmic Policing in Canada: The Current Landscape") and Part 5 ("International Human Rights and *Charter* Rights Implications of Algorithmic Policing"). To conclude Part 3, Section 3.2 contextualizes algorithmic policing technologies in relation to traditional policing methods.

99 Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", (2018) 81 Proceedings of Machine Learning Research 1, <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>; Brendan Klare, Mark Burge, Joshua Klontz, et al, "Face Recognition Performance: Role of Demographic Information", (2012) 7(6) IEEE Transactions in Info Forensics & Security 1789, <https://ieeexplore.ieee.org/document/6327355>. Similarly, in algorithmic policing programs, the existing data about police activity may be used in data processing to draw inferences regarding risk, such that data about police activity becomes a proxy for data about past criminal activity even though those are two very different metrics. In other words, police data tends to reflect law enforcement behaviour rather than portraying a true depiction of where criminal activity has taken place and by who. For more details regarding how police data does not objectively or accurately reflect criminal activity, see Section 2.2 ("Bias and Inaccuracies in Police Data").

100 Richardson, Schultz, and Crawford adopted the term "dirty data" from the field of data mining, where the term means missing, erroneous, or inconsistently represented data: Rashida Richardson, Jason M Schultz & Kate Crawford, "Dirty Data, Bad Predictions: How civil rights violations impact police data, predictive policing systems, and justice" (May 2019) 94:192 New York University Law Review 193 at 195, <https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf>.

## 3.2. What Makes Algorithmic Policing Different?

Algorithmic policing is related to, but different from, big data policing methods, which are used alongside conventional policing methods. The state's surveillance infrastructure and law enforcement's big data ecosystem form the backdrop of and fuel for algorithmic policing technologies. Today, police services in Canada have access to unprecedented and ever-growing amounts of data. Police services rely on a variety of interconnected systems to track criminal activity, crime patterns, suspects, victims, and investigations.[101] Data collection and tracking by law enforcement actors have resulted in a number of municipal, regional, provincial, and federal databases and internal records management systems.[102] Over time, data collection and aggregation methods have evolved with the advent of technology. For example, law enforcement actors have sought access to smart city data,[103] social media data, mobile device information (including location) obtained remotely,[104] and private sector consumer data (such as surveillance cameras built into "smart home" devices).[105]

101 In British Columbia, for example, all provincial and municipal police agencies use a centralized provincial records management system (RMS) known as the Police Records Information Management Environment (PRIME-BC). In addition, municipal police agencies also have access to an integrated data mining and data analytics system known as the Consolidated Records and Intelligence Mining Environment (CRIME), which is administered and run by the Vancouver Police Department. Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019); see also Jun Min Chang, "Vancouver C.R.I.M.E. System" (1 August 2013) *Blue Line* <https://www.blueline.ca/vancouver_c-r-i-m-e-_system-2784/>.

102 These databases include, for example, Canadian Police Information Centre (CPIC), Ontario Police Technology Information Cooperative (OPTIC) or Niche, the RCMP's Police Information Portal (PIP) and Police Information Retrieval System (PIRS), the Canadian Criminal Real Time Identification Services (CCRTIS), the Automated Criminal Intelligence Information System (ACIIS), and others that facilitate business intelligence, mobile report, and digital evidence management: See Alison Brooks, "Law Enforcement Information Management Study" (October 2014) *IDC* at 12-22, <https://cacp.ca/index.html?asst_id=977>. Generally speaking, these databases are designed to store and share information about criminal records, outstanding charges, warrants, persons of interest, stolen property, person-specific flags to caution police officers who may interact with them, and other information of interest.

103 For example, electronic transit passes in several Canadian cities resulted in their respective transit agencies sharing commuters' private travel data with police, without a warrant: Ben Spurr, "Metrolinx has been quietly sharing Presto users' information with police" (3 June 2017) *The Toronto Star* <https://www.thestar.com/news/gta/2017/06/03/metrolinx-has-been-quietly-sharing-presto-information-with-police.html>; *CBC News*, "Police use of Compass Card data raises alarm for B.C. civil liberties advocate" (9 August 2017) <https://www.cbc.ca/news/canada/british-columbia/police-use-of-compass-card-data-raises-alarm-for-b-c-civil-liberties-advocate-1.4240452>; Jacques Marcoux, "Winnipeg Transit gave Peggo card travel history to police without warrants" (7 June 2017) *CBC News* <https://www.cbc.ca/news/canada/manitoba/winnipeg-transit-peggo-data-police-1.4148965>; see also Teresa Scassa, "As smart cities become our norm, we must be smart about a data strategy" (13 February 2019) *Hill Times* <https://www.hilltimes.com/2019/02/13/smart-cities-become-norm-must-smart-data-strategy/188280>.

104 This capability is enabled through International Mobile Subscriber Identity (IMSI) catchers, also known as cell-site simulators, which are "devices that impersonate cell phone towers, convincing mobile devices to interact with them as they normally would only interact with a service provider's tower": Tamir Israel & Christopher Parsons, *Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada* (August 2016) at 2, <https://citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf>. Police services in Calgary, Winnipeg, and Toronto, as well as the Ontario Provincial Police and RCMP have all been confirmed to use or have used IMSI catchers, thus indiscriminately collecting data from all cellphones within range: Matthew Braga & Dave Seglins, "Cellphone surveillance technology being used by local police across Canada" (13 April 2017) *CBC News* <https://www.cbc.ca/news/technology/cellphone-surveillance-police-canada-imsi-catcher-privacy-1.4066527>; Kate Allen, Jayme Poisson & Wendy Gillis, "Two years after they said they didn't, Toronto police admit they use Stingray cellphone snooping device" (5 March 2018) *The Toronto Star*, <https://www.thestar.com/news/gta/2018/03/05/two-years-after-they-said-they-didnt-toronto-police-admit-they-use-stingray-cellphone-snooping-device.html>.

105 See, e.g., Jennifer Valentino-DeVries, "Google's Sensorvault Is a Boon for Law Enforcement. This is How It Works" (13 April 2019) *New York Times* <https://www.nytimes.com/2019/04/13/technology/google-sensorvault-location-tracking.html>; Sam Biddle, "Amazon's Home Surveillance Chief Declared War on 'Dirtbag Criminals' as Company Got Closer to Police" (14 February 2019) *The Intercept* <https://theintercept.com/2019/02/14/amazon-ring-police-surveillance/>.

Big data policing methods are characterized by three central features that are used to distinguish big data generally from prior data processing methods, and thus, to distinguish big data policing from conventional policing methods.[106] These features are known as the "three Vs," each referring to the unprecedented extent of the component: volume (massive quantities of data are collected and processed for law enforcement purposes, far beyond what a human would be able to manually process or what traditional, non-AI software could process); velocity (law enforcement is able to process surveillance and police data at unprecedented speeds, up to in real-time); and variety (many different types of data sets are now available to police to use in monitoring and investigations, from a diverse range of sources that can be integrated with each other, combined, and cross-referenced to result in deeper, more detailed, or further-reaching insights and inferences).[107]

Algorithmic policing technologies are distinguishable from both conventional and big data policing methods, and they warrant specific attention and concern.[108] First, such technologies take big data policing methods to an even greater level of scale. Big data sources, with their formidable volume and range of information, sustain the algorithmic technologies that authorities might use. As a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) shared in an interview, "I wouldn't have been able to use [algorithmic modelling] in the past because I wouldn't have had the volume of data or statistical capacity."[109] Second, algorithmic methods enable a wider range of data collection, aggregation, and analysis than used with conventional or big data policing methods. For example, surveillance methods that are algorithmically automated to perform various tasks relating to data collection, aggregation, and analysis (such as facial recognition, social media monitoring, and social network analysis) are less constrained by cost and resources as compared to conventional methods. The AI Now Institute articulates the distinction between algorithmic and traditional surveillance as follows:

> 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. Thus, they can serve to further centralize these capabilities in the hands of a small number of actors. 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

106 See e.g., Alison Brooks, "Law Enforcement Information Management Study", IDC (October 2014) <https://cacp.ca/index.html?asst_id=977>, at 6-7; Greg Ridgeway, "Policing in the Era of Big Data" (2018) 1 Annual Review of Criminology 401 at 402-03; and "3D Data Management: Controlling Data Volume, Velocity, and Variety", META Group (6 February 2001). <https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>.

107 It should be noted that a report by the United Kingdom Information Commissioner's Office states, "Recently, some have suggested that the three Vs definition has become tired through overuse and that there are multiple forms of big data that do not all share the same traits. While there is no unassailable single definition of big data, we think it is useful to regard it as data which, due to several varying characteristics, is difficult to analyse using traditional data analysis methods." "Big data, artificial intelligence, machine learning and data protection" (4 September 2017) United Kingdom Information Commissioner's Office, at 6 (footnotes omitted) <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>. While recognizing this, the "three Vs" characterization remains useful for the purposes of this report and distinguishing between conventional policing, big data policing, and algorithmic policing, in particular. See, e.g., Greg Ridgeway, "Policing in the Era of Big Data" (2018) 1 Annual Review of Criminology 401 at 402-03, describing the role of big data in policing based on these traits.

108 Upturn, *Stuck in a Pattern: Early evidence on "predictive policing" and civil rights* (August 2016) at 1 <https://www.upturn.org/static/reports/2016/stuck-in-a-pattern/files/Upturn_-_Stuck_In_a_Pattern_v.1.01.pdf>.

109 Interview of a representative for the Saskatchewan Police Predictive Analytics Lab by Cynthia Khoo (23 July 2019).

> 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.[110]

Transparency surrounding algorithmic policing technologies is also distinct from conventional and big data methods of policing. Algorithm-driven tools are often black boxes in a way that conventional tools are not. For example, actuarial risk assessments that social scientists have developed and validated have been used in the corrections and sentencing contexts for many years in Canada,[111] as well as in criminal justice systems in other jurisdictions,[112] albeit not without critique and controversy.[113] These assessments can be explained and assessed by social scientists, including what specific factors were included and how much weight was given to any particular factor. Machine-learning algorithms, on the other hand, may generate and follow rules that are indiscernible to human observers. As a result, humans may be unable to determine what factors are considered by a machine-learning algorithm or how they are weighted.[114] Even experts may be unable to parse the hundreds to thousands of steps in a particular algorithm or the multitude of data points that the algorithm uses to arrive at a particular outcome.[115] The outcome is that algorithmic policing technologies might use mathematical systems to come to conclusions that are utterly opaque to the developers of the systems, those tasked with using the output data in law enforcement and criminal justice, or those affected by the algorithmic policing technologies.

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

111 See, e.g., *Ewert v Canada*, 2018 SCC 30 at para 11.

112 Royal United Services Institute, *Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges* (September 2018) at 6 <https://rusi.org/sites/default/files/201809_whr_3-18_machine_learning_algorithms.pdf.pdf>.

113 See e.g., *Ewert v Canada*, 2018 SCC 30; Margaret Shaw & Kelly Hannah-Moffat, "Gender, Diversity And Risk Assessment In Canadian Corrections" (September 2000) 47:3 Probation Journal 163.

114 "More advanced algorithmic systems, which include machine learning approaches, are used with problems where pre-existing rules or theories do not capture the desired input-output relationships well. As a result, machines craft the relationship between inputs and outputs backwards from the data, usually without regard for human interpretability. In some cases, this can allow machines to make much more effective input-output connections – which computer scientists call predictions – than hand-crafted rule-based systems could." Michael Veale, "Algorithms in the Criminal Justice System" (June 2019), Law Society of England and Wales at 10 <https://www.lawsociety.org.uk/support-services/research-trends/algorithm-use-in-the-criminal-justice-system-report/>.

115 "[T]hese new systems go beyond simply helping human crime analysts digest data. They aim to automatically predict future crime to inform police decisions. To do so, these systems make judgments about what the data means — flagging people most likely to be involved in violent crime in the future, for instance, or weighing hundreds or thousands of factors in ways that no human analyst can fully grasp." Upturn, *Stuck in a Pattern: Early evidence on "predictive policing" and civil rights* (August 2016) at 2 <https://www.upturn.org/static/reports/2016/stuck-in-a-pattern/files/Upturn_-_Stuck_In_a_Pattern_v.1.01.pdf>.

# 4. Algorithmic Policing in Canada: The Current Landscape

Algorithmic policing technologies are present or under consideration throughout Canada in the forms of both predictive policing and algorithmic surveillance tools. Within the last decade, police services' strategic plans, budget documents, and annual reports have reflected plans to adopt algorithmic policing methods, under terms such as 'predictive', 'data-driven', or 'intelligence-led' policing, supported by greater emphasis on data analytics.[116] Some police services have begun to pilot and implement algorithmic policing systems,[117] or have expressed an interest during research interviews conducted for this report, which adds to growing interest among law enforcement generally.[118]

Part 4 of this report provides a factual overview of the Canadian algorithmic policing landscape. The research findings set out in this section were obtained using information gathered through desk research (including the integration of media reports), FOI requests, and formal research interviews. The representatives of Canadian law enforcement who were interviewed for this reported include: Ryan Prox, Special Constable in Charge (S/Constable), Crime Analytics Advisory & Development Unit, at the Vancouver Police Department; a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL); a member of law enforcement in Calgary, Alberta; and a law enforcement representative in Canada.

The following sections each review algorithmic policing initiatives and practices that have been undertaken by police services in Canada: location-focused algorithmic policing technologies (Section 4.1), person-focused algorithmic policing technologies (Section 4.2), and algorithmic police surveillance methods (Section 4.3). Section 4.4 discusses the limitations of the research findings, and Section 4.5 provides a summary and analysis of the research findings regarding the current landscape of algorithmic policing in Canada. This part of the report (Part 4) focuses on laying out the factual landscape as is, to the extent the authors could determine it; analysis and critical implications of these technologies are presented later in Part 5 ("International Human Rights and *Charter* Rights Implications of Algorithmic Policing").

116 See, e.g., Winnipeg Police Service 2011 Annual Report at page 9; London Police Service 2013 Annual Report at page 17, https://www.londonpolice.ca/en/About/resources/Documents/2013-Annual-Report.pdf; Peel Regional Police 2017 Budget Document at pages 4 and 11, https://www.peelpoliceboard.ca/en/board-meetings/resources/2017-Peel-Regional-Police-Budget.pdf; Ottawa Police Service June 2018 Modernization Roadmap Report at page 10, http://app05.ottawa.ca/sirepub/agdocs.aspx?doctype=agenda&itemid=375842; Edmonton Police Service 2018 Annual Policing Plan at pages 5 and 6, https://edmontonpolicecommission.com/wp-content/uploads/2019/03/2018-Annual-Policing-Plan.pdf.

117 Matt Meuse, "Vancouver police now using machine learning to prevent property crime" (22 July 2017) *CBC News* <https://www.cbc.ca/news/canada/british-columbia/vancouver-predictive-policing-1.4217111>; Meaghan Craig, "Saskatoon police lead the country with Predictive Analytics Lab" (15 January 2016) *Global News* <https://globalnews.ca/news/2455063/saskatoon-police-lead-the-country-with-predictive-analytics-lab/>.

118 See e.g., Peter Sloly, "Emerging tech that can make smart cities safer", *Blue Line* (8 October 2018) <https://www.blueline.ca/emerging-tech-that-can-make-smart-cities-safer-5710/>; Cory Schactel, "More Data, More Problems", *Avenue Magazine Edmonton* (5 June 2019) <https://www.avenueedmonton.com/innovation/more-data-more-problems/>; and Richard Boire, "Data-Driven Decisions for Law Enforcement in Toronto", *Machine Learning Times* (17 August 2018) <https://www.predictiveanalyticsworld.com/machinelearningtimes/data-driven-decisions-for-law-enforcement-in-toronto/9640/>.

In some instances, a given technology may be used for capabilities other than algorithmic predictions, such as organizing and linking data, without drawing algorithmic predictions based on the data. However, current possession of the capability by Canadian law enforcement is also considered relevant and within the scope of this report. Reference is made throughout each section to parallel examples in peer jurisdictions to further illustrate potential uses and risks of each technology in question.

To conclude this introduction of Part 4, the following highlight box, **In Focus #2: Overview of the Canadian Criminal Justice System**, provides information regarding the structure and process of the law enforcement and criminal justice system in Canada. This context helps to demonstrate where algorithmic policing technologies fit in within Canada's law enforcement and criminal justice system.

# Overview of the Canadian Criminal Justice System

In Canada's federal system of government, each level of government—federal, provincial /territorial, and municipal—has a role in the criminal justice system. The federal government is responsible for creating and reforming criminal law offences, which are set out in the *Criminal Code* and other federal statutes, such as the *Controlled Drugs and Substances Act*. The provinces have the authority to establish police forces, prosecution services, parole services, and other related agencies such as victims' compensation programs. With the consent of the provinces and territories, police services have developed through delegated authority in many municipalities across Canada (such as Vancouver, Calgary, and Toronto) and First Nations communities. Ontario and Quebec have province-wide police services (the Ontario Provincial Police and La Sûreté du Québec). The Royal Canadian Mounted Police (RCMP) is a national police service that serves the remaining areas that are not already policed by First Nations, provincial, or municipal police services. Where the RCMP operates, it does so by virtue of the delegated authority of the provincial or territorial government in that area.

Certain features of criminal investigations and criminal proceedings tend to be similar across Canada. These similarities arise, in part, because Canada has one set of criminal laws across the country and because all law enforcement authorities and Crown prosecutors must operate within the constitutional limits of the *Canadian Charter of Rights and Freedoms*.[119] However, even though much of the criminal justice system is the same across Canada, local or regional policy choices and resource constraints means that some police practices or the quality of access to justice may vary across Canada.

The main stages of criminal investigations and proceedings in Canada are as follows:

1. Police services investigate people by gathering information and evidence.
2. Police officers have limited powers to restrain the liberty of suspects during a criminal investigation (i.e., investigative detention and arrest powers). It is unlawful to exercise these powers in a manner that infringes on *Charter* rights.
3. After gathering available evidence, the police may lay a criminal charge (or charges) against the defendant if the investigating officer has reasonable and probable grounds to believe the individual committed an offence.
4. If a criminal charge is laid, it must be determined whether the accused will be released or detained in pretrial custody while the criminal charges work their way through the criminal court system (bail).

119 *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution Act*, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.

Depending on the circumstances (e.g., the nature of the offence or the accused's prior record), the accused is either released at the scene of the arrest by the arresting officer (e.g., at the side of the road), released from a police detachment (e.g., after being processed), released from a criminal court on bail by a justice of the peace or judge, or detained in custody by a criminal court judge pending trial.

5. Once charges are laid, criminal proceedings commence in court. Crown prosecutors take control of the case and receive evidence from the investigating police service.

6. All individuals before the courts are presumed innocent. Criminal proceedings come to a conclusion in the following ways: a) a withdrawal or stay of the charges by the Crown, b) participation by the defendant in a diversion program prior to a withdrawal or stay of the charge (stayed or withdrawn charges mean that the person is innocent of the charges), c) a guilty plea by the defendant and corresponding waiver of the right to a trial on the merits, or d) a criminal trial where the accused is presumed innocent and must be acquitted unless the prosecution proves guilt (of the charges laid) beyond a reasonable doubt before a judge or jury.

7. Criminal sentencing occurs if an individual is found guilty of an offence either as a result of pleading guilty or having been found guilty in a criminal trial.

8. A number of processes relating to any criminal sentence imposed may occur, including probation, imprisonment, and parole proceedings.

9. After a finding of guilt and sentencing, a defendant has rights of appeal with respect to the conviction and/or sentence imposed.

10. Following the completion of a criminal sentence, the Parole Board of Canada administers Canada's system of determining whether any criminal record suspension (formerly referred to as pardons) is available.[120]

Law enforcement actors investigate and gather evidence through a vast range of methods and processes. Some police investigations are reactive (e.g., responding to a 911 call) while others are pre-emptive and attempt to detect crime without an express request for help from the community. In order to build a criminal case, law enforcement authorities may rely on many different information sources such as witness statements, recorded conversations, (e.g., copies of text messages or emails, or an intercepted recording of a phone call), CCTV video footage, business records, or observations

120 A record suspension means that the individual's criminal record is removed from the national criminal record database, which would potentially assist the individual to find employment or education opportunities without a visible scar of a criminal conviction on their record.

by police officers—or data gathered through the algorithmic technologies examined in this report. All methods must occur within constitutional limits though, in practice, many investigations are ultimately found to be unconstitutional in one or more ways. The *Charter* provides a right to seek the exclusion of unconstitutionally obtained evidence.[121] However, data obtained and methods used by police may never be scrutinized by courts if information about those practices is never disclosed in criminal court cases or if the defendant does not have the financial ability to bring a *Charter* application.

While it is possible, in theory, for prosecution and law enforcement authorities to use algorithmic technologies at many stages of the criminal justice process—for example, algorithmic risk assessment technologies have been developed, adopted, or considered in the contexts of pretrial detention (bail), sentencing, parole, and corrections[122]—the technologies examined in this report are primarily linked to the initial information gathering and monitoring stage of police work.

121 *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution Act*, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11, s 24(2).

122 Section 4.2.3 ("Algorithmic Risk Assessments in the Criminal Justice System") below provides a brief overview of algorithmic risk assessment technologies.

# 4.1. Location-Focused Algorithmic Policing

Location-focused algorithmic policing systems purport to identify where and when potential criminal activity might occur. The algorithms that drive these systems examine patterns and correlations in historical police data to attempt to make predictions about the future. Law enforcement agencies may then decide to intervene to deter or detect criminal activity by taking actions like increased patrolling at the targeted locations.

Police services in North America have long used non-AI methods to try to determine crime "hot spots"—geographic areas that are perceived or assumed to have relatively high concentrations of crime.[123] Modern techniques continue this method by using algorithms to crunch extensive volumes of data and purportedly identify connections that would otherwise remain undetected by a human analyst.

Location-focused algorithmic policing technologies may take different variables into account. For example, PredPol, one of the most well-known examples of this technology and used by over 90 police departments in the United States,[124] relies on four data points for its algorithm: crime type, location, date, and time.[125] Other popular algorithmic policing software systems, such as HunchLab,[126] may use additional variables including the location and type of buildings (e.g., schools, churches, bars, or liquor stores) and census data.[127] The Risk Terrain Modelling product developed by the Rutgers University Center on Public Security relies on sets of factors, including the types of commercial establishments present in an area and more problematic factors (due to their association with discriminatory over-policing of marginalized communities), such as public calls of "disorder" and certain types of housing, to try to predict where crimes such as car theft and gun violence are likely to occur.[128]

123 Council of Canadian Academies, *Policing Canada in the 21st Century: New Policing for New Challenges* (Ottawa, 2014) at 23-24.

124 Caroline Haskins, "Dozens of Cities Have Secretly Experimented With Predictive Policing Software" (6 February 2019) *Vice*, <https://www.vice.com/en_us/article/d3m7jq/dozens-of-cities-have-secretly-experimented-with-predictive-policing-software>. In April 2020, one of the highest-profile and longest-standing examples of PredPol implementation, its use by the Los Angeles Police Department (LAPD), was shut down by the LAPD, ostensibly "not because of concerns that activists have raised but because of financial constraints due to COVID-19, the disease caused by the novel coronavirus". Caroline Haskins, "The Los Angeles Police Department Says It Is Dumping A Controversial Predictive Policing Tool", *BuzzFeed News* (21 April 2020) <https://www.buzzfeednews.com/article/carolinehaskins1/los-angeles-police-department-dumping-predpol-predictive>.

125 PredPol, "The Three Pillars of Predictive Policing", <https://www.predpol.com/law-enforcement>.

126 In 2018, HunchLab was acquired by ShotSpotter, a company that produces an algorithmic gunshot detection tool that was previously considered (and ultimately rejected) for adoption by the Toronto Police Service. "Shotspotter announces acquisition of HunchLab to Springboard into AI-Driven Analysis and Predictive Policing" (3 October 2018) <https://www.shotspotter.com/press-releases/shotspotter-announces-acquisition-of-hunchlab-to-springboard-into-ai-driven-analysis-and-predictive-policing/>; Jeff Gray, "Toronto police end ShotSpotter project over legal concerns", *Globe and Mail* (13 February 2019) <https://www.theglobeandmail.com/canada/toronto/article-toronto-police-end-shotspotter-project-over-legal-concerns/>.

127 Leslie Kennedy, Joel Caplan & Eric Piza, "A Multi-jurisdictional Test of Risk Terrain Modeling and a Place-based Evaluation of Environmental Risk-Based Patrol Deployment Strategies" (2015), Rutgers Center on Public Security, at <www.rutgerscps.org/uploads/2/7/3/7/27370595/nij6city_resultsexecsum_final.pdf>, cited in Andrew Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (New York: NYU Press, 2017) at 71-72.

128 *Ibid* at 67-68.

The remainder of this section will provide an overview of specific location-focused algorithmic policing technologies in use by Canadian police services, although a given technology may be used for capabilities other than algorithmic predictions (e.g., used for organizing data alone). Section 4.1.1. will discuss the GeoDASH Algorithmic Policing System implemented by the Vancouver Police Department, and Section 4.1.2. will discuss the Toronto Police Service's use of Environics Analytics, IBM's Cognos Analytics, and IBM's Statistical Package for the Social Sciences software.

### 4.1.1. Vancouver Police Department: GeoDASH Algorithmic Policing System

The Vancouver Police Department (VPD) uses a machine-learning location-focused algorithmic system and user interface known as GeoDASH. GeoDASH uses historical police data to try to predict where and when break-and-enter crimes are likely to occur. Specifically, the algorithms generate six location-based forecasts, at 24-hour intervals, for every 2-hour window between 7:00 a.m. and 6:59 a.m. the next day; each forecast is a 100-metre-square area or 500-metre-square area.[129] The GeoDASH algorithmic policing system—or 'GeoDASH APS', a term used for the purposes of this report[130]—is the first of its kind in Canada, and it was created through a three-way private-public undertaking between a consortium of academic researchers from a multitude of academic institutions in Canada and internationally, in-house staff at the VPD, and Latitude Geographics. The system underwent a six-month study from April 1 to September 30, 2016.[131] During the pilot study, the stakeholders tested predictions for residential break-and-enter offences. Following the conclusion of the pilot, the VPD announced in 2017 that GeoDASH would be formally implemented as a wider routine practice.[132]

The GeoDASH APS relies on four data inputs: type of crime, geographical coordinates, date, and time. The VPD provides the algorithms with data arising exclusively from cases that were triggered by a complaint from a civilian to police and excludes all police-initiated reports (according to S/Constable Ryan Prox, civilian reports of property crimes constitute approximately 90% of all property-crime data).[133] For example, if a police officer was on patrol and happened to witness a burglary taking place,

129 Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019); and Matt Meuse, "Vancouver police now using machine learning to prevent property crime," *CBC* (22 July 2017) <https://www.cbc.ca/news/canada/british-columbia/vancouver-predictive-policing-1.4217111>.

130 The VPD's algorithmic policing tool is commonly associated with its crime "hot-spot" mapping application, GeoDASH (Geographic Data Analysis and Statistics Hub). However, an interview clarified that GeoDASH refers to the user interface alone, which visualizes the algorithm's outputs, among other data, in a mapping application for users. The underlying algorithmic technology has no name. Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019). For ease of reference, this report will refer to the entire algorithmic policing system (the algorithmic technology combined with the GeoDASH interface that facilitates its use) as the GeoDASH algorithmic policing system ("GeoDASH APS"). "GeoDASH" will be reserved to refer to the user interface alone, to which the VPD is able to add a variety of software applications, only one of which is the predictive policing technology.

131 Vancouver Police Department, "Vancouver Police adopt new technology to predict property crime" (21 July 2017) <https://mediareleases.vpd.ca/2017/07/21/vancouver-police-adopt-new-technology-to-predict-property-crime/>.

132 Vancouver Police Department, "Vancouver Police adopt new technology to predict property crime" (21 July 2017) <https://mediareleases.vpd.ca/2017/07/21/vancouver-police-adopt-new-technology-to-predict-property-crime/>

133 Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019).

that incident would not form part of the training data given to the algorithms.[134] The purpose of this policy is to reduce both the risk and the perception that police bias influences the training data or algorithms.[135]

After the system identifies high-risk locations, uniformed officers in marked cars are assigned to patrol these areas in order to deter criminal activity. According to an internal document, these teams actively look for "suspicious activity during their patrols and will engage in proactive activities, such as monitoring laneways and identifying potential POIs [persons of interest] / Known Offenders entering into the area."[136] The VPD may also notify civilian neighbourhood block watches in forecasted residential areas and ask them to exercise extra vigilance in their areas during the relevant time periods.[137]

According to Prox, the predictive policing team at the VPD is heavily influenced by the General Data Protection Regulation (GDPR) and European privacy law, and is wary of predictive policing developments in the United States.[138] As such, the VPD has proactively taken measures to mitigate potential harm and discrimination from the GeoDASH APS. A unique feature of the VPD program is its use of "exclusionary zones", which take account of "sensitive areas" of the city that give rise to over-policing concerns, such as the Downtown Eastside (DTES) neighbourhood. If any of the forecasted high-risk locations fall within an exclusionary zone, it is automatically replaced with the location that is identified to have the next highest risk of break-and-enter activity. As a result, the predictive system does not send officers to these designated zones even if they are initially identified as "high risk" by the algorithms.

The DTES is currently the only exclusionary zone the VPD has identified, and it was marked as such from the beginning of the initiative.[139] The VPD also monitors for potential over-policing resulting from the GeoDASH APS in other communities, tracking and monitoring how often the GeoDASH APS deploys officers to any given neighbourhood in the City of Vancouver, with special attention to any areas considered "socioeconomically or culturally sensitive" (one example being the South Slope neighbourhood in Vancouver, which has a large Indo-Canadian community).[140] At time of writing, the VPD did not determine that they had found over-representation of particular neighbourhoods in any of the forecasted areas, and thus had not added any further exclusionary zones.[141]

134 *Ibid.*

135 I did not want to have any data that could be perceived as having police bias in terms of generating the calls. [...] Whether I believe it's true or not that that [preconceived notions of criminality predisposing police to deploy to certain areas, resulting in potential self-fulfilling prophecy] happens at the Vancouver Police, I didn't want the spectre that that could even be entering into the data bias. Based on that, I made a decision that we would only use public-initiated reported property crime." *Ibid.*

136 Vancouver Police Department, "Predictive Policing" (obtained through freedom of information request 18-3224A_2).

137 Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019).

138 *Ibid.*

139 *Ibid.*

140 *Ibid.*

141 *Ibid.*

Additionally, to remain alert to the possibility of algorithmically over-policing other communities, the VPD relies on meetings held every 3-4 months between the predictive policing unit and the community policing services unit.[142] At these meetings, the latter might communicate if there were concerned or at-risk communities not on the former's radar.[143] One example was the emergence of social housing initiatives in South Vancouver. The VPD worked with the City of Vancouver to identify the locations of those initiatives and related outreach programs, then monitored for overrepresentation of those areas within the GeoDASH APS forecasts (and had found no overrepresentation at the time of the interview).[144]

Another area that has been of concern when using the GeoDASH APS is location-based police stops and detention. Regarding the danger of algorithm-driven police stops and detentions, Prox stated, "In terms of training, we make it very clear that if the police officers are deployed at forecasted locations, you cannot use the forecasting system as grounds for a street check."[145] The VPD attempted to measure, during the predictive policing pilot study, if more street checks were occurring in GeoDASH APS forecasted boxes, compared to locations that were not within boxes. However, according to Prox, there was not enough data to support any meaningful metrics, due to a low total number of street checks within forecasted locations overall.[146]

### 4.1.2. Toronto Police Service: Environics Analytics and IBM "Crime Insight and Prevention" Software

There are indications that the Toronto Police Service (TPS) may be considering, or is interested in, developing a location-focused algorithmic program in the future. Since at least 2016, the TPS has collaborated with Environics Analytics. Environics Analytics is a firm that primarily provides data analytics services for business and marketing purposes[147] to "explore the use of data and technology in a more optimal alignment of police resources and crime."[148] In 2018, the Senior Vice President of Environics Analytics wrote that one of the goals of the collaboration was to develop algorithmic models that identify high crime areas.[149] According to Richard Boire, factors such as the previous year's crime rate, age, income, and dwelling types in a given geographical area are used to predict the

142 *Ibid.*

143 *Ibid.*

144 *Ibid.*

145 *Ibid.*

146 *Ibid.*

147 Environics Analytics, "How we help", <https://www.environicsanalytics.com/en-ca/how-we-help>. It offers a number of proprietary databases, including a database called CrimeStats, which uses statistics, demographics, and computer modelling to determine the likelihood of crime for any location in Canada, the US, and the UK.

148 Richard Boire, "Data-Driven Decisions for Law Enforcement in Toronto" (17 August 2018) *Predictive Analytics Times*, <https://www.predictiveanalyticsworld.com/patimes/data-driven-decisions-for-law-enforcement-in-toronto/9640/>.

149 *Ibid.*

level of crime in that area.[150] The algorithmic model informs the number of officers that the TPS assigns to an area in the next 12 months.[151]

However, in an interview, a law enforcement representative in Canada confirmed that the TPS does not currently engage in algorithmically driven predictive policing. The representative also stated that the TPS is mindful of related issues and does not intend to adopt such technology immediately, and to their knowledge, had not engaged with vendors to this end. The representative did indicate that the TPS was interested in using data to inform decisions about public safety concerns such as gun violence and property crime.[152]

In addition to Environics, the TPS has access to IBM's Cognos Analytics and SPSS (Statistical Package for the Social Sciences) software.[153] Both of these programs are part of IBM's "Crime Insight and Prevention solution", which uses data mining and location-focused predictive modeling. IBM states that these tools will allow law enforcement agencies to "anticipate incidents, profile crimes and criminals, improve solved crime rates, and optimize resources use".[154] Cognos is a data analytics tool that uses AI and machine learning to discover patterns and translate data analysis into plain language.[155] SPSS offers advanced statistical analysis and algorithmic analytics functions.[156] While these programs offer algorithmically powered predictive policing capabilities, the TPS has stated that it is not using them for predictive purposes; instead, they use them for reporting and statistical insights.[157] Full use of these programs' capabilities for algorithms and automation are not in place at least in part because of the Service's resource limitations, according to the law enforcement representative interviewed.[158] The TPS has also stated that it would require alignment with provincial and/or federal governance strategies in order to consider implementing a predictive policing program.[159]

## 4.2. Person-Focused Algorithmic Policing

Person-focused algorithmic policing systems are ostensibly designed to identify individuals who are likely to be involved in future criminal activity, or they are designed to assess what level of risk a particular individual has for either engaging in or being the victim of future criminal activity. Such algorithmic assessments do not rely primarily on environmental factors or geographical crime data, as

150 *Ibid.*

151 *Ibid.*

152 Interview of a law enforcement representative in Canada by Yolanda Song & Cynthia Khoo (28 June 2019).

153 *Ibid.*

154 IBM Software Group, "Crime prediction and prevention: A safer public through advanced analytics" (June 2010) IBM Software Group White Paper, 4.

155 IBM, "IBM Cognos Analytics", <https://www.ibm.com/ca-en/marketplace/business-intelligence>.

156 IBM, "IBM SPSS software", <https://www.ibm.com/analytics/spss-statistics-software>.

157 Interview of a law enforcement representative in Canada by Yolanda Song & Cynthia Khoo (28 June 2019).

158 *Ibid.*

159 *Ibid.*

in the case of location-focused policing; instead, they process personal details, such as information about family, friends, or associates; their social media activity; criminal records; or appearance in other police databases, that are associated with a specific individual.[160] These factors are used as input data for a person-focused algorithmic policing tool, which then provides the output data of a 'risk score' for a given individual. The risk score is intended to reflect the predicted likelihood that the individual will commit or be involved in criminal activity in the future, or within a given time frame.[161]

Law enforcement agencies may act on these algorithmic predictions in a number of ways, including targeting identified individuals for increased monitoring or contacting identified individuals ostensibly to deter them from any criminal activity that the algorithm has predicted they may engage in—regardless of whether the individual was, in fact, going to engage in criminal activity. Where an individual is forecast to be at risk for criminal involvement or for harm by criminal activity, but not necessarily perpetrating it, police services may instead connect them with social services. The result of person-focused algorithmic policing systems is that individuals are potentially brought into contact with the criminal justice system on the basis of inaccurate, unreliable, or biased technology. Police services may rely on algorithmic predictions to interfere with an individual's right to privacy or liberty, for example, but the individual has few to no safeguards in place to prevent the violation of their constitutional or human rights.[162]

Person-focused algorithmic policing systems in various cities in the United States have been in place for years and use different methods of data analysis. For example, starting in 2012 the Chicago Police Department (CPD) maintained a Strategic Subjects List (SSL, colloquially referred to as the "heat list") of individuals who were purportedly at risk of being a perpetrator or victim of gun violence.[163] The heat list used an algorithm that examined 11 variables that reportedly included prior criminal history, parole status, and police notations on purported gang membership;[164] arrest data that was used by the CPD to create SSL risk scores was provided in a publicly available data portal.[165] In January 2020, the CPD decommissioned the use of the program for reasons that included the lack of reliability of the model.[166]

160 Andrew G Ferguson, "Policing Predictive Policing" (2017) 94:5 Washington University Law Review 1109 at 1137-42.

161 See e.g., "The information displayed represents a de-identified listing of arrest data from August 1, 2012 to July 31, 2016, that is used by the Chicago Police Department's Strategic Subject Algorithm ... to create a risk assessment score known as the Strategic Subject List or 'SSL.' These scores reflect an individual's probability of being involved in a shooting incident either as a victim or an offender. Scores are calculated and placed on a scale ranging from 0 (extremely low risk) to 500 (extremely high risk). Based on this time frame's version of the Strategic Subject Algorithm, individuals with criminal records are ranked using eight attributes, not including race or sex." "Strategic Subject List" (7 December 2017) Chicago Data Portal <https://data.cityofchicago.org/Public-Safety/Strategic-Subject-List/4aki-r3np>.

162 These points will be expanded on in more detail in Part 5 ("International Human Rights and *Charter* Rights Implications of Algorithmic Policing") of the report.

163 Andrew Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (New York: NYU Press, 2017) at 46.

164 *Ibid* at 46-49. As noted in Section 2.2 ("Bias and Inaccuracies in Police Data") of this report, factors such as "gang membership" can be highly discretionary and prone to error and discriminatory bias.

165 "Strategic Subject List" (7 December 2017) Chicago Data Portal <https://data.cityofchicago.org/Public-Safety/Strategic-Subject-List/4aki-r3np>. Another well-known predictive policing program that was later shut down, Operation LASER, by the Los Angeles Police Department, is discussed below in Section 4.2.1 ("Calgary Police Service: Palantir Gotham and IBM i2 Analyst Notebook").

166 Sam Charles, "CPD decommissions 'Strategic Subject List'", *Chicago Sun Times* (27 January 2020), <https://chicago.suntimes.com/city-hall/2020/1/27/21084030/chicago-police-strategic-subject-list-party-to-violence-inspector-general-joe-ferguson>.

In New Orleans, the police department used software developed by Palantir Technologies to identify individuals at risk of being perpetrators or victims of violence by analyzing their associations using a method known as social network analysis (SNA).[167] The Palantir software integrated separate city databases into unified systems and identified hidden relationships in the data held within those databases.[168]

Some law enforcement actors in Canada have expressed less enthusiasm for person-focused approaches to algorithmic policing compared to location-focused approaches. S/Constable Ryan Prox of the VPD stated that person-based forecasting for criminal activity is "too high risk" and that "ethically, it would be reprehensible to move in that direction."[169] Prox was specifically concerned with person-focused predictive policing programs seen in Los Angeles, New Orleans, and Chicago, making the following observation regarding their potential impact on affected communities in the United States: "If you have an ethnically biased algorithm, you could then convert a community into a police state where you have such overrepresentation of police resources, in a very confined geospatial area, that overrepresentation of police resources could transform a community into…akin to almost being under siege."[170]

The remainder of this section will provide an overview of specific person-focused algorithmic policing technologies in use, under development, or possessed by Canadian police services. Section 4.2.1. will discuss the Calgary Police Service's use of software by Palantir Technologies and the IBM i2 Analyst Notebook, the latter of which is used for algorithmic social network analysis. Section 4.2.2 will discuss the algorithmic policing technology being developed in-house at the Saskatchewan Police Predictive Analytics Lab (SPPAL). Section 4.2.3 will briefly note the use of algorithmic risk assessment tools throughout other stages of the criminal justice system, including for bail, sentencing, and parole.

### 4.2.1. Calgary Police Service: Palantir Gotham and IBM i2 Analyst Notebook

At the end of 2012, the Calgary Police Service (CPS) acquired a software licence from Palantir Technologies for $1.4 million.[171] The CPS currently uses the 2018 version of Palantir's Gotham product[172]

167 Social network analysis (SNA) "is based on the premise that the relationships between individuals can inform and even predict an individual's behavior" and is used in policing to "analyze the capacities of criminal networks, how such networks affect criminal activities, and the diffusion of violent crime within a community or across a population." See Andrew Papachristos & Michael Sierra-Arévalo, "Policing the Connected World" (2018) *Office of Community Oriented Policing Services,* at viii <https://cops.usdoj.gov/RIC/Publications/cops-w0859-pub.pdf>. SNA in Canada is discussed below in Section 4.3 ("Algorithmic Surveillance Tools").

168 Andrew Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (New York: NYU Press, 2017) at 49-51.

169 Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019).

170 *Ibid.*

171 City of Calgary, "Purchase Order" (obtained through freedom of information request 2018-G-0203).

172 Calgary Police Service, "Transition from Palantir 2012 to PG2018" (obtained through freedom of information request 18-G-0814).

to integrate its various internal data sources into one unified system for data access and analysis.[173] Documents prepared by Palantir and the CPS indicate that open source information (e.g., publicly available social media and other online content), email and telecommunications information, and third-party commercial information (e.g., financial records and credit history) can also be incorporated into the system.[174] However, a law enforcement member in Calgary reported that the CPS uses Palantir to integrate certain internal files, data about dispatch calls, and its Niche record management system (RMS). The Niche system contains some of the CPS's previously siloed data sources, such as information about frequent offenders.[175]

According to CPS records that were released through an FOI request, Palantir Gotham enables authorized CPS users to search through integrated data to detect and visualize associations between individuals, organizations, locations, police incident reports, checkups (similar to street check or carding data), properties, and vehicles.[176] The associations and connections generated by Palantir are used to inform officers' and analysts' understanding of individuals' relationships and behaviours.[177]

According to a 2014 draft Privacy Impact Assessment (PIA) conducted by the CPS, information about physical characteristics, relationships, interactions with police, and "possible involved activities" (an open-ended and undefined category of input) is stored for all individuals who interact with the police, including victims and witnesses. For individuals who are suspected to have committed an offense, further data, such as data about their religious affiliations, is collected.[178] The CPS also uses Palantir to map out where crimes and calls for service are taking place.[179]

The CPS recognized in its draft PIA that assessments using the Palantir system could present false associations between innocent individuals and criminal organizations and suspects.[180] The draft PIA proposed measures meant to mitigate such risks, including establishment of data entry rules, reliance on the software's audit capabilities that enable tracking changes made to the data, and use of a data-modelling feature that purportedly allows analysts to avoid drawing incorrect associations.[181] At least one major element of the accountability framework set out in the draft PIA, the Palantir Platform

173 Calgary Police Service, "Calgary Police Service Palantir Implementation Privacy Impact Assessment: June 1, 2014 Draft" at 9, (obtained through freedom of information request 18-G-1921).

174 *Ibid* at 15, 47; Palantir, "Palantir Platform Capabilities Brief" (11 October 2012), presentation to Calgary Police Service (obtained through freedom of information request 18-G-1921).

175 Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).

176 Calgary Police Service, "Transition from Palantir 2012 to PG2018" (obtained through freedom of information request 18-G-0814).

177 Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).

178 Calgary Police Service, "Calgary Police Service Palantir Implementation Privacy Impact Assessment: June 1, 2014 Draft" at 29-30, (obtained through freedom of information request 18-G-1921).

179 Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).

180 Calgary Police Service, "Calgary Police Service Palantir Implementation Privacy Impact Assessment: June 1, 2014 Draft" at 35, (obtained through freedom of information request 18-G-1921).

181 *Ibid*.

Governance Entity, is not currently in operation.[182] The Palantir Platform Governance Entity was intended to be responsible for overseeing data quality processes, implementing new features and data sources for the Palantir system, and periodically reviewing privacy implications.[183] According to a member of law enforcement in Calgary, an Information Management Working Group is in place to review proposed changes to any of the agency's systems, including the data management consequences of such changes, and an Information Management Steering Committee oversees the working group to provide strategic guidance and oversight.[184] However, the CPS did not disclose any final or formalized policies or guidelines for the use of Palantir software in response to an FOI request that was submitted to obtain information on their use of Palantir systems.

Where Palantir technology has been deployed in the United States, the software has been used to facilitate high-profile and controversial initiatives. In Los Angeles, as part of the LAPD's Los Angeles Strategic Extraction and Restoration ("Operation LASER") program, Palantir technology has reportedly been used to integrate and analyze data from various local, statewide, and national law enforcement sources, as well as non-law enforcement data about social services, health services, foreclosures, social media, utility bills, and even phone records from pizza chains.[185] The resulting inferences are used to identify zones that forecast hotspots for gun-related crime. Persons deemed to be "Chronic Offenders" are also targeted in order to track their movements and activity, to notify the targeted individual that they are being watched in an attempt to deter potential criminal activity, or to remove the individual from an area or neighbourhood.[186] These programs have been met with significant community backlash and opposition[187] as well as criticism from the Inspector General of the Los Angeles Police Department (LAPD), whose office identified serious problems with the LAPD's data practices and oversight mechanisms.[188] The Inspector General recommended that the program be curtailed, limiting the broad exercise of police discretion with respect to labelling individuals as chronic offenders, and that the program should generally be subject to a number of oversight, transparency, and due process mechanisms.[189] The LAPD shut down Operation LASER in April 2019, after a meeting where "members of the department's civilian oversight panel questioned the effectiveness" of the program's algorithmic policing methods.[190]

182 Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).

183 Calgary Police Service, "Calgary Police Service Palantir Implementation Privacy Impact Assessment: June 1, 2014 Draft" at 20, (obtained through freedom of information request 18-G-1921).

184 Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).

185 Andrew Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (New York: NYU Press, 2017) at 9, 99-100; Mark Smith, "Review of Selected Los Angeles Police Department Data-Driven Policing Strategies" (12 March 2019) Los Angeles Police Commission Inspector General, at 5 <http://www.lapdpolicecom.lacity.org/031219/BPC_19-0072.pdf>.

186 Mark Smith, "Review of Selected Los Angeles Police Department Data-Driven Policing Strategies" (12 March 2019) Los Angeles Police Commission Inspector General, at 5-9 <http://www.lapdpolicecom.lacity.org/031219/BPC_19-0072.pdf>.

187 Stop LAPD Spying Coalition, "Before the Bullet Hits the Body: Dismantling Predictive Policing in Los Angeles" (8 May 2018), <https://stoplapdspying.org/wp-content/uploads/2018/05/Before-the-Bullet-Hits-the-Body-May-8-2018.pdf>.

188 Mark Smith, "Review of Selected Los Angeles Police Department Data-Driven Policing Strategies" (12 March 2019) Los Angeles Police Commission Inspector General, at 5-9 <http://www.lapdpolicecom.lacity.org/031219/BPC_19-0072.pdf>.

189 *Ibid.*

190 Mark Puente, "LAPD ends another data-driven crime program touted to target violent offenders", (12 April 2019) *Los Angeles Times,*

As noted above, the CPS is not currently using Palantir technology for its algorithmic policing capabilities such as those the LAPD has relied on. The CPS relies on Palantir's software to integrate and organize data, rather than draw algorithmic inferences or predictions from it. However, this does not necessarily mean that the CPS will never begin to use Palantir's algorithmic policing features in the future.

In addition, the CPS does engage in algorithmic social network analysis, through a combination of Palantir and IBM's i2 Analyst Notebook. Palantir is used to link and build networks that draw relationships between data in the CPS's own databases, such as data stored in the Niche records management system. Specifically, in Palantir, "[p]ersons are linked together based on an event that has occurred or been recorded in [the CPS's] system." The relational network built in Palantir is then imported into the IBM i2 Analyst Notebook, which contains a built-in social network analysis tool. This tool ranks central actors and key players within a particular social network, based on metrics such as "betweenness, closeness, degree, and eigenvector (hub and authority) centrality measures".[191]

Recent reports suggest that Palantir has been seeking to expand the use of its technology in Canada generally, which may increase the uptake of its algorithmic policing capabilities by law enforcement agencies across the country. In August 2019, Canada's former ambassador to the United States, David MacNaughton, resigned from his position as Ambassador in order to be appointed head of Palantir's Canadian operations out of headquarters based in Ottawa.[192] MacNaughton then announced, in April 2020, that Palantir has been in dialogue with the federal government and with the governments of Ontario, Alberta, and British Columbia regarding their responses to the COVID-19 pandemic.[193]

Palantir's decision to expand into Ottawa may, in part, be influenced by Canadian privacy laws that reduce the company's ability to obtain Canadian law enforcement authorities as clients while operating out of the United States. Generally speaking, law enforcement authorities are bound by privacy legislation and privacy obligations under the *Charter*, which limit the circumstances under which law enforcement actors are permitted to transmit or store an individual's personal data extraterritorially.[194] Palantir's technology may necessitate data-sharing with the company for certain functions. In a contract with the City of New Orleans, the City was supposed to provide Palantir with access to all "data and records sources" that the City wanted analyzed in Palantir's "integrated analytical

---

<https://www.latimes.com/local/lanow/la-me-laser-lapd-crime-data-program-20190412-story.html>.

191 Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019); and Pak Chung Wong, et al, "Visual Matrix Clustering of Social Networks" (2013) 33:4 IEEE Computer Graphics and Applications 88 at 90.

192 Justin Ling, "Palantir's big push into Canada," OpenCanada.org, Centre for International Governance Innovation (25 October 2019), <https://www.opencanada.org/features/palantirs-big-push-into-canada/>.

193 Murad Hemmadi, "Palantir's MacNaughton says data-mining firm is working with Ottawa, three provinces on COVID-19," The Logic (30 April 2020), <https://thelogic.co/news/exclusive/palantirs-macnaughton-says-data-mining-firm-is-working-with-ottawa-three-provinces-on-covid-19/>.

194 *Wakeling v United States of America*, 2014 SCC 72. Some provinces have data localization obligations applicable to public agencies (*Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, s 30.1; *Personal Information International Disclosure Protection Act*, SNS 2006, c 3, ss 9(2)(d), 9(3)(b)), or other barriers to the disclosure of private data outside of Canada's borders. For example, Alberta's privacy legislation applicable to public sector agencies such as the CPS (the Freedom of Information and Protection of Privacy Act) does not appear to authorize the disclosure of data by law enforcement authorities to private companies at all, and Section 40 of the Act permits disclosure to law enforcement agencies in foreign countries only "under an arrangement, written agreement, treaty or legislative authority".

environment."[195] Given that Palantir may require its customers to provide the company with direct access to any data that is subject to algorithmic analysis, Palantir's expansion of operations inside Canada's borders may be an effort to enable or encourage greater adoption of its technologies among Caandian law enforcement agencies, by reducing the risk of violating data localization laws.

### 4.2.2. Saskatchewan Police Predictive Analytics Lab (SPPAL)

In November 2015, the Saskatoon Police Service (SPS) partnered with the University of Saskatchewan and the Government of Saskatchewan to form the Saskatchewan Police Predictive Analytics Lab (SPPAL), which is housed at SPS headquarters.[196] The SPPAL is intended to address a number of areas of crime and community safety issues, beginning with a project focused on missing persons. By examining risk factors and behaviour patterns among missing youth in Saskatchewan, the SPPAL is developing a preliminary algorithmic model to identify children and youth who are at risk of going missing.[197] Once implemented, the model will be shared with social service partners, though in some cases it has been shared already, for testing purposes.[198]

The SPPAL has been working with municipal police data from the SPS alone, to the authors' knowledge as of February 14, 2020, though an agreement with the Saskatchewan Association of Chiefs of Police will provide the Predictive Analytics Lab with access to data from all municipal police services in the province and data from the RCMP "F" Division.[199] The SPPAL has also expressed its intention to eventually include social media data in the training and development of its models.[200] An interview with a representative from the SPPAL made clear that the project is still in early stages and that the SPPAL is considering multiple options for data management and data sharing with municipal police agencies, with particular concern for security capabilities such as keeping collected data confidential and encrypted.[201]

195 "License and Services Agreement," entered into as of February 23, 2012 by Palantir Technologies Inc. and the City of New Orleans, <https://www.documentcloud.org/documents/4344821-K12-168-Palantir-Technologies.html>.

196 Meaghan Craig, "Saskatoon police lead the country with Predictive Analytics Lab" (15 January 2016) *Global News* <https://globalnews.ca/news/2455063/saskatoon-police-lead-the-country-with-predictive-analytics-lab/>. Notably, the SPPAL representative explained that the project was housed within the SPS by virtue of that agency already having the infrastructure and institutional resources to support the required level of security and other technical and organizational demands. Additional reasons were that police are usually the department that receives missing person calls—the focus of the SPPAL's inaugural project—and the involvement of officers who have already sworn an oath. However, the representative suggested that provided sufficient funding, resources, and infrastructure were available, a project such as the Predictive Analytics Lab could equally be established as a "Community Solutions Lab", independent of police services. Interview of a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) by Cynthia Khoo (23 July 2019).

197 Amelia Thatcher, "Stopping crime - by the numbers" (3 October 2016) 78:2 *Gazette* <http://www.rcmp-grc.gc.ca/en/gazette/stopping-crime-the-numbers>.

198 Interview of a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) by Cynthia Khoo (23 July 2019). In these cases, the SPPAL's algorithmic model has been shared with social service agencies, which tested the model in-house on their own data and provided the SPPAL with feedback. This prevented social services data from having to be shared with the SPPAL or the SPS at this stage for testing purposes.

199 *Ibid.*

200 *Ibid.*

201 *Ibid.*

The work the SPPAL is engaged in has been described as an extension of the "Hub model" of tracking risk.[202] This model involves systematic information sharing between social service agencies and law enforcement actors in order to monitor and flag individuals or communities that are considered to be marginalized and at risk.[203] One of the key goals of the SPPAL is to predict risk and intervene at an earlier stage in an individual's life, before they get to the point where someone would bring their case to a Hub program.[204] A representative from SPPAL advised that, following deployment, the missing persons algorithmic model would be evaluated using methods developed by partners at the University of Saskatchewan.[205]

The SPPAL's current project is unique in that it claims to focus on preemptively identifying potential victims or those who may cause harm to themselves. These assessments are conducted using risk/need analysis and prevention strategies as opposed to predicting potential perpetrators as has been the case with the person-focused algorithmic policing programs in Chicago, New Orleans, and Los Angeles. However, the SPPAL intends to expand the scope of its algorithmic work to address other safety concerns and community issues such as repeat and violent offenders, domestic violence, the opioid crisis, and individuals with mental illness who have come into conflict with the criminal justice system.[206] According to the SPPAL representative who was interviewed for this report, "We're selecting complex problems where we feel like we can impact people who are vulnerable, to help them be safe, helping our communities be safe."[207]

### 4.2.3. Algorithmic Risk Assessments in the Criminal Justice System

Many person-focused algorithmic policing technologies take the form of algorithmic risk assessments. Such assessments purport to calculate a person's level of ostensible risk, such as whether they are at high or low risk of violence or of reoffending. For example, in the United Kingdom, the Durham Constabulary uses the Harm Assessment Risk Tool (HART) to predict whether detained individuals are at low, moderate, or high risk of offending within a two-year period. The prediction is then used to influence officers' decision whether to initiate a prosecution by laying charges against the individual in question, or instead refer the individual to a diversionary scheme involving an out-of-court rehabilitation

202 For an explanation of the Hub model in relation to algorithmic policing, see IN FOCUS #3: The Hub Model of Community Safety.

203 Abeba Taddese, "Saskatchewan, Canada: The Hub Model for Community Safety" Results for America, <http://results4america.org/wp-content/uploads/2017/07/LandscapeCS_Canada_4.pdf>; Nathan Munn, "Police in Canada Are Tracking people's 'Negative' Behavior In a 'Risk' Database" (27 February 2019) Vice <https://www.vice.com/en_us/article/kzdp5v/police-in-canada-are-tracking-peoples-negative-behavior-in-a-risk-database>.

204 Interview of a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) by Cynthia Khoo (23 July 2019).

205 *Ibid.*

206 "Saskatoon police analytics lab will try to predict crime before it happens," *CBC News* (14 January 2016) <https://www.cbc.ca/news/canada/saskatoon/saskatoon-police-analytics-lab-will-try-to-predict-crime-before-it-happens-1.3403632>; Meaghan Craig, "Saskatoon police lead the country with Predictive Analytics Lab" (15 January 2016) *Global News* <https://globalnews.ca/news/2455063/saskatoon-police-lead-the-country-with-predictive-analytics-lab/>; Interview.

207 Interview of a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) by Cynthia Khoo (23 July 2019).

program. The HART model considers factors related to the individual's offending behaviour, as well as age, gender, postcode, and intelligence reports.[208]

Person-focused algorithmic risk assessments can also be used elsewhere in the criminal justice system. While this report focuses specifically on the policing context, it is important to flag the algorithmic prediction systems at play in the pretrial (bail), sentencing, and corrections stages of the criminal justice system.[209]

> *What's the definition of "at risk" and how do we label people who are at risk, and what definition of the idealized citizen are we operating on?*
>
> *- Black Legal Action Centre (BLAC)*[210]

Algorithmic risk assessment tools are used throughout the United States in pretrial proceedings regarding bail and post-trial proceedings regarding sentencing and parole. Canadian researchers, government agencies, and startup companies have begun considering algorithmic risk assessment instruments in bail as well.[211] The Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) tool is widely used across the United States to assess a defendant's risk of reoffending for the purposes of informing pretrial detention, sentencing, and parole decisions.[212] The algorithm(s) underlying COMPAS is proprietary and not disclosed to defendants or their lawyers. It is reportedly derived from a set of 137 questions that are answered by the defendant or pulled from police data.[213] The survey includes questions about the criminal records and behaviours of the defendant's family and friends as well as questions related to the defendant's education level and employment.[214]

208 Hannah Couchman, "Policing by Machine: Predictive policing and the threat to our rights," (January 2019) Liberty, at 50-51 <https://www.libertyhumanrights.org.uk/sites/default/files/LIB%2011%20Predictive%20Policing%20Report%20WEB.pdf>. The tool has received criticism for its consideration of postal code data, which may act as proxies for race and thereby lead to racially discriminatory results. See also Matt Burgess, "UK police are using AI to inform custodial decisions - but it could be discriminating against the poor", (1 March 2018) *Wired* <https://www.wired.co.uk/article/police-ai-uk-durham-hart-checkpoint-algorithm-edit>.

209 See e.g., Tom Simonite, "Algorithms Were Supposed to Fix the Bail System. They Haven't," *Wired* (19 February 2020) <https://www.wired.com/story/algorithms-supposed-fix-bail-system-they-havent/>; Ashley Mullen, "Incarceration or E-Carceration: California's SB 20 Bail Reform and the Potential Pitfalls for Pretrial Detainees" (2018) 104 Cornell Law Review 1867; Alicia Solow-Niederman, YooJung Choi & Guy Van den Broeck, "The Institutional Life of Algorithmic Risk Assessment" (2019) 34 Berkeley Technology Law Journal 705; and Carolyn McKay, "Predicting risk in criminal procedure: actuarial tools, algorithms, AI and judicial decision-making" (2020) 32:1 Current Issues in Criminal Justice 22.

210 Interview of Black Legal Action Centre by Cynthia Khoo (12 July 2019).

211 See e.g., Alyshah Hasham, "Soon, intelligent machines could help decide whether to keep people in jail. It's time to prepare," *Toronto Star* (19 July 2019) <https://www.thestar.com/news/gta/2019/07/19/soon-intelligent-machines-could-help-decide-whether-to-keep-people-in-jail-its-time-to-prepare.html>; and Agnese Smith, "Automating Justice" (13 March 2018) *CBA National*, <https://nationalmagazine.ca/en-ca/articles/law/ethics/2018/automating-justice>.

212 Julia Angwin et al., "Machine Bias" (23 May 2016) *ProPublica*, <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>.

213 *Ibid.*

214 An investigation by ProPublica found that COMPAS produced disparate results for different racial groups, with Black defendants being more

Multiple studies in Saskatchewan have investigated algorithmic pretrial risk assessment methods with respect to pretrial detention and sentencing, with researchers noting that no such models have been deployed or validated in the Canadian context.[215] The Ontario government has also begun to explore the use of a risk assessment tool similar to the COMPAS in pretrial detention decisions, and it has previously completed a feasibility study of such tools.[216]

In the corrections context, researchers at the University of Saskatchewan are conducting a machine-learning project based on, and envisioned to replace, the Level Service Inventory - Ontario Revised (LSI-OR).[217] The LSI-OR is an instrument that is used to carry out risk and needs assessments every six months for "all adult inmates undergoing any institutional classification or release decision, for all young offenders both in secure and open custody and for all probationers and parolees."[218] If this technology is adopted, it will serve as the first example in Canada of an algorithmic technology used in the corrections context to directly affect decisions about the liberty of individuals.

---

likely to be falsely labelled high risk than white defendants, while white defendants were more likely to be falsely labelled low risk: *Ibid*. While *ProPublica*'s characterization of the algorithm as racially biased was challenged by the developer and by a group of criminologists, the fact remains that Black defendants are more likely to bear the cost of the algorithm's inaccuracies than are white defendants. See Northpointe Inc., "COMPAS Risk Scales: Demonstrating Accuracy Equity and Predictive Parity", (8 July 2016) <https://www.documentcloud.org/documents/2998391-ProPublica-Commentary-Final-070616.html>; Anthony Flores et al., "False Positives, False Negatives, and False Analyses: A Rejoinder to 'Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And it's Biased Against Blacks.'" (September 2016) 80:2 Federal Probation 38 <https://www.uscourts.gov/sites/default/files/80_2_6_0.pdf>; Matthias Spielkamp, "Inspecting Algorithms for Bias" (12 June 2017) *MIT Technology Review*, <https://www.technologyreview.com/s/607955/inspecting-algorithms-for-bias>.

215 John-Etienne Myburgh, Carolyn Camman & J. Stephen Wormith, "Review of Pretrial Risk Assessment and Factors: Predicting Pretrial Release Failure" (November 2015) *University of Saskatchewan*, at 49 <https://cfbsjs.usask.ca/documents/research/research_papers/ReviewOfPTRAandRiskFactorsPredictingPretrialReleaseFailure.pdf>.

216 Agnese Smith, "Automating Justice" (13 March 2018) *CBA National*, <https://nationalmagazine.ca/en-ca/articles/law/ethics/2018/automating-justice>.

217 The Centre for Forensic Behavioural Science and Justice Studies, "Current Projects", *University of Saskatchewan*, <https://cfbsjs.usask.ca/research/current-projects.php>.

218 *Ibid*.

# The Hub Model of Community Safety

The Hub model is a form of person-focused risk forecasting that has been adopted by a number of Canadian government agencies. This type of program is known by various names, most commonly the "Hub model"[219] (in Saskatchewan) or "situation tables" (in Ontario) and is described as follows:

> Situation Tables offer a venue for service providers from various sectors (police, education, addictions, social work, mental health, etc.) to regularly convene and discuss clients who meet a defined threshold of risk. The intent of these discussions is to formulate a plan of intervention that mobilizes multiple sectors, collaborating to provide services and support to the individual or families. In order to mitigate risk before harm occurs, Situation Tables aim to connect clients to services within 24 to 48 hours of a case being presented to the group.[220]

Situation tables are intended to facilitate ameliorative responses to those deemed at risk as well as to gain efficiencies by integrating public service silos, so persons in need do not fall into the cracks between different government agencies. There were approximately 100 situation tables across Canada as of 2016.[221] The number of agencies, ministries, and organizations discussing and sharing sensitive information about a particular person or family can vary. One hub in Prince Albert, Saskatchewan involves at least thirteen[222] while the "connectivity tables" in Waterloo, Ontario feature up to thirty.[223]

This widespread adoption of the Hub model is noteworthy because it relies on a distinctive system of information sharing between law enforcement actors and other public sector services. The Hub model is not included as an example of algorithmic policing technology *per se* because it remains unclear whether the methodology adopted in the model relies on algorithms when the agencies involved are determining risk levels for a given individual or family. Nevertheless, the potential use of Hub model data in algorithmic policing methods was recognized by Public Safety Canada in 2015 when it reported that "[i]ntegrated health, social services, education and criminal justice data analysis will help to identify and plan predictive risk patterns at local, regional and provincial levels".[224] In 2019, *VICE Motherboard*

219 Abeba Taddese, "Saskatchewan, Canada: The Hub Model for Community Safety" *Results for America*, <http://results4america.org/wp-content/uploads/2017/07/LandscapeCS_Canada_4.pdf>.

220 Correctional Service Canada, "Success in Reintegration: The Potential Application of Situation Tables to Community Corrections" (July 2017), <https://www.csc-scc.gc.ca/research/rr-17-02-eng.shtml> (citations omitted).

221 *Ibid*.

222 Prince Albert Community Mobilization, "CMPA Team", <https://www.srsd119.ca/departments/teacherinformation/SSS/community_resources/Tri%20Fold%20Brochure%20Prince%20Albert%20Community%20Mobilization.pdf>.

223 Carizon, Langs & Taylor Newberry Consulting, "An Evaluation of Connectivity Tables in Waterloo Region" (2017) at 1, <https://www.langs.org/about-us/publications-and-reports/connectivity-evaluation-sheet-2017.pdf>.

224 Public Safety Canada, "Economics of Policing and Community Safety: Policy Makers' Dialogue on Privacy and Information Sharing" (January 2015) at 13 <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2015-plcy-mdps/2015-plcy-mdps-eng.pdf>. The report also notes, "The identification of recurring issues has led the province [Saskatchewan] to advance the establishment of more Centres of Responsibility (COR) in order to continue the multi-sector work toward systemic change and wider applications of predictive analytics." *Ibid*, at 23. While the previous COR in Prince Albert, SK, has been shut down, "the provincial government will look to implement a COR model within the Ministry of Corrections and Policing that will work with all 15 Hubs across the province." Peter Lozinski, "Centre of responsibility ceasing operations", Prince Albert Daily

reported that sensitive information had been collected into Risk-driven Tracking Databases (RTDs) in Ontario and Saskatchewan in order to generate individual and community risk profiles.[225] According to the former Ministry of Community Safety and Correctional Services (now the Ministry of the Solicitor General) in Ontario, the RTD "can be used by communities to collect information about local priorities (i.e., risks, vulnerable groups, and protective factors) and evolving trends."[226] The Ministry recommended using this data "in conjunction with other local data sources from various sectors."[227]

---

Herald (3 April 2019) <https://paherald.sk.ca/2019/04/03/centre-of-responsibility-ceasing-operations/>.

225 Nathan Munn, "Police in Canada Are Tracking People's 'Negative' Behavior In a 'Risk' Database", Vice (27 February 2019) <https://www.vice.com/en_us/article/kzdp5v/police-in-canada-are-tracking-peoples-negative-behavior-in-a-risk-database>. See also Minister of Community Safety and Correctional Services, "Community Safety and Well-being Planning Framework" <https://www.mcscs.jus.gov.on.ca/english/Publications/MCSCSSSOPlanningFramework.html>.

226 *Ibid*.

227 *Ibid*.

# 4.3. Algorithmic Surveillance Tools

Algorithmic technologies are used by law enforcement authorities to power or assist their surveillance activities. There is a range of algorithmic surveillance technologies, including automated licence plate readers, social media surveillance software, facial recognition technology, and social network analysis algorithms, available to law enforcement actors and currently in use in Canada. This section provides an overview of each of these technologies and discusses how they have been, or are being, used or considered by Canadian law enforcement authorities.

## 4.3.1. Automated Licence Plate Readers

An automated licence plate reader (ALPR) is "a license plate recognition application whereby vehicles observed by infrared cameras have their license plates read, recorded and checked against a preloaded database using pattern recognition software."[228] Cameras are mounted on police vehicles and scan licence plates on parked or moving vehicles as the police vehicle drives on public roadways, or cameras are installed in fixed positions along motorways where they scan licence plates as motorists drive by on the highway. The technology is used across Ontario, British Columbia, Saskatchewan, Alberta, Nova Scotia, Quebec, and Prince Edward Island by law enforcement authorities. ALPR systems enable surveillance and profiling through the systematic collection of bulk data such as the date, time, and geolocation of vehicles and the registration information (i.e., identity information) associated with those vehicles. In 2017, the Information and Privacy Commissioner of Ontario published a set of non-binding guidelines that proposed necessary oversight and controls on how the tool should be used, given the substantial amount of information that can be obtained and analyzed through the use of this tool.[229] The BC Information and Privacy Commissioner also investigated the use of ALPR technology by the Victoria Police Department in partnership with the RCMP and compelled the local agency to modify the technology to comply with BC privacy law.[230]

## 4.3.2. Social Media Surveillance

Social media surveillance involves using algorithms to mine personal information from social media platforms. Such surveillance is intended to gather information about and from individuals' online activities, and it attempts to detect patterns among and connections between users. Non-algorithmic social media surveillance has been used to monitor online activity around events such as protests by equality-seeking social movements, and that use has raised concerns for the human rights impact

228 Robert J Howe, "Privacy Impact Assessment: Automatic License Plate Recognition (ALPR)" (October 2009) *Royal Canadian Mounted Police*, at 12 <https://robwipond.com/ref/RCMP%20ALPR%20PIA.pdf> (obtained through access to information request by Rob Wipond, available at https://robwipond.com/archives/831). See Christopher Parsons, "Privacy Tech-Know Blog: Who's Watching Where You're Driving?" (13 June 2017) *Office of the Privacy Commissioner of Canada* <https://www.priv.gc.ca/en/blog/20170613>.

229 *Guidance on the Use of Automated Licence Plate Recognition Systems by Police Services* [PDF].

230 Information and Privacy Commissioner of Ontario, "Guidance on the Use of Automated Licence Plate Recognition Systems by Police Services" (July 2017) <https://www.oipc.bc.ca/investigation-reports/1480>.

of more powerful, algorithm-driven versions of such tools.[231] Software by Media Sonar provides a prominent example of social media surveillance technology. This Ontario-based company was banned from the Twitter and Instagram platforms in 2016 for violating the social media companies' privacy policies.[232] The bannings followed the American Civil Liberties Union's (ACLU) revelation that the company had been encouraging law enforcement agencies to identify "threats to public safety" by tracking protest-related keywords, such as #BlackLivesMatter and related hashtags.[233]

At least two Canadian police services, the Calgary Police Service (CPS) and the Toronto Police Service (TPS), have previously used Media Sonar. A member of law enforcement from Calgary stated in May 2019 that although the CPS had previously used software to monitor for "upcoming protests" or "to get a feel for what might be happening," it no longer used Media Sonar or any other social media mining software because the companies had become less useful after losing their access to major social media platforms such as Facebook and Twitter.[234] The CPS has a written policy that addresses Internet investigations and criminal intelligence, which encompasses gathering information from social media websites.[235] Under the policy, officers may collect publicly available data, including data processed by third-party social network aggregators and software. Officers are restricted, however, to collecting only information that is linked to a specific investigative purpose, including "threat-related information." The policy does not define what "threat-related information" means[236] nor does it restrict the CPS from using products like Media Sonar in the future, should they become useful once more for investigations.

The TPS has used a social media analytics product by Sysomos,[237] a Toronto-based company that was acquired by media intelligence company Meltwater in April 2018.[238] Meltwater made the following statement about the acquisition: "In order to enhance the search and analytics experience in the Sysomos Platform, we will leverage the AI models and information extracted from the unstructured

231 See e.g., "Using the information [the RCMP] received and data collected from social media, the Mounties identified 313 activists — attendees of protests on issues ranging from natural resource development to missing and murdered indigenous women... The RCMP then narrowed that list to 89 individuals it said met 'the criteria for criminality' and created unique profiles for each one." Sean Craig, "RCMP tracked 89 indigenous activists considered 'threats' for participating in protests," *National Post* (13 November 2016) <https://nationalpost.com/news/canada/rcmp-tracked-89-indigenous-activists-considered-threats-for-participating-in-protests>. Law enforcement authorities collecting personal information and surveilling activists in this manner has been heavily criticized and censured by human rights experts and civil liberties advocates. For discussion and analysis of how social media surveillance engages the right to privacy and to be free from unreasonable search and seizure, see Section 5.2 ("Right to Privacy"). For discussion regarding social media surveillance and the rights to freedom of expression and freedom of assembly, see Section 5.3 ("Rights to Freedom of Expression, Peaceful Assembly, and Association").

232 Amanda Margison, "Twitter and Instagram ban London, Ont., company for helping police track protesters" *CBC News* (19 January 2017) <https://www.cbc.ca/news/canada/toronto/twitter-bans-firm-police-protesters-1.3942093>.

233 Matt Cagle, "This Surveillance Software is Probably Spying on #BlackLIvesMatter" (15 December 2015) ACLU NorCal, <https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter>.

234 Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).

235 Calgary Police Service, "Internet Investigations and Criminal Intelligence Ref #IN-026" (obtained through freedom of information request 18-G-1921).

236 *Ibid*. at 4.

237 *R v Elliot*, 2016 ONCJ 35.

238 Mike Butcher, "Media monitor Meltwater acquires social analytics player Sysomos" (24 April 2018) *Tech Crunch* <https://techcrunch.com/2018/04/24/media-monitor-meltwater-acquires-social-analytics-player-sysomos/>.

web by Meltwater." Meltwater has also marketed itself to law enforcement agencies in the UK and the US.[239] The extent to which TPS continues to use Meltwater/Sysomos software or any other social media surveillance software is unknown. (The law enforcement representative interviewed was not part of the relevant unit and could not speak to the matter.)[240]

In 2019, investigative reports described the RCMP's expanded use of social media monitoring software that was provided by a company, Carahsoft, in the United States.[241] The software, called Social Studio, was developed by Salesforce to collect and analyze open source bulk data of social media content. The RCMP used the software as part of "Project Wide Awake." Project Wide Awake involved analyzing social media content in the course of active investigations as well as in a systematic and proactive manner to attempt to predict crime that might happen in the future. In November 2019, CBC News learned through FOI requests that the RCMP had launched an internal audit of its monitoring and collection of social media data across Canada to determine the legality of its practices.[242]

In April 2020, the RCMP released a contract tender that indicated that the RCMP is seeking to expand the reach of its social media surveillance capabilities.[243] According to the contract tender, one of the "mandatory" features of the software that the RCMP seeks to purchase is that the software must be able to do the following: "harvest and structure data into data-sets" that must be stored on servers located in Five Eyes countries; access "dark web (DarkNet) data sources"; and create a searchable database that aggregates "data sources automatically, anonymously, and continuously" in order to collect and index data.[244] The RCMP indicates in its tender that the technology "must provide a minimum of fifteen data sources as well as two Darknet data sources or a custom / proprietary algorithm".[245] Examples of data sources include: social networking sites (such as Facebook), micro-blogging sites (such as Twitter or Tumblr), photo and video sharing sites (such as Instagram and YouTube), personal blogging sites, virtual worlds (such as World of Warcraft and Farmville), "location based services" (including "Check-ins, Facebook Places, Foursquare, Yelp"), group buying sites (such as Groupon), and "social bookmarking and news aggregation" sites (such as Digg and Delicious).[246]

239 See North Wales Police, "2018/621 - Meltwater" (27 July 2018) <https://www.north-wales.police.uk/media/654896/2018-621-meltwater.pdf>; Brennan Center for Justice, "Mapping Reveals Rising Use of Social Media Monitoring Tools by Cities Nationwide" (16 November 2016) <https://www.brennancenter.org/blog/mapping-reveals-rising-use-social-media-monitoring-tools-cities-nationwide>.

240 Interview of a law enforcement representative in Canada by Yolanda Song & Cynthia Khoo (28 June 2019).

241 Bryan Carney, "'Project Wide Awake': How the RCMP Watches You on Social Media", *The Tyee* (25 March 2019) <https://thetyee.ca/News/2019/03/25/Project-Wide-Awake/>.

242 Catharine Tunney, "RCMP launches review of its social media monitoring operation", *CBC News* (5 November 2019), <https://www.cbc.ca/news/politics/rcmp-social-media-review-1.5346741>.

243 Jim Bronskill, "RCMP seeks to boost social media mining for threats ranging from disease to shootings", *Toronto Star* (28 April 2020), <https://www.thestar.com/news/canada/2020/04/28/rcmp-seeks-to-boost-social-media-mining-for-threats-ranging-from-disease-to-shootings.html>.

244 Public Works and Government Services Canada, "Request for a Standing Offer: Social Media Monitoring" (14 April 2020), <https://buyandsell.gc.ca/cds/public/2020/04/14/112c1c96f1d023a6072973f9550dd80c/ABES.PROD.PW__CY.B007.E78652.EBSU000.PDF> at 12.

245 Public Works and Government Services Canada, "Request for a Standing Offer: Social Media Monitoring" (14 April 2020), <https://buyandsell.gc.ca/cds/public/2020/04/14/112c1c96f1d023a6072973f9550dd80c/ABES.PROD.PW__CY.B007.E78652.EBSU000.PDF> at 12.

246 Public Works and Government Services Canada, "Request for a Standing Offer: Social Media Monitoring" (14 April 2020), <https://buyandsell.gc.ca/cds/public/2020/04/14/112c1c96f1d023a6072973f9550dd80c/ABES.PROD.PW__CY.B007.E78652.EBSU000.PDF>

During informal consultations for this report, the authors learned that the Ontario Provincial Police may have designed and is now using an algorithmic surveillance technology known as the "ICAC Child On-line Protection System (ICACCOPS)."[247] Based on information received during this informal consultation, it appears that the ICACCOPS software is a technology that is designed to scan online chat rooms, use some automated technological means (of unknown sophistication level) to keep the chat room 'open,' so messages do not automatically disappear at the conclusion of the conversation, and scrape and store the content of the chat room conversations into a searchable database that is accessible to law enforcement authorities. Reportedly, the technology appears to enable law enforcement authorities to gain access to particularly private chat conversations, such as chat conversations involving two or few participants alone, including chat rooms that are password-protected. It is also reportedly the case that at least the OPP as well as the Waterloo Regional Police Service (WRPS) have used this technology without seeking judicial approval in the form of a warrant, despite the fact that the use of this technology appears to enable law enforcement authorities to intercept private communications.[248] While there is little information publicly available about the ICACCOPS database and no reported criminal cases in Canada where the use of the ICACCOPS database has become public knowledge, the front end of the software is available online.[249] 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 became known), a 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.[250] 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.

---

at 45.

247 United States Department of Justice, Office of Juvenile Justice and Delinquency Prevention, "ICAC Child On-line Protection System (ICACCOPS) Improvements: Award Information", <https://ojjdp.ojp.gov/funding/awards/2018-mc-fx-k063>.

248 Intercepting private communications is a law enforcement technique that requires obtaining prior judicial approval in the form of a wiretap warrant under the Criminal Code, and it is an offence in Canada to intercept private communications without lawful authority: *R v TELUS Communications Co*, 2013 SCC 16; *R v Jones*, [2017] 2 SCR 696; *R v Mills*, 2019 SCC 22. The precise manner in which these wiretap-related provisions of the *Criminal Code* apply will partially depend on the capabilities of the ICACCOPS technology, and the use to which it is put. Some complicating factors may arise depending on the geographic location of law enforcement authorities that operate the technology. However, based on information that is known, if the OPP is obtaining ongoing access to a technology that "interjects itself into the communication process in real-time through technological means" (*R v Jones*, [2017] 2 SCR 696 at para 72) it would likely meet the definition of an interception under the *Criminal Code*. It is an offence under section 184 of the *Criminal Code* to intercept private communications without lawful authority. Pursuant to sections 193(1), (2)(b), and 2(e) of the *Criminal Code*, it is also an offence under section 193 of the *Criminal Code* to "use" unlawfully intercepted private communications, even for the purpose of a criminal investigation. Exemptions from this offence are set out in relation to "disclosure" of such private communications. The offence of unlawfully using intercepted private communications has not previously been the subject of focused judicial analysis in Canada, although the related language in section 193 in regards to "disclosure" of intercepted private communications was considered in *Wakeling v United States of America*, 2014 SCC 72. Even assuming the provisions under the *Criminal Code* do not strictly render the use of ICACCOPS in Canada to be unlawful offence, there would nevertheless be significant constitutional concerns under section 8 of the *Charter* if Canadian law enforcement authorities were permitted to circumvent the strict privacy safeguards under the wiretap-related provisions of the *Criminal Code* by knowingly relying on unlawfully intercepted private communications that were intercepted by foreign law enforcement authorities and made accessible on a real-time basis in Canada.

249 "ICACCOPS", <https://www.icaccops.com/users/login.aspx?ReturnUrl=%2Fusers> (accessed 30 April 2020).

250 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.

While the OPP designed the tool, the authors received information that the OPP made contact with their United States counterparts about the tool, and the ICACCOPS database is now being operated and maintained in the United States for use by law enforcement authorities, with access being given to investigators, for example, at the OPP and the WRPS. The OPP and the WRPS will be the first Canadian law enforcement authorities publicly reported to have used this technology. In a 2018 document concerning funding for further research to expand the surveillance capability, the United States Department of Justice implicitly suggested that the ICACCOPS technology was one of potentially multiple technologies that were designed to "efficiently and effectively parse through digital evidence, expedite evidence collection and transfer of digital files, facilitate decryption, address mobile chat encryptions, automate data intelligence, and support [the Internet Crimes Against Children (ICAC) Task Force program]."[251] In particular, one application for funding submitted to the Department of Justice stated that the "ICACCOPS supports investigations of Internet chat rooms, online solicitations, enticements and dark web activity."[252] The authors of this report did not receive any information through FOI requests that disclosed that the OPP may be using this technology.

The Ottawa Police Service's Strategic Operations Centre (OPSOC) has reportedly also deployed a form of social media surveillance. According to an article by *VICE Motherboard*, OPSOC provides "virtual backup" to patrol units of the Ottawa Police Service by performing real-time analyses of information obtained from police databases and online sources. These analyses are meant to provide officers with situational awareness of a given scene. It is not publicly known at the time of writing whether OPSOC currently has, or uses, any form of algorithmic or predictive analytics. The OPSOC is, however, reported to be developing algorithmic capabilities to supplement its current capabilities.[253]

## 4.3.3. Facial Recognition

Facial recognition software is a biometric identification technology that uses "computer algorithms to pick out specific, distinctive details about a person's face from a photograph, a series of photographs, or a video segment. These details, such as the distance between the eyes or the shape of the chin, are then converted into a mathematical representation and compared to data on other faces previously collected and stored in a face recognition database."[254] Facial recognition may take the form of "one-to-one", which compares a face to a specific individual's photo in a database to verify that person is who they claim to be, or "one-to-many", which compares a face to all photos in a database to identify who a person is.[255]

251 United States Department of Justice, "OJJDP FY 2018 Strengthening Investigative Tools and Technology for Combating Child Sexual Exploitation", OMB No 1121-0329, <https://ojjdp.ojp.gov/sites/g/files/xyckuh176/files/media/document/OJJDP-2018-14460.PDF> at 5.

252 United States Department of Justice, Office of Juvenile Justice and Delinquency Prevention, "ICAC Child On-line Protection System (ICACCOPS) Improvements: Award Information", <https://ojjdp.ojp.gov/funding/awards/2018-mc-fx-k063>.

253 Nathan Munn, "'Predictive Policing' Is Coming to Canada's Capital, and Privacy Advocates Are Worried", *VICE Motherboard* (13 February 2017) <https://www.vice.com/en_us/article/jpaew3/ottawa-police-strategic-operations-centre-canada-surveillance>.

254 Jennifer Lynch, "Face Off: Law Enforcement Use of Face Recognition Technology" (February 2018) *Electronic Frontier Foundation*, at 4-5, <https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf>.

255 Future of Privacy Forum, "Understanding Facial Detection, Characterization and Recognition Technologies" (March 2018) <https://fpf.org/wp-content/uploads/2018/09/FPF_FaceRecognitionPoster_R5.pdf>.

Mug-shot photographs are collected under the *Identification of Criminals Act*, which provides that individuals may be photographed without their consent if they are charged with, convicted of, or alleged to have committed an indictable offence.[256] Both the Calgary Police Service (CPS) and the Toronto Police Service (TPS) use facial recognition software from NEC Corporation—confirmed to be NeoFace Reveal in the case of the CPS[257]—to search photographs and composite drawings of unknown individuals against the agencies' mug-shot databases. The CPS also retains unidentified images to search them against new mug-shot photos that are subsequently collected.[258] The Ottawa Police Service (OPS) conducted a three-month long pilot program with NeoFace Reveal, ending in March 2019, and has stated that they are not currently using the product.[259] The Edmonton Police Service (EPS) has also recently announced that it plans to use facial recognition technology in relation to its mug-shot database by later in 2020.[260] Similarly, it became known in 2020 that York Regional Police has budgeted $1.68 million in 2019 to acquire a facial recognition and automated palm and fingerprint recognition system at some point between 2019 and 2021.[261] The Peel Regional Police Service confirmed that they will also be obtaining a license to use the same system.

Both the CPS and the TPS state that facial recognition matches are not meant to be used as indisputable positive identification and, instead, are meant only to provide investigative leads.[262] Prior judicial authorization is not obtained before specialized CPS or TPS staff conduct a facial recognition inquiry with this software.[263] In 2012, British Columbia's Information and Privacy Commissioner found that the VPD was using facial recognition technology and driver's licence photographs, which were held by the province's public automotive insurer, without seeking individual consent or obtaining prior judicial authorization.[264] The Commissioner ordered the warrantless practice be discontinued.

256 Calgary Police Service, "Facial Recognition Technology, Ref #IN-006-1" at 1 (obtained through freedom of information request 18-G-1921); *Identification of Criminals Act*, RSC 1985, c I-1, s. 2(1); *Identification of Criminals Act*, RSC 1985, c I-1, s. 2(1).

257 "Facial Recognition To Aid Investigations", City of Calgary Newsroom (3 November 2014) <https://newsroom.calgary.ca/facial-recognition-to-aid-investigations/>; Kate Allen and 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>.

258 Calgary Police Service, "Facial Recognition 2018" at 10 (obtained through freedom of information request 18-G-1921).

259 Shaamini Yogaretname, "Ottawa police piloted controversial facial recognition software last year", *Ottawa Citizen* (14 February 2020) <https://ottawacitizen.com/news/local-news/ottawa-police-piloted-controversial-facial-recognition-software-last-year/>.; and Shaamini Yogaretnam, "Chief says facial recognition software test drew on police mug shot database", *Ottawa Citizen* (26 February 2020) <https://ottawacitizen.com/news/local-news/chief-says-facial-recognition-software-test-drew-on-police-mug-shot-database/>.

260 Anna Junker, "Edmonton police unveil details on use of facial recognition technology", *The Edmonton Journal* (19 February 2020), <https://edmontonjournal.com/news/local-news/edmonton-police-unveil-details-on-use-of-facial-recognition-technology>.

261 Nathan Munn, "Police Forces in Canada Are Quietly Adopting Facial Recognition Tech", *VICE Media* (23 June 2020), <https://www.vice.com/en_ca/article/xg8wp4/police-forces-in-canada-are-quietly-adopting-facial-recognition-tech>.

262 Mark Saunders, "Toronto Police Services Board Report: Facial Recognition System" (17 May 2019) at 2 <http://www.tpsb.ca/images/agendas/PUBLIC_AGENDA_May30.pdf>.

263 *Ibid*. at 3.

264 Office of the Information & Privacy Commissioner, "Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia" (16 February 2012) <https://www.oipc.bc.ca/investigation-reports/1245>.

As of February 2020, federal and provincial privacy regulators were investigating the use of a facial recognition company called Clearview AI following reporting that the company was selling its services to over 600 law enforcement agencies, primarily in the United States.[265] Clearview AI reportedly scraped approximately 3 billion images from the Internet and aggregated the images for use in law enforcement investigations. Continued media reporting in Canada led to the revelation that the RCMP, members of the Calgary Police Service and Edmonton Police Service,[266] and multiple policing services throughout Ontario, including the TPS, the Peel Regional Police Service, Halton Police Service, Ottawa Police Service, Durham Regional Police Service, Niagara Regional Police Service, and Hamilton Police Service had used Clearview AI.[267] These revelations occurred only after some agencies had denied using the tool, purportedly due to not realizing individual officers had engaged in unauthorized use of Clearview AI in their work.[268] Moreover, FOI records indicated that the RCMP "denied using facial recognition software on Canadians three months after it had entered into a contract with controversial U.S. company Clearview AI", according to reporting by *The Tyee*.[269] Although Clearview AI announced in July 2020 that it will no longer offer facial recognition services in Canada, and has indefinitely suspended its contract with the RCMP,[270] it is only one of many companies offering such services. Facial recognition technology as a category remains an ongoing issue in Canada.

Facial recognition technology has also been the focus of widespread concern and increasingly decisive action in the United States. As of writing, four cities have banned the use of facial recognition technology by government and law enforcement: Boston and Somerville in the state of Massachusetts,[271] and San Francisco and Oakland in the state of California.[272] Additionally, in June 2020, the Association

265 Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It", *The New York Times* (18 January 2020), <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>; "Privacy watchdogs to probe Clearview AI's facial-recognition technology", *CBC News* (21 February 2020), <https://www.cbc.ca/news/canada/toronto/clearview-ai-police-use-1.5471493>.

266 "Both the Calgary Police Service and the Edmonton Police Service had denied use of the software earlier this month, but both have since come forward with reports that several of their officers had tested the Clearview AI software. Staff Sgt. Gordon MacDonald, of the Calgary police criminal identification section, said the service wouldn't be interested in software that uses open-source images due to ethical concerns." Alanna Smith, "Two Calgary officers tested Clearview AI facial-recognition software", *Calgary Herald* (29 February 2020). <https://calgaryherald.com/news/local-news/two-calgary-officers-tested-clearview-ai-facial-recognition-software/>.

267 "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-any-investigative-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-last-year>.

268 See e.g., "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>.

269 Bryan Carney, "FOI Documents Confirm RCMP Falsely Denied Using Facial Recognition Software", *The Tyee* (16 April 2020) <https://thetyee.ca/News/2020/04/16/RCMP-FOI-Facial-Recognition/>.

270 Office of the Privacy Commissioner of Canada, "Clearview AI ceases offering its facial recognition technology in Canada" (6 July 2010) <https://priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_200706/>.

271 Sean Philip Couter, "Boston City Council votes to ban facial-recognition technology", *Boston Herald* (24 June 2020) <https://www.bostonherald.com/2020/06/24/boston-city-council-votes-to-ban-facial-recognition-technology/>; and Caroline Haskins, "A Second U.S. City Has Banned Facial Recognition", *VICE Motherboard* (28 June 2019) <https://www.vice.com/en_ca/article/paj4ek/somerville-becomes-the-second-us-city-to-ban-facial-recognition>.

272 Kate Conger, Ricahrd Fausset & Serge F Kovaleski, "San Francisco Bans Facial Recognition Technology," *New York Times* (14 May 2019)

for Computing Machinery (ACM) United States Technology Policing Committee (USPTC) publicly called for "an immediate suspension of the current and future private and governmental use of facial recognition (FR) technologies in all circumstances known or reasonably foreseeable to be prejudicial to established human and legal rights".[273] In its statement of principles, the ACM USPTC provided its findings that facial recognition technology is "not sufficiently mature and reliable to be safely and fairly utilized without appropriate safeguards against adversely impacting individuals, particularly those in vulnerable populations" and that "its use has often compromised fundamental human and legal rights of individuals to privacy, employment, justice and personal liberty".[274]

Major technology players have added their weight to concerns about facial recognition, contributing to a rising tide questioning the value and impacts of the technology. IBM publicly withdrew from any further development or sales of facial recognition technology, citing concerns with racial profiling by police.[275] Microsoft stated that it would refuse to sell its facial recognition technology to police services until there are federal laws in place that regulate its use.[276] Amazon imposed on itself a one-year moratorium on sales of facial recognition technology to police services, ostensibly to "give Congress enough time" to implement regulations.[277] Google has also indicated support for a temporary ban on facial recognition technology.[278] In 2019, Axon Enterprise (formerly TASER) banned facial recognition systems from its body cameras.[279] While these industry stances have been critiqued for being insufficient, self-serving, opportunistic, or ineffectual,[280] that even dominant purveyors of facial

---

<https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html>; and Sarah Ravani, "Oakland bans use of facial recognition technology, citing bias concerns," *San Francisco Chronicle* (17 July 2019) <https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php>.

273 The ACM is "the world's largest educational and scientific computing society" and its USTPC "serves as the focal point for ACM's interaction with all branches of the US government, the computing community, and the public on policy matters related to information technology." "ACM US Technology Policy Committee Urges Suspension of Private and Governmental Use of Facial Recognition Technologies" (30 June 2020), Association for Computing Machinery <https://www.acm.org/media-center/2020/june/ustpc-issues-statement-on-facial-recognition-technologies>.

274 Statement on Principles and Prerequisites for the Development, Evaluation and Use of Unbiased Facial Recognition Technologies" (30 June 2020), ACM US Technology Policy Committee <https://www.acm.org/binaries/content/assets/public-policy/ustpc-facial-recognition-tech-statement.pdf>.

275 Alex Hern, "IBM quits facial-recognition market over police racial-profiling concerns," *Guardian* (9 June 2020) <https://www.theguardian.com/technology/2020/jun/09/ibm-quits-facial-recognition-market-over-law-enforcement-concerns>; and Jay Peters, "IBM will no longer offer, develop, or research facial recognition technology," *The Verge* (8 June 2020) <https://www.theverge.com/2020/6/8/21284683/ibm-no-longer-general-purpose-facial-recognition-analysis-software>.

276 Jay Greene, "Microsoft won't sell police its facial-recognition technology, following similar moves by Amazon and IBM," *Washington Post* (11 June 2020) <https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/>.

277 "We are implementing a one-year moratorium on police use of Rekognition" (10 June 2020), *Amazon* <https://blog.aboutamazon.com/policy/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition>; Karen Weise & Natasha Singer, "Amazon Pauses Police Use of Its Facial Recognition Software," *New York Times* (10 June 2020) <https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html>.

278 Michael Kan, "Google: Temporary Ban on Facial-Recognition Tech Might Be Necessary," *PCMag* (21 January 2020) <https://www.pcmag.com/news/google-temporary-ban-on-facial-recognition-tech-might-be-necessary>.

279 Charlie Warzel, "A Major Police Body Cam Company Just Banned Facial Recognition," *New York Times* (27 June 2019) <https://www.nytimes.com/2019/06/27/opinion/police-cam-facial-recognition.html>.

280 See e.g., Zack Whittaker, "Amazon's facial recognition moratorium has major loopholes," *Techcrunch* (10 June 2020) <https://techcrunch.com/2020/06/10/amazon-rekognition-moratorium/>; Will Knight, "IBM's Withdrawal Won't Mean the End of Facial Recognition," *Wired* (10 June

recognition technology have seen fit to make such commitments to any extent is further indication of the high-risk nature of this technology, with respect to its impacts on constitutional and human rights and freedoms.[281]

## 4.3.4. Social Network Analysis

Social network analysis (SNA) "is based on the premise that the relationships between individuals can inform and even predict an individual's behavior."[282] SNA "uses statistical and visualization techniques to describe how social actors are affected by those around them and, in turn, how these individuals affect the actors they are connected to, and how the set of actors and relationships between them affect real-world behavior"—such as criminal activity.[283] The availability of machine learning combined with the rise of social media surveillance, licence plate recognition, facial recognition technologies, and other mass surveillance tools to aggregate information has led various law enforcement agencies to focus their attention on the potential uses of SNA in the context of algorithmic policing.[284]

In addition to the Calgary Police Service engaging in SNA as described above in Section 4.2.1 ("Calgary Police Service: Palantir and IBM i2 Analyst Notebook"), a paper commissioned by Public Safety Canada in 2012 developed and proposed an SNA tool. This tool would have automatically detected criminal organizations within large social networking data sets, and would have been based on co-offender network analysis of police data from British Columbia.[285] Further, in its *Policy on eliminating racial profiling in law enforcement*, the Ontario Human Rights Commission identified social network analysis as a potential source of adverse impacts on racialized communities where algorithmic policing is involved.[286]

---

2020) <https://www.wired.com/story/ibm-withdrawal-wont-mean-end-facial-recognition/>; Kate Kaye, "IBM, Microsoft, and Amazon's face recognition bans don't go far enough," *Fast Company* (13 June 2020) <https://www.fastcompany.com/90516450/ibm-microsoft-and-amazons-face-recognition-bans-dont-go-far-enough>; Laurie Clarke, "Amazon's facial recognition stunt is pure PR," New Statesman Tech (10 June 2020) <https://tech.newstatesman.com/security/amazons-facial-recognition-stunt>; "Why Amazon's temporary ban of police use of facial recognition is not enough" (11 June 2020), *Privacy International*, <https://privacyinternational.org/news-analysis/3896/why-amazons-temporary-ban-police-use-facial-recognition-not-enough>.

281 For a detailed analysis of facial recognition technology and its high risk of violating and degrading the right to privacy, see "IN FOCUS #5: Facial Recognition Technology and the Erosion of Privacy Rights" in Section 5.2.4 ("Data Accuracy: Inaccurate Data and Inaccurate Algorithms") of this report.

282 Andrew Papachristos & Michael Sierra-Arévalo, "Policing the Connected World" (2018) *Office of Community Oriented Policing Services*, at viii <https://ric-zai-inc.com/Publications/cops-w0859-pub.pdf>.

283 *Ibid*.

284 See e.g., Andrew Papachristos & Michael Sierra-Arévalo, "Policing the Connected World" (2018) *Office of Community Oriented Policing Services*, at 21 <https://ric-zai-inc.com/Publications/cops-w0859-pub.pdf>.

285 Uwe Glässer et al., "Estimating Possible Criminal Organizations from Co-offending Data" (November 2012) *Public Safety Canada*, <http://publications.gc.ca/collections/collection_2012/sp-ps/PS14-7-2012-eng.pdf>; see also *Public Safety Canada*, "Organized Crime Research Brief no. 28: Data mining for Possible OC" at 1-2 <https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rgnzd-crm-brf-28/index-en.aspx>.

286 Ontario Human Rights Commission, "Policy on eliminating racial profiling in law enforcement" at 4.2.6.2, <http://www.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement>.

## 4.4. Limitations of Research Findings

The findings in Part 4 describe how law enforcement agencies across Canada have started to consider, develop, or use a variety of algorithmic policing methods. However, this review does not necessarily represent a complete factual record of the extent to which law enforcement agencies across Canada use or are developing algorithmic policing technologies. There are at least three reasons for why this is so: lack of transparency on the part of law enforcement regarding their use of new police surveillance technologies, barriers to access to information in Canada's FOI request processes, and law enforcement's ability to claim privilege over information that would otherwise be disclosed in response to an FOI request. The remainder of this section will discuss each of these research limitations.

First, generally speaking, law enforcement has historically been reticent to disclose their use of novel police surveillance technologies.[287] Avoidance of disclosure regarding the use of novel surveillance technology includes, for example, dropping criminal charges seemingly in order to avoid having to reveal details about the use of cell site simulators (also known as IMSI catchers), which simulate cell phone towers in order to capture personal data from people's mobile phones.[288] It is unfortunately not unusual for the Canadian public to become aware of the use or development of novel policing technologies only after they have been used or tested by police agencies for extended periods. Transparency is an essential component of existing police oversight and accountability mechanisms in Canada, without which lawmakers cannot provide guidance to or appropriately regulate law enforcement authorities. Transparency also enables policymakers and the public to more effectively consider and develop informed law and policy with regard to the range of limitations that are required to safeguard constitutional and human rights and balance the public interests at stake.[289] Nonetheless, despite some transparency measures being in place, the point remains that it would not be realistic to assume that the public in Canada currently has access to the complete factual record regarding the extent to which algorithmic policing technologies are currently in use.

Second, there are multiple challenges associated with FOI request processes in Canada. These challenges include, for example, significant delay, the difficulty of crafting sufficiently broad or accurately specific request terms, high processing fees, and the high number of law enforcement institutions and related agencies at the municipal, provincial, and federal levels. It is, therefore,

287 For example, in 2017, the public learned that the RCMP implemented a controversial meta-data analysis program only after the program was later abandoned by the agency: Jim Bronskill, "RCMP created metadata-crunching tool to glean criminal intelligence", *Global News* (9 May 2017), <https://globalnews.ca/news/3437034/rcmp-created-metadata-crunching-tool-to-glean-criminal-intelligence/>. See also, 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>.

288 Justin Ling, "A mob trial is over after Canadian cops refuse to disclose their surveillance techniques", *Vice* (21 March 2017), <https://www.vice.com/en_ca/article/ywn7gm/a-mob-trial-is-over-after-canadian-cops-refuse-to-disclose-their-surveillance-techniques>. See generally Tamir Israel & Christopher Parsons, "Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada" (August 2016), Citizen Lab <https://citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf>.

289 Transparency has already been identified as one of the core principles in the Government of Canada's Directive on Automated Decision-Making, which identifies transparency as one of the core principles guiding the integration of artificial intelligence and automated decision making in public sector services: Government of Canada, "Directive on Automated Decision-Making" (5 February 2019) <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592>.

impossible to conclude that the documents relied on in writing this report are exhaustive of the algorithmic policing technologies used or being developed by Canadian law enforcement agencies. As one example of the inadequacy of the FOI request process, in May 2019, the public became aware that the TPS had purchased a facial recognition system in March 2018 and had not disclosed this to the public.[290] The authors of this report had previously submitted an FOI request to the TPS, which included a broad request for records relating to facial recognition during a time period that included March 2018. The TPS did not provide any information or responsive documents regarding the use of facial recognition, despite the fact that it is now known tha the police service spent $451,718 on a facial recognition system during the time period that was the subject of the FOI request.[291] Several FOI requests from various agencies remain outstanding even at the time of writing.

Third, in many cases, FOI requests were returned with responses that claimed privilege—i.e., an assertion that the responding agency is not disclosing, and is not required to disclose, the requested materials for legal reasons. Based on these responses, some law enforcement agencies may be asserting privilege with respect to some algorithmic policing methods that are under development or in use if the agency is taking the position that such methods are subject to investigative privilege. Investigative privilege is invoked by government agencies and, where legitimate, it permits law enforcement actors to keep certain police techniques confidential that would otherwise be disclosed in a given legal process (e.g., through an FOI request). Such privilege must be established by the law enforcement actor on a case-by-case basis. To establish a valid claim of investigative privilege, the information in question must: 1) be used by a police agency in a law enforcement capacity, 2) not be publicly known, and 3) capable of assisting potential offenders to interfere with or defeat police investigative functions if disclosed.[292] Due to time constraints, the authors have not appealed these claims specifically to information and privacy commissioners to adjudicate the appropriateness of law enforcement actors' invocation of investigative privilege; as such, it remains to be seen if their claims of privilege with regard to algorithmic policing technologies are valid or not.[293]

## 4.5. Concluding Comments: The Current State of Algorithmic Policing in Canada

In sum, the findings in Part 4 showcase that algorithmic technologies are being used, are in development, or are under consideration in a variety of policing-related contexts in Canada. At least two police services, the Vancouver Police Department and the Saskatoon Police Service, have developed or are developing algorithmic policing technologies for the purposes of guiding police action and

290 Kate Allen and 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>.

291 Phillip Lee-Shanok, "Privacy advocates sound warning on Toronto police use of facial recognition technology", *CBC News* (30 May 2019), <https://www.cbc.ca/news/canada/toronto/privacy-civil-rights-concern-about-toronto-police-use-of-facial-recognition-1.5156581>.

292 *R v Amer*, 2017 ABQB 651 at para 37.

293 See Tamir Israel & Christopher Parsons, *Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada* (August 2016) at 31-49, <https://citizenlab.ca/wp-content/uploads/2016/09/20160818-Report-Gone_Opaque.pdf>, discussing the meaningful limits of investigative privilege in greater detail in a similar context relating to another novel policing technology.

intervention. Other police services, such as in Calgary and Toronto, have acquired technological tools that jurisdictions outside of Canada have leveraged to build algorithmic policing systems. Additionally, numerous law enforcement agencies use algorithmic surveillance technologies (e.g., automated licence plate readers, facial recognition, and social media monitoring algorithms) or are developing such technologies.

At the same time, based on the formal research interviews and desk research conducted for this report, the use of algorithmic policing systems does not appear to be widespread in Canada, even if the factual record on this point is not definitive. The relatively low level of adoption of these technologies by Canadian police services may be the result of a number of potential factors, including policymakers' and law enforcement agencies' cautious approaches to adopting or integrating algorithmic technologies, or budgetary or resource constraints that have limited the procurement or use of these technologies.

It is against the backdrop of the research findings presented in Sections 4.1 through 4.4 that a legal and policy analysis of the human rights and constitutional law implications of algorithmic policing technologies is set out in Part 5 ("International Human Rights and *Charter* Rights Implications of Algorithmic Policing"). Despite the seeming (at time of writing) relative absence of widespread development or adoption of these technologies in Canada, it is evident from the research findings presented above that algorithmic policing technologies are being used, are in development, or are under consideration in a variety of law enforcement-related contexts in Canada. As such, an analysis of these technologies through the lens of human rights and constitutional law is not only warranted, but overdue. It is through assessing the human rights and constitutional law implications of this class of law enforcement technologies that society can ensure that their use or potential development does not unjustly violate the fundamental human rights and freedoms of impacted individuals and communities.

# 5. International Human Rights and *Charter* Rights Implications of Algorithmic Policing

Algorithmic policing technologies raise a range of legal and policy issues that cut across several human rights protected in the *Canadian Charter of Rights and Freedoms* ("the *Charter*")[294] and in international human rights law. Part 5 of this report presents and analyzes the implications of the use of algorithmic policing technology through the lens of several of these rights. Canadian and international human rights law both guarantee the human rights examined in this report; accordingly, each right is analyzed under both legal regimes.

Section 5.1 provides a background overview of the domestic and international laws that govern Canada's human rights obligations and introduces the authors' approach to the human rights analysis of algorithmic policing technologies. The subsequent sections in Part 5 each analyze algorithmic policing through the lens of a specific human right: the right to privacy (Section 5.2); the right to freedom of expression, peaceful assembly, and association (Section 5.3); the right to equality and freedom from discrimination (Section 5.4); the right to liberty and to be free from arbitrary detention (Section 5.5); the right to due process (Section 5.6); and the right to a remedy (Section 5.7). Each section briefly introduces the right being considered and how it is protected in Canadian and international law, then it analyzes the specific issues and concerns that algorithmic policing technology raises with respect to that right.

## 5.1. Introduction to a Human Rights Analysis of Algorithmic Policing

Canada's human rights obligations are governed by the *Charter*, quasi-constitutional domestic legislation, and the international human rights instruments it has ratified. All government action must comply with these laws, including actions involving algorithmic policing methods that law enforcement engages in. The legal analysis presented throughout this report explicitly draws on international human rights law as a complementary source of Canada's human rights obligations for two reasons.

First, international human rights law can provide an international, normative moral force that holds governments and businesses to certain overarching human rights standards and obligations. International human rights law acts as an external standard by way of providing a frame of reference against which Canadian state (in)action is measured. This is particularly so when governments must consider what use to make, if any, of emerging technologies, or technologies that have not yet been exposed to independent legal scrutiny. Such technologies can often raise novel issues that have not yet been the subject of constitutional litigation in Canada.

294 *Canadian Charter of Rights and Freedoms*, s 7, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.

Second, international human rights obligations are a component of Canada's legal system. Canada is obligated to comply with and implement its international human rights law commitments under the international legal system. Within the domestic legal system, prohibitive rules of customary international law are automatically incorporated into domestic law, and international treaties or conventions become binding in Canadian law if given effect through Canada's domestic law-making process.[295] Of course, it is true that, as a sovereign state, Canada may override international treaty and customary law through domestic legislation that contradicts these commitments.[296] Nevertheless, domestic legislation must comply with Canada's constitution. When applying the *Charter*, its text will often be interpreted to provide protection at least as great as that afforded by similar provisions in international human rights documents to which Canada is a party.[297]

As a result, if police practices that relate to the use of algorithmic policing technology violate international human rights obligations, the Canadian government is responsible for taking legislative or other appropriate action to bring such police practices into compliance with those obligations. Further, all domestic legislation must be compliant with the *Charter*, the interpretation of which is informed by international human rights obligations.

Public information about the extent to which algorithmic policing technologies are used in Canada is incomplete.[298] As a result, the legal and policy analyses in Sections 5.2–5.7 are necessarily prospective. In some cases, the analyses are hypothetical insofar as they are based on the relevant literature, cases, and studies of algorithmic policing technologies in other jurisdictions, particularly the United States and United Kingdom. Some issues—such as the black box problem, feedback loops, and automation bias—appear more than once throughout the human rights analysis due to their cross-cutting nature and because they engage multiple rights simultaneously.

Given the rapid advancement of technology and its tendency to outpace legal safeguards for human rights, this report's analysis serves as a guide to potential human rights concerns that must be taken into account if—and before—Canadian police services continue or expand the use of algorithmic policing technology. In the absence of caution and due diligence, there is a severe risk of human rights and *Charter* rights becoming an afterthought in relevant laws, policies, and discussions, rather than a necessary starting point.

295 *R v Hape*, [2007] 2 SCR 292 at para 39; Kazemi Estate v Islamic Republic of Iran, 2014 SCC 62 at para 149.

296 *Ibid.*

297 *Kazemi Estate v Islamic Republic of Iran*, 2014 SCC 62 at para 150.

298 The explanation for why information is incomplete is due to the challenges outlined in Section 1.2 ("Methodology") and Section 4.4 ("Limitations of Research Findings"). It includes assertions of privilege, the unfulfilled FOI requests, lack of transparency among some police services, and lack of publicly available information regarding uses of the examined technologies by Canadian police services.

# Business and Human Rights

This report focuses on the constitutional and human rights obligations of the Canadian government and Canadian law enforcement agencies, but the private sector also plays a role in developing and implementing law enforcement technologies, including in algorithmic policing. Many of the policing strategies examined in this report require technology and technological assistance from private companies. In some cases, police services purchase off-the-shelf solutions, such as PredPol, which is developed and owned entirely by a private company. In other cases, law enforcement agencies may work together with private companies to develop a predictive policing program. For example, the Vancouver Police Department developed its GeoDASH system in partnership with Latitude Geographics, and the Toronto Police Service has explored a collaboration with Environics Analytics in its data-driven policing solutions.

While international human rights obligations primarily rest with states, businesses also have responsibilities to respect human rights under the United Nations Guiding Principles on Business and Human Rights ("Guiding Principles").[299] These responsibilities are independent from, and supplementary to, businesses' obligations under domestic legislation. The Guiding Principles set out best practices for businesses while also delineating governments' obligations to hold businesses accountable for human rights violations caused by their activities. Domestically, Quebec's *Charter of Human Rights and Freedoms* also applies to private actors and could potentially establish a cause of action for human rights breaches caused by private companies.[300]

In the context of algorithmic policing, these obligations mean that private actors, such as Palantir Technologies, Environics Analytics, NEC Corporation, IBM, ShotSpotter, Clearview AI, and others, have an international normative responsibility to assess the demonstrated and potential impacts of their business activities on human rights. Companies must demonstrate sensitivity to the ways in which their operations could affect the human rights of marginalized and vulnerable populations. Such populations include "[I]ndigenous peoples; women; national or ethnic, religious and linguistic minorities; children; persons with disabilities; and migrant workers and their families."[301] Meeting these responsibilities would require companies to engage in due diligence regarding their potential human rights impacts.[302] Due diligence includes consultation with racialized and other disproportionately

299 United Nations Human Rights Office of the High Commissioner, "Guiding Principles on Business and Human Rights: Implementing the United Nations 75 'Protect, Respect and Remedy' Framework," A/ HRC/17/31 (New York and Geneva, 2011) <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf>.

300 *Charter of Human Rights and Freedoms*, RSQ, c C-12.

301 United Nations Human Rights Office of the High Commissioner, "Guiding Principles on Business and Human Rights: Implementing the United Nations 75 'Protect, Respect and Remedy' Framework," A/ HRC/17/31 (New York and Geneva, 2011) <http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf> at page 14.

302 *Ibid*, at pages 17-19.

criminalized communities,[303] and addressing adverse human rights impacts that are caused by their technologies and services, including impacts on the right to privacy and the right to equality and non-discrimination.[304]

The integrated involvement of private businesses—specifically multinational technology companies—in traditional government functions such as policing also raises questions concerning corporate social responsibility and technology ethics. These questions about the human rights consequences of technological advances have motivated broader cultural discourse that interrogates the governing power of the contemporary technology sector,[305] driven by both external and internal critics.[306]

While private sector activities are not the main subject matter of this report—which focuses on the algorithmic policing activities of law enforcement agencies, including their use of private sector technologies—the authors note throughout where the involvement of private businesses is particularly salient to a given issue. Further, these companies and their potential to detrimentally affect the ability of individuals and marginalized communities to exercise their guaranteed human rights warrants further research in their own right.

303 *Ibid*, at page 19.

304 *Ibid*, at pages 20-21.

305 See e.g., Alexis Madrigal, "The Coalition Out to Kill Tech as We Know", *The Atlantic* (4 June 2019) <https://www.theatlantic.com/technology/archive/2019/06/how-politicians-and-scholars-turned-against-big-tech/591052/> ("At a broad ideological level, two things have happened. First, the idea of cyberspace, a transnational, individualistic, largely unregulated, and free place that was not exactly located in any governmental domain, has completely collapsed. Second, the mythology of tech as the carrier of progress has imploded, just as it did for the robber barons of the late 19th century, ushering in the trust-busting era"); ; see also e.g., Casey Newton, "The tech backlash is real, and it's accelerating", *The Verge* (17 September 2019), <https://www.theverge.com/interface/2019/9/17/20869495/tech-backlash-nyt-rob-walker-antitrust-privacy>; Madhumita Murgia and Siddarth Shrikanth, "How Big Tech is struggling with the ethics of AI", *The Financial Times* (28 April 2019) <https://www.ft.com/content/a3328ce4-60ef-11e9-b285-3acd5d43599e>; Margi Murphy, "Facebook removed from S&P list of ethical companies after data scandals", *The Telegraph* (13 June 2019) <https://www.telegraph.co.uk/technology/2019/06/13/facebook-gets-boot-sp-500-ethical-index/>; Enrique Dans, "Can Employees Force A Company To Be More Ethical?", *Forbes* (19 June 2018) <https://www.forbes.com/sites/enriquedans/2018/06/19/can-employees-force-a-company-to-be-more-ethical/#4e78a19e27e3>; Darrel M. West, "The role of corporations in addressing AI's ethical dilemmas", *Brookings* (13 September 2018) <https://www.brookings.edu/research/how-to-address-ai-ethical-dilemmas/>.

306 See e.g., Daisuke Wakabayashi and Scott Shane, "Google Will Not Renew Pentagon Contract That Upset Employees", *The New York Times*, (1 June 2018) <https://www.nytimes.com/2018/06/01/technology/google-pentagon-project-maven.html>; Julie Carrie Wong, "'We won't be war profiteers': Microsoft workers protest $480m army contract", *The Guardian* (22 February 2019) <https://www.theguardian.com/technology/2019/feb/22/microsoft-protest-us-army-augmented-reality-headsets>; Samantha Maldonado, "U.S. tech industry becomes hotbed for employee activism", *The Globe and Mail* (25 August 2019) <https://www.theglobeandmail.com/business/technology/article-us-tech-industry-becomes-hotbed-for-employee-activism/>; see also Emily Birnbaum, "Over 1,000 students across 17 colleges pledge not to work at Palantir over ICE work", *The Hill* (16 September 2019) <https://thehill.com/policy/technology/461573-over-1000-students-across-17-colleges-pledge-not-to-work-at-palantir-over>.

## 5.2 Right to Privacy

Algorithmic policing technologies engage the right to privacy as a result of the data collection, processing, and disclosure methods that these technologies rely on in order to draw inferences and forecast or reveal information about individuals. Research findings in Part 4 indicated that Canadian law enforcement agencies are beginning to adopt different kinds of algorithmic policing technologies and may choose to expand their use of such technology in the future. Protections for privacy must be integrated at the forefront of existing and future initiatives because the data collection and processing capabilities associated with algorithmic policing technology may threaten the public's right to be secure against privacy invasions. Without adequate limits and oversight that ensure any use of such technology is necessary and proportionate to legitimate aims, unchecked authority to use algorithmic policing technologies risks leaving individuals with unlawfully attenuated privacy rights—never knowing when, and to what extent, the state is monitoring and recording them.

Privacy is a fundamental human right that is recognized in the *Universal Declaration of Human Rights*,[307] and the *American Declaration of the Rights and Duties of Man* (the "Bogota Declaration", covering North and South America),[308] and it is protected in international instruments such as the *International Covenant on Civil and Political Rights*[309] (ICCPR) and the *Convention on the Rights of the Child*.[310] The right is essential to human dignity and autonomy, and it is foundational in a free and democratic society.[311] Privacy "gives us a space to be ourselves without judgement, allows us to think freely without discrimination, and is an important element of giving us control over who knows what about us."[312]

Two overarching features of legal protection for privacy are most pertinent when assessing algorithmic policing technology. First, Canadian and international human rights law provide protection for a zone of privacy. The UN High Commissioner for Human Rights (OHCHR) has defined privacy as a "presumption that individuals should have an area of autonomous development, interaction, and liberty" which is free from state interference.[313] In Canadian law, the protected zone of privacy is defined aspirationally insofar as the zone is associated with what individuals should be entitled to expect. The zone of

307 Universal Declaration of Human Rights, adopted December 10, 1948, G.A. Res. 217A(III), U.N. Doc. A/810 at 71 (1948), art 12.

308 Inter-American Commission on Human Rights (IACHR), *American Declaration of the Rights and Duties of Man*, 2 May 1948, adopted by Canada in 1948, art 5.

309 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966 <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>, art 17.

310 *Convention on the Rights of the Child* (CRC), adopted November 20, 1989, G.A. Res. 44/25, annex, 44 U.N. GAOR Supp. (No. 49) at 167, U.N. Doc. A/44/49 (1989), entered into force September 2, 1990, ratified by Canada 1991, <https://www.ohchr.org/en/professionalinterest/pages/crc.aspx>, art 16.

311 UN Human Rights Council, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at para 11.

312 Privacy International, "What is Privacy", <https://privacyinternational.org/explainer/56/what-privacy>.

313 UN Human Rights Council, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at para 5; see also, United Nations General Assembly, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin" (28 December 2009) A/HRC/13/37 <https://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/A-HRC-13-37.pdf> at para 11.

privacy does not depend on artificial distinctions between public and private spaces,[314] or public and private information.[315] The right must be applied in a way that is equally meaningful for all individuals, especially given the vulnerabilities that are experienced by particular communities (i.e., racialized, socio-economically disadvantaged, or otherwise historically marginalized groups).[316] The OHCHR and Supreme Court of Canada have recognized that protecting informational privacy, which covers information about a person and their life, is particularly crucial in today's digital society.[317]

Second, constitutional safeguards and the ICCPR prohibit unreasonable invasions of privacy by law enforcement authorities or the government. Under the ICCPR, state interferences with privacy must be authorized by a sufficiently precise law and must be necessary and proportionate to achieving a legitimate aim that is the purpose of the intrusion.[318] The *Charter*, under section 8, also recognizes that invasions of privacy by law enforcement authorities or the government are particularly damaging in a free and democratic society.[319]

This Section 5.2 ("Right to Privacy") sets out how algorithmic policing engages the right to privacy in four key ways. First, there are privacy concerns linked to the data collection that is often associated with algorithmic policing (Section 5.2.1). Second, the consolidation and processing of that data may lead to algorithmic inferences and outputs that implicate privacy rights and reinforce the need for oversight (Section 5.2.2). Further problems may arise when data is shared between law enforcement agencies, other government bodies, and the private sector (Section 5.2.3). Finally, the creation or use of data that is inaccurate may give rise to additional privacy issues (Section 5.2.4). The emergent conclusion from this analysis is that algorithmic policing technologies potentially threaten protected privacy interests in meaningful and novel ways. This prospective threat reinforces the need to establish limits on how law enforcement agencies can use technologies, such that their uses are proportional to the privacy interests at stake and governed by independent and meaningful oversight.

314 *R v Wise*, [1992] 1 SCR 527; R v Jarvis, 2019 SCC 10.

315 *R v Spencer*, [2014] 2 SCR 212 at para 38; The UN Human Rights Committee has expressed concerns about state authorities' treatment of all data gathered in "public areas" as freely accessible and in the public domain. See: United Nations Human Rights Committee, "Concluding observations on the seventh periodic report of Colombia" (17 November 2016) CCPR/C/COL/Co/7 <https://tbinternet.ohchr.org/_layouts/15/treatybodyexternal/Download.aspx?symbolno=CCPR%2fC%2fCOL%2fCO%2f7&Lang=en> at para 32.

316 International law bodies and experts have acknowledged that marginalized and minority groups are particularly vulnerable to state surveillance and violations of privacy. See e.g., United Nations General Assembly, Human Rights Council, "Report of the Special Rapporteur to the Human Rights Council on the implications of States' surveillance of communications on the exercise of the human rights to privacy and to freedom of opinion and expression" (17 April 2013) A/HRC/23/40 <https://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf> at para 51; and United Nations, General Assembly, Committee on Social, Humanitarian and Cultural Issues, "The Right to Privacy in the Digital Age" (16 November 2016) A/C.3/71/L.39/Rev.1 <https://undocs.org/A/C.3/71/L.39/Rev.1>.

317 *R v Spencer*, [2014] 2 SCR 212 at para 40; UN Human Rights Council, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at paras 5-7.

318 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 paras 23, 25 and 28. See also "The International Principles on the Application of Human Rights to Communications Surveillance", (September 2013) <https://necessaryandproportionate.org/principles>.

319 *R v Dyment*, [1988] 2 SCR 417; see also *Schreiber v Canada (Attorney General)*, [1998] 1 SCR 841.

## 5.2.1. Data Collection: Mass Surveillance and Public Space

Many algorithmic policing methods rely on the aggregation and analysis of massive volumes of data, such as personal background information, communications data, biometric data, geolocation data, or social media data. While law enforcement agencies may already possess some information or data sets that are used by algorithmic technologies, the algorithmic surveillance methods discussed in Part 4 tend to rely on, and enable, systematic collection of new data. New data collection methods obtain data from online or physical environments that law enforcement authorities assume are not protected by the right to privacy.[320] In fact, assertions by law enforcement that information is somehow publicly or freely available to them to use for law enforcement purposes are controversial and often asserted because no technology-specific law exists yet that either permits or disallows the collection in the first place.

This section specifically focuses on data that is collected from locations that law enforcement authorities often assert or assume are unprotected under the *Charter* and international human rights law. These locations will be described as "public locations" for the purpose of this analysis. This section shows how algorithmic surveillance technologies may interfere with individual privacy and, therefore, infringe section 8 of the *Charter* and the right to privacy when those technologies are used by law enforcement in the absence of judicial oversight or limits defined by necessity and proportionality.

Law enforcement usage of sophisticated surveillance technologies "for forward-looking, 'fishing expedition[s] in the hope of uncovering evidence of crime'"[321] tends to pose acute constitutional and international human rights concerns. Three guiding factors clarify why safeguards are necessary when it comes to algorithmic surveillance methods that rely on the systematic collection of data from public locations: 1) data collection by a law enforcement agency in particular, as opposed to a civilian member of the public, attracts distinct oversight requirements under privacy law; 2) the availability of new, sophisticated methods of data analysis heightens the privacy consequences created by data collection; and 3) *Charter* and human rights law protects privacy as anonymity.

**Data collection by law enforcement is distinct under privacy law**: Individuals retain a unique expectation of privacy from law enforcement agencies. This expectation means that individuals retain aright to the protection of their privacy from law enforcement even if information has already been disclosed or made public for other purposes to non-law enforcement actors.[322] While individuals

320 Algorithmic surveillance technologies that automate the collection of data tend to rely on data found in public places, as other types of data collection methods are generally already subject to the warrant and production order regime in Canada, such that collection of the data cannot be automated without violating established section 8 principles and laws.

321 *R v Jones*, [2017] 2 SCR 696, at para 74, citing *R v Finlay* (1985), 23 CCC (3d) 48 (Ont CA), at p 70; 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 paras 23, 25, and 28; UN Human Rights Council, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at paras 35 and 39.

322 UN Human Rights Council, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at para 6. The OHCHR has also stated that data sharing between law enforcement agencies and other state agencies risks violating privacy rights "because surveillance measures that may be necessary and proportionate for

do inevitably lose some degree of control over their personal information when it is shared with others, they may reasonably expect that the information will not be divulged further to (or collected by) law enforcement.[323] The right to retain protection for information that has already been shared with third parties for limited purposes flows from the fact that "all information about a person is in a fundamental way [their] own, for [them] to communicate or retain for [themselves] as [they see] fit."[324]

The constitutional protection of persons' (semi-) publicly available personal information is consistent with how public and private sector agencies are regulated under privacy legislation in Canada. For example, the Office of the Privacy Commissioner ruled in 2013 that government monitoring and collection of personal information from the personal Facebook page of Cindy Blackstock, a well-known Indigenous rights activist, violated the *Privacy Act*. The *Privacy Act* restricts the collection of personal information, "whether the personal information is available publicly or not."[325]

**The availability of more advanced methods of data analysis heightens the privacy interests engaged by the collection of data**: Analyzing whether law enforcement agencies' data collection practices interfere with an individuals' privacy requires an assessment of what the information reveals about individuals' private lives and how the law enforcement agency might use the data. Viewed in isolation, some types of publicly available personal data may not appear to reveal sensitive or personal information. For example, a single social media post or the geolocation data of a vehicle at a single moment in time is relatively less revealing than other types of sensitive data such as medical records or what is communicated in one-on-one text messages or phone communications. However, when personal information is systematically collected so it can be linked and analyzed by algorithmic surveillance technologies, the privacy implications of the data collection practice can be significant.[326] The aggregation and algorithmic analysis of data can potentially reveal a detailed picture about individuals that they may not expect to exist, let alone expect to be in the possession of the government. Indeed, it is the creation of this more detailed portrait of an individual's private life that provides the reason for algorithmic surveillance-based tools—they collect and reveal information that is otherwise unavailable to law enforcement.[327]

---

one legitimate aim may not be so for the purposes of another": 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 27.

323 *R v Wise*, [1992] 1 SCR 527; R *v Cole*, 2012 SCC 3; *R v Marakah*, 2017 SCC 59; *R v Jones*, 2017 SCC 60.

324 *R v Spencer*, [2014] 2 SCR 212 at para 40, citing *R v Dyment*, [1988] 2 SCR 417 at para 22, quoting from Government of Canada, Report of the Task Force established by the Department of Communications/Department of Justice, Privacy and Computers (Ottawa: Information Canada, 1972) at p 13; UN Human Rights Council, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at paras 7, 20.

325 Office of the Privacy Commissioner of Canada, "Aboriginal Affairs and Northern Development Canada wrongly collects information from First Nations activist's personal Facebook page" (29 October 2013) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2012-13/pa_201213_01>.

326 *R v Rogers Communications*, 2016 ONSC 70; 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> para 19.

327 This scenario assumes that the data collected and profile created of an individual is accurate and not distorted by bias or errors. Where such data or the resulting profile is inaccurate, it is not only the impacted individual's privacy rights that are engaged (due to the initial data collection), but they may also be subjected to other harms that violate their other human rights, such as being wrongfully detained or arrested,

**The *Charter* and human rights law protect privacy as anonymity**: Algorithmic surveillance methods have the potential to undermine protected forms of anonymity in public life. The Supreme Court of Canada recognized that "some degree of anonymity is a feature of much Internet activity"[328] when it held that law enforcement authorities must possess a warrant to obtain the subscriber information behind an IP address. Individuals often know little about the scope of their electronic footprint (and the extent to which electronic activity creates records at all), and they may be even less aware of the ways in which the anonymity of their electronic footprint may be undermined or extinguished through contemporary data-processing methods. The aggregation and analysis of metadata and other open source electronic records without judicial oversight could provide questionable access to information that the Supreme Court has said cannot be obtained through direct means. Privacy safeguards, including prior judicial authorization, are therefore necessary when law enforcement agencies collect and analyze content and metadata that is captured from online platforms or other environments where individuals operate freely with relative anonymity.

The social media surveillance methods described in Section 4.3 ("Algorithmic Surveillance Tools") illuminate the aforementioned three reasons why such technologies need to be contained through oversight and limits that ensure necessity and proportionality of use. The RCMP has taken the position that they can use online social media surveillance because this form of surveillance relies on open source, or publicly available data.[329] However, the RCMP's position presents an oversimplification of the privacy interests at stake. First, when individuals use social media, they do not expect to have their information systematically collected by law enforcement.[330] Second, social media platforms contain a wealth of information about individuals' intimate lives, personal relationships, and everyday activities that is generally not provided by users for law enforcement purposes. Professor Teresa Scassa has pointed out that police often access this information in ways that do not alert users to the fact that they are being monitored or having their data used in a police investigation.[331] As noted in Section 4.2 ("Person-Focused Algorithmic Policing"), the SPPAL has indicated that it intends to start mining social media data to enable its person-focused algorithmic policing technology, with some such collections potentially including social media data captured from vulnerable individuals such as minors. The privacy interests at stake are further heightened when social media data is systematically collected over time and analyzed to generate an even more revealing picture of an individual. Third, online social media engagement is an example of the freedom that anonymity enables in public space. In online

---

thus violating their rights to liberty and to be free from arbitrary detention.

328 *R v Spencer*, [2014] 2 SCR 212 at para. 48.

329 Bryan Carney, "'Project Wide Awake': How the RCMP Watches You on Social Media", *The Tyee* (25 March 2019) <https://thetyee.ca/News/2019/03/25/Project-Wide-Awake/>.

330 *R v Spencer*, [2014] 2 SCR 212 at para 38-50: "[t]he mere fact that someone leaves the privacy of their home and enters a public space does not mean that the person abandons all of his or her privacy rights, despite the fact that as a practical matter, such a person may not be able to control who observes him or her in public."

331 Teresa Scassa, "Law Enforcement in the Age of Big Data and Surveillance Intermediaries: Transparency Challenges" (December 2017) 14:2 *Scripted* 239 at 251, <https://script-ed.org/wp-content/uploads/2017/12/scassa.pdf>.

environments, activity occurs within a "situational landscape"[332] in which individuals do not expect to be systematically surveilled, similar to their expectation of being able to blend into a crowd. While individuals may be aware that their social media profiles are in the public domain, it does not follow that they expect police services to be systematically watching.

Given the potential privacy interests that are engaged when law enforcement conducts mass data collection, a key question that arises from section 8 of the *Charter* and international human rights law is whether pre-emptively collecting data in the hopes of forecasting potential crime or for general information gathering is either necessary or proportionate.[333] Section 8 generally requires that whenever law enforcement actors intrude into a protected sphere of privacy, they must have reasonable grounds to believe that the information sought will reveal evidence of a crime.[334] Pre-emptive fishing expeditions could hardly satisfy that standard. When interpreting *Charter* standards, it bears reiterating that the principles of necessity and proportionality are touchstones in applying many private and public sector privacy laws.[335]

Judicial oversight must also regulate preservation of the public interests at stake when law enforcement seeks to rely on algorithmic surveillance technologies.[336] 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 independent civilian oversight agencies.[337] 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 forms of privacy be subject to meaningful oversight.

332 *R v Wise*, [1992] 1 SCR 527.

333 *R v Jones*, [2017] 2 SCR 696 at para 74, citing *R v Finlay* (1985), 23 CCC (3d) 48 (Ont CA), at p 70.

334 *R v Rogers Communications*, 2016 ONSC 70. There are, of course, context-specific exceptions to this general proposition where the public interests at stake may warrant a departure from this principle (such as various exigent circumstances relating to public safety and destruction of evidence).

335 For example, the Ontario Court of Appeal ruled in 2007 that a by-law that required pawn shops to report the names of all customers vending goods to the shop was invalid under MFIPPA. This included a ruling that the collection was not justified under law enforcement purposes either because the "transmission [of the data] occurs before there is any basis to suspect that the goods that were sold … were stolen and is made with no limit as to its use by the police or by those to whom the police may share the information". *Cash Converters v Oshawa*, 2007 ONCA 502, at para 38.

336 *Hunter v Southam*, [1984] 2 SCR 145; *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.

337 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.

## 5.2.2. Data Processing: Data Analytics and Algorithmic Outputs

Data collection and data processing activities by law enforcement raise related, but distinct, privacy concerns. Whereas Section 5.2.1 ("Data Collection: Mass Surveillance and Public Space") addressed the privacy implications linked to the data collection practices associated with algorithmic policing technology, this section (Section 5.2.2) focuses on law enforcement activities that involve the processing and analysis of information that law enforcement authorities already control. Data processing activities engage unique privacy interests and, therefore, must be necessary and proportionate and in the service of a legitimate purpose.[338]

Data analytics can reveal insights about individuals and their identities, movements, interests, beliefs, and social networks. Such insights are drawn not only from data, but from metadata—information about phone calls, emails, social media posts, and other communications apart from the content of the messages (e.g., time, date, location, sender, or recipient)—which can give rise to inferences about individuals' private lives when aggregated and analyzed.[339] Pattern recognition algorithms can draw out information about protected characteristics, such as race or ethnicity, religious belief, age, gender, and sexual orientation, even when this data is not explicitly included in the original data sets.[340] Privacy rights therefore attach not only to data that is collected but also to inferences drawn from combined pieces of data and to outputs of algorithmic processing.[341] The existence of current algorithmic processing methods raises new questions about the extent to which personal information in existing police databases that has been used for traditional policing methods (e.g., conducting isolated queries at the officer level in a specific investigation) should be used in the service of algorithmic policing technology. The more numerous and detailed inferences that may arise from the greater technological capability of algorithmic analysis heighten the privacy interests at stake.[342] Many police databases predate algorithmic technologies and, as discussed in Section 2.2 ("Bias and Inaccuracies in Police

338 UN Human Rights Council, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at para 29; *Re (X)*, 2016 FC 1105 at paras 79 and 265.

339 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 19; Andrew Ferguson, *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement* (New York: NYU Press, 2017), at 119-120. <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/>; *R v Rogers Communications*, 2016 ONSC 70; *R v Spencer*, [2014] 2 SCR 212.

340 See the discussion of proxy data in Section 5.4.2 ("Algorithmic Bias and 'Feedback Loops of Injustice'"), including examples of how algorithms have been used to infer race, gender, and medical conditions from data such as postal codes, online search terms, Facebook "likes", and purchasing history. See also UN General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/73/348 (29 Aug 2018) <https://undocs.org/A/73/348> at para 34 ("AI methods on social media platforms are used to infer and generate sensitive information about people that they have not provided or confirmed, such as sexual orientation, family relationships, religious views, health conditions, or political affiliation").

341 UN Human Rights Council, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at para 30.

342 For example, law enforcement actors are often called to attend at scenes involving criminal complaints, but so too are they called to attend at a host of non-criminal incidents involving medical issues, mental health crises, or other family-related matters. Information relating to such occurrences may well make it into a police database, but it is far from clear what legitimate law enforcement purpose would enable services from making use of personal data for pattern recognition algorithms or other algorithmic assessments. See also the public outcry arising when individuals learned that their photos and images shared in one context were repurposed for use in training data sets for facial recognition algorithms: Olivia Solon, "Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent", NBC News (12 March 2019) <https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921>.

Data"), may contain data that are inappropriate for such technologies to work upon. In recognition of such concerns, a representative from the SPPAL noted that their team has been considering using machine learning to create synthetic data sets; these data sets would then be used to test their algorithmic models and simulate the outcomes of adjusting different variables.[343] This would, in theory, allow SPPAL to reduce the need to use data from real people and to mitigate associated privacy risks. However, even synthetic data sets may engage privacy concerns, due to the potential need to use real data to train the algorithm so that it can generate useful synthetic data sets.[344]

While section 8 most visibly regulates law enforcement's collection of information by requiring agents to obtain a search warrant prior to conducting searches and seizures in criminal investigations, constitutional safeguards under section 8 also protect the privacy interests that are engaged by the use of seized information.[345] In short, section 8 protections may be engaged by algorithmic policing technologies based upon how they process collected data. For example, police services' use of facial recognition systems to identify images of unknown individuals poses privacy issues that are distinct as compared to the services' possession of databases of mug-shot photographs. Similarly, ALPR technology poses unique privacy issues at the time that it is used, as compared to noting an individual's location and licence plate in a police notebook. In both cases, the heightened interests arise from the combination of existing privacy stakes and the more advanced surveillance and data analysis capability being used by law enforcement agencies.[346]

Thus, while much of section 8 jurisprudence focuses on the regulation of data collection, the courts and privacy regulators will likely be increasingly required to consider what safeguards are necessary if or when law enforcement agencies use algorithmic tools to process collected information to derive insights into people and their alleged activities.

### 5.2.3. Data Sharing: Public Bodies and Private Companies

Surveillance and data collection that is necessary and proportionate for one legitimate objective may not be for another.[347] In 2012, BC's Information and Privacy Commissioner found that law enforcement's

343 Interview of a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) by Cynthia Khoo (23 July 2019).

344 See e.g., Information and Privacy Commissioner for British Columbia, "Investigation Report P19-01: Full Disclosure: Political parties, campaign data, and voter consent", (6 February 2019) <https://www.oipc.bc.ca/investigation-reports/2278> at 25-26 (regarding Facebook's "Lookalike" feature).

345 *R v Reeves*, 2018 SCC 56; *Wakeling v. United States of America*, 2014 SCC 72.

346 For example, the Information and Privacy Commissioner for British Columbia found that any subsequent use of "non-hit" information collected under a police ALPR program was unlawful under the applicable privacy legislation: Office of the Information & Privacy Commissioner, "Investigation Report F12-04 – Use of Automated Licence Plate Recognition Technology by the Victoria Police Department" (15 November 2012), <https://www.oipc.bc.ca/investigation-reports/1480>. Law enforcement agencies also increasingly have data available to them through private surveillance networks, such as a licence plate tracking database by the company Digital Recognition Network (DRN). DRN's database purportedly contains nine billion licence plate scans "crowdsourced by hundreds of repo men who have installed cameras that passively scan, capture, and upload the license plates of every car they drive by to DRN's database", allowing both private investigators and law enforcement to "track the movements of car owners over long periods of time." Joseph Cox, "This Company Built a Private Surveillance Network. We Tracked Someone With It", *VICE Motherboard* (17 September 2019) <https://www.vice.com/en_ca/article/ne879z/i-tracked-someone-with-license-plate-readers-drn>.

347 UN Human Rights Council, "The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for

use of facial recognition technology and driver's licence photographs, which were held by the province's public automotive insurer, violated provincial privacy legislation.[348] The public insurer could not permit use of its database for a purpose that had not been disclosed to customers;[349] thus, law enforcement was prohibited under the legislation from repurposing the driver's licence database into a policing tool without court authorization.[350]

Person-focused predictive policing depends on building a detailed profile of a person by combining different types of data and information about them to assess potential future behaviour or risk. One way that police services obtain data, which they may not have access to otherwise, is by collecting it from other entities, including private companies and government bodies, that have collected the data for their own purposes.

> *How do you monitor what you do with the data? For example, around carding [by police services], people are very concerned with what they do with the data. Where is the data being shared? Who else has access?*
>
> *- Black Legal Action Centre (BLAC)*[351]

The Hub model of policing (see **In Focus #3: The Hub Model of Community Safety**) serves as an example of the privacy concerns that are associated with data sharing between law enforcement authorities and other third-party actors. This model is a risk assessment program that could be considered a precursor of a kind of algorithmic policing technology. The Hub model brings together school staff, social service agencies, health providers, and police services to share information about individuals who are believed to be at risk.[352] The information compiled in Hub databases tends to be

---

Human Rights" (30 June 2014) A/HRC/27/37 <https://undocs.org/A/HRC/27/37>, at para 27; Office of the Privacy Commissioner of Canada, "Canada Border Services Agency – Scenario Based Targeting of Travelers – National Security" (2017) <https://www.priv.gc.ca/en/opc-actions-and-decisions/audits/ar-vr_cbsa_2017/>; Office of the Information & Privacy Commissioner, "Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia" (16 February 2012) <https://www.oipc.bc.ca/investigation-reports/1245>; Re (X), 2016 FC 1105; *Wakeling v. United States of America*, 2014 SCC 72. Generally speaking, under the *Criminal Code* and related privacy legislation, many court-authorized seizures place constraints on the retention and sharing of information obtained. For example, Part VI of the *Criminal Code* makes it a criminal offence to share intercepted communications unless authorized by the *Code*.

348 *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165.

349 Office of the Information & Privacy Commissioner, "Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia" (16 February 2012) <https://www.oipc.bc.ca/investigation-reports/1245>.

350 *Ibid*. At the time of its investigation, the Information and Privacy Commissioner found that in the years 2011-2012, the insurer had received 15 requests directly from police forces for assistance in identifying individuals, and on at least one occasion, the insurer had provided police with the possible identity of an individual based only on a police request; no warrant or subpoena was required for the disclosure: Office of the Information & Privacy Commissioner, "Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia" (16 February 2012) <https://www.oipc.bc.ca/investigation-reports/1245>, at para 96.

351 Interview of Black Legal Action Centre by Cynthia Khoo (12 July 2019).

352 Nathan Munn, "Canada's 'Pre-Crime' Model of Policing Is Sparking Privacy Concerns", *VICE Motherboard* (19 January 2017) <https://www.vice.com/en_us/article/mg7w4x/canada-hub-and-cor-policing-privacy-police>.

extremely sensitive; it includes the individual's age group, sex, location, and over a hundred factors, such as suspected mental health issues, alcohol and drug use, "negative peers," obnoxious or disruptive behaviour, missing school, physical health, and poverty, that supposedly indicate risk.[353]

The Hub model's data-sharing practices contribute to and rely on risk-driven tracking databases that are accessible to and used by law enforcement actors. Such uses include assessing and analyzing database information using algorithmic methods, such as those currently being developed at the SPPAL.[354] These programs give rise to constitutional and privacy issues despite efforts to build in privacy filters, which are designed to screen data at various stages to determine levels of sharing and to assuage privacy concerns about inappropriate sharing or use of the information.[355] For example, the Saskatchewan Information and Privacy Commissioner found that the de-identifying measures in the Hub program in Saskatchewan were deficient.[356] Moreover, systematic data sharing with law enforcement actors has constitutional ramifications, namely, the potential violation of section 8 rights given law enforcement's ability to access individuals' personal data through the Hub without safeguards such as prior judicial authorization. The law already provides a potential remedy: non-police actors in the Hub program may become bound by more stringent *Charter* obligations under certain circumstances.[357] Non-police actors can sometimes become police agents who are bound by the same constitutional limits as law enforcement authorities with respect to the collection or seizure of private information.[358] Specifically, where non-law enforcement actors search or seize private information at the request of law enforcement, section 8 protections apply to the actions of the police agent (including the need to

353 Nathan Munn, "Police in Canada Are Tracking People's 'Negative' Behavior In a 'Risk' Database", *VICE Motherboard* (27 February 2019) <https://www.vice.com/en_us/article/kzdp5v/police-in-canada-are-tracking-peoples-negative-behavior-in-a-risk-database>.

354 Nathan Munn, "Canada's 'Pre-Crime' Model of Policing Is Sparking Privacy Concerns", *VICE Motherboard* (19 January 2017) <https://www.vice.com/en_us/article/mg7w4x/canada-hub-and-cor-policing-privacy-police>; Nathan Munn, "Police in Canada Are Tracking People's 'Negative' Behavior In a 'Risk' Database", *VICE Motherboard* (27 February 2019) <https://www.vice.com/en_us/article/kzdp5v/police-in-canada-are-tracking-peoples-negative-behavior-in-a-risk-database>.

355 Third-party agencies must themselves independently comply with applicable privacy legislation, which regulates the collection, retention, use, and disclosure of personal information or personal health information. The UN High Commissioner for Human Rights has suggested that "use limitations" should be in place to control the sharing of data between law enforcement and other state organs, as information collected for one purpose may not be necessary and proportionate for another (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 paras 26-27). This section instead looks at what obligations may arise under the *Charter* where such third parties interact with law enforcement entities in a manner such that their conduct gives rise to *Charter* rights or violations.

356 Saskatchewan Information & Privacy Commissioner, "Investigation Report 105/2014: Community Mobilization Prince Albert" (10 November 2014) <https://oipc.sk.ca/assets/foip-investigation-105-2014.pdf>, at pages 11-18.

357 *R v Orlandis-Habsburgo*, 2017 ONCA 649; *R v Pohoretsky*, [1987] 1 SCR 945; *R v Dersch*, [1993] 3 SCR 768 at para 20. A law enforcement representative in Canada advised during a research interview that Hub tables in Toronto receive the majority of their cases through referrals from the Toronto Police Service (TPS), suggesting that many individuals may be moved out of the law enforcement context and transitioned to one or more social service agencies with a view of providing support, as opposed to social service agencies referring cases to law enforcement. Interview of a law enforcement representative in Canada by Yolanda Song & Cynthia Khoo (28 June 2019). However, this does not alleviate concerns with those who seek social services and are ultimately drawn into the criminal justice system through being brought to a Hub.

358 *R v Orlandis-Habsburgo*, 2017 ONCA 649; *R v Pohoretsky*, [1987] 1 SCR 945; *R v Dersch*, [1993] 3 SCR 768 at para 20; and *R v Jarvis*, [2002] 3 SCR 757. Additionally, mandatory third-party retention provisions are considered neither necessary nor proportionate measures under international human rights law with respect to the right to privacy, particularly without the inclusion of limitations on how the retained data may be later used. 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 paras 26-27.

obtain prior judicial authorization).[359] These safeguards apply to the police agent because the criminal law enforcement arm of the state cannot rely on the seizure of private data by other governmental actors to circumvent the guarantees of section 8.[360]

Even if an agency relationship between police and non-police actors does not arise, if, on its own initiative, a governmental actor conducts an investigation for a criminal law purpose, individuals under investigation would again be entitled to the same *Charter* protections that arise in the course of a police investigation. These *Charter* rights would include the right to silence, the right to counsel, and the protection against unreasonable searches and seizures. Prior judicial authorization would be required before the government agent seized an individual's personal records and shared them with law enforcement agencies.[361]

Consequently, profound constitutional ramifications would arise if public service personnel (e.g., teachers, social workers, or health care providers) were transformed into police agents under the law, which a *Charter* analysis may require as a result of their systematic data sharing practices with police services under a Hub program. Such data sharing arrangements could also erode public trust in essential social services and public service employees or deter vulnerable individuals from accessing such services.[362]

Similar constitutional issues and privacy concerns may arise with other algorithmic policing tools when law enforcement agencies seek access to data sets collected by private companies.[363] For example, the Calgary Police Service (CPS) uses software from Palantir Technologies that can integrate third-party commercial information, such as financial records, shipping records, telecommunications information, and wire transfers, with police databases,[364] although the CPS did not appear to be employing these capabilities, based on a research interview conducted in May 2019.[365] Facial recognition tools used by law enforcement agencies can be used to process images taken from private individuals' or businesses' databases or surveillance systems.[366] These information-sharing arrangements are

359 *Ibid* and *R v Orlandis-Habsburgo*, 2017 ONCA 649. In some circumstances, the individual who is the subject of "investigation" and faces potential criminal jeopardy may be entitled to other *Charter* protections such as the right to counsel: *R v Jarvis*, [2002] 3 SCR 757.

360 *R v Colarusso*, [1994] 1 SCR 20.

361 *R v Jarvis*, [2002] 3 SCR 757.

362 See, for example, *R v Pohoretsky*, [1987] 1 SCR 945; *R v Dersch*, [1993] 3 SCR 768 at para 20.

363 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 27.

364 Calgary Police Service, "Palantir Platform Capabilities Brief" (obtained through freedom of information request 18-G-1921); Calgary Police Service, "Calgary Police Service Palantir Implementation Privacy Impact Assessment", at p 47 (obtained through freedom of information request 18-G-1921).

365 Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).

366 Hannah Devlin, "'We are hurtling towards a surveillance state': the rise of facial recognition technology", *The Guardian* (5 October 2019), <https://www.theguardian.com/technology/2019/oct/05/facial-recognition-technology-hurtling-towards-surveillance-state>. For an example of far-reaching facial recognition technology that law enforcement agencies have already been using in the United States, developed and sold by a company called Clearview AI, see: Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It", *New York Times* (18 January 2020) <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

vulnerable constitutionally because customers who might have consented to having a private business collect their image for customer service purposes have not done so on the basis that they were also consenting to sharing their information with police services for law enforcement purposes.[367] Commercial privacy legislation in Canada—governed by the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) and provincial counterparts—also does not authorize disclosure without consent to law enforcement, unless law enforcement has "lawful authority" to access the information.[368] "Lawful authority" is determined outside of this privacy legislation by reference to section 8 of the *Charter*, including its standards for reasonable expectations of privacy.[369]

If other Canadian law enforcement agencies develop algorithmic policing tools that depend on data-sharing practices between private sector entities and law enforcement agencies, constitutional issues will be engaged. Data sharing between private companies and law enforcement may render data collection and sharing activities by the private company unlawful or unconstitutional, regardless of whether the data sharing occurred as discrete instances or as part of a formalized or routine sharing system with law enforcement.[370] Law enforcement, in effect, cannot collect personal data and information from private businesses that police officers could not otherwise collect directly, and any efforts to do so may represent an unlawful circumvention of privacy and constitutional laws that are in place to protect citizens from potential abuses of power by the state. Allowing law enforcement agencies to access data they could not constitutionally obtain, through a private company that obtained the data legally, could represent an unconstitutional expansion of the state's ability to monitor and track individuals without justification or judicial oversight.

### 5.2.4. Data Accuracy: Inaccurate Data and Inaccurate Algorithms

Data accuracy is a core privacy principle in international human rights and Canadian privacy law. The ICCPR protects the right of individuals to request the rectification of incorrect personal data that is collected or processed by public or private actors.[371] Domestic privacy legislation also generally requires public institutions to take reasonable steps to ensure the accuracy of the personal

367 In many cases, private business may not have obtained the requisite consents to collect facial images for even non-law enforcement purposes: Julia Carrie Wong, "Google reportedly targeted people with 'dark skin' to improve facial recognition", *The Guardian* (3 October 2019), <https://www.theguardian.com/technology/2019/oct/03/google-data-harvesting-facial-recognition-people-of-color>.

368 See e.g., *Personal Information Protection and Electronic Documents Act*, RSC 2000, c 5, s 7(3)(c.1).

369 *R v Spencer*, [2014] 2 SCR 212 at paras 60-66, considering the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5.

370 *R v Orlandis-Habsburgo*, 2017 ONCA 649 at paras 31-33 and 98-115; *R v Cole*, 2012 SCC 53; *R v Reeves*, 2018 SCC 56; *R v Spencer*, [2014] 2 SCR 212.

371 UNHRC, *General Comment No 16 on Article 17 (Right to Privacy)*, 32nd Sess, adopted 8 April 1988, UN Doc HRI/GEN/1/Rev9 (Vol I), at para 10 <https://undocs.org/HRI/GEN/1/Rev.9(Vol.I)>. See also UN Human Rights Council, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018), A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at para 29. The Organisation for Economic Co-operation and Development (OECD), of which Canada is a member, has also published privacy guidelines that call for collected personal data to be accurate, complete, and up-to-date; see Organisation for Economic Co-operation and Development, "OECD Guidelines governing the protection of privacy and transborder flows of personal data" (1980, revised in 2013) <http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>, at para 8.

information that they collect and use.[372] Similar obligations apply to private vendors of policing technology or private sector actors that provide information to the police.[373]

Data accuracy rights are not, however, the only issue engaged by inaccurate data. Such inaccuracies may lead to high-stakes errors when processed by algorithmic policing technologies. The reliability of algorithmic tools cannot be assumed until each tool is independently and rigorously tested to confirm that it meets an acceptable level of reliability. Ultimately, the accuracy of the input data will inevitably inform the overall reliability of the algorithmic tool.

In Canada, police services regularly use information that may be inaccurate, unreliable, or based on biased generalizations. The Canadian Police Information Centre (CPIC), a central database that stores criminal record information and is accessible by government departments and law enforcement agencies across the country, has been widely criticized for being out of date and inaccurate.[374] The Ontario Court of Justice has declined, for example, to take judicial notice of the reliability of the database and affirmed that it is the government's onus to establish the reliability of the information if it wants to rely on it when interfering with an individual's liberty.[375] Social media data and other open source information can be unreliable but is accessed by law enforcement with little oversight.[376] Young people may be labelled in police databases as gang-involved, based on unvalidated information from school staff or local service providers,[377] or on information that may be based on bias or assumptions about race, neighbourhood, and friends.[378] On their own, these errors can lead to grave consequences for the rights and lives of individuals and their families.[379] Compounding such errors by feeding them

372 See, e.g., *Privacy Act*, RSC 1985, c P-21, s 6(1); *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25, s 35 (Alberta); *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, s 28 (British Columbia); *The Local Authority Freedom of Information and Protection of Privacy Act*, SS 1990-91, c L-27.1, s 26 (Saskatchewan).

373 See *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5; and Office of the Privacy Commissioner of Canada, "Accuracy" (May 2013) <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_04_accuracy/>.

374 Alyshah Hasham, "Criminal-record database spotty and out of date, lawyers lament", *The Toronto Star* (9 December 2016) <https://www.thestar.com/news/crime/2016/12/09/criminal-record-database-spotty-and-out-of-date-lawyers-lament.html >; Brigitte Bureau, "RCMP database remains out of date, police and prosecutors say", *CBC News* (10 March 2015) <https://www.cbc.ca/news/politics/rcmp-database-remains-out-of-date-police-and-prosecutors-say-1.2989397>.

375 *R v White*, 2006 ONCJ 147 at para 28.

376 Nathan Munn, "Canadian Cops Will Scan Social Media to Predict Who Could Go Missing", *VICE Motherboard* (17 April 2019) <https://www.vice.com/en_us/article/mb8jzp/canadian-cops-will-scan-social-media-to-predict-who-could-go-missing>; Bryan Carney, "'Project Wide Awake': How the RCMP Watches You on Social Media", *The Tyee* (25 March 2019) <https://thetyee.ca/News/2019/03/25/Project-Wide-Awake/>; Amanda Pfeffer, "Doubts swirl around new Ottawa police nerve centre", *CBC News* (31 May 2017) <https://www.cbc.ca/news/canada/ottawa/opsoc-ottawa-police-strategic-operations-centre-1.4138242 >; Calgary Police Service, "Internet Investigations and Criminal Intelligence Ref #IN-026", at p 47 (obtained through freedom of information request 18-G-1921).

377 Interview of a researcher at a Toronto-based community service provider involved in criminal justice issues, by Yolanda Song & Cynthia Khoo (8 May 2019).

378 Nathan Munn, "This B.C. city is tackling gang violence by profiling high school students", *VICE Motherboard* (7 January 2019). <https://www.vice.com/en_ca/article/59vv8x/this-bc-city-is-tackling-gang-violence-by-profiling-high-school-students>.

379 See Section 2.1 ("Criminal Justice and Systemic Discrimination in Canada"), discussing the impact of criminal justice processes on individuals.

into algorithmic policing tools further magnifies this risk as it further raises the possibility that the data is used and acted upon by law enforcement agencies in their decision making and investigations.[380]

> *I worry about systems that may be built on limited or flawed data.*
>
> *- Jonathan Rudin (Lawyer, Author, and Program Director at Aboriginal Legal Services)*[381]

Despite the potential consequences and harms of law enforcement relying on inaccurate data in criminal investigations, some Canadian provinces exempt personal data that is collected for law enforcement purposes from data accuracy obligations.[382] Even where the law does impose standards of accuracy on information used by police, it is not clear how this requirement can be rigorously enforced. Practitioners of criminal law regularly deal with cases that involve individuals who have had their lives impacted in any number of ways by errors in police records and databases. In many cases, by the time the error is discovered and corrected—often at the initiative of the affected individual — the consequence(s) of the mistake(s) have already occurred (e.g., a wrongful arrest or charge leads to the loss of an employment opportunity due to an erroneous criminal record check). Moreover, little meaningful remedy is easily available. When data is shared within government or between public and private entities, it can be incredibly difficult for individuals to even identify who holds what information about them.[383]

The *Charter* also protects individuals who have been subjected to police powers (e.g., arrest or detention) or invasions of privacy as a result of erroneous information. In order to justify interferences with liberty or privacy, the state must show that there were reasonable grounds to justify the interference. The reasonable grounds standard to justify interference with privacy or liberty requires an individualized assessment,[384] and an inquiry into whether any information relied upon to justify an interference is sufficiently reliable and credible. Notably, even aside from data inaccuracy problems, it is unlikely that the reasonable grounds standard could ever be satisfied on the basis of algorithmic predictions alone.[385] By nature, predictive algorithms supplant individually assessed characteristics

380 See Section 2.2 ("Bias and Inaccuracies in Police Data").

381 Interview of Jonathan Rudin by Cynthia Khoo & Yolanda Song (8 May 2019), speaking on behalf of himself only, in a personal capacity.

382 *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31, s 40(3); *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c M.56, s 30(3).

383 UN Human Rights Council, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29> at para 13. For example, given "people generally have little idea how, why, and for what reasons their information is collected, processed, and disclosed to other parties by the companies they entrust with their data", a web application called Access My Info (AMI) was designed by Open Effect and the Citizen Lab to help individuals to create justified requests for copies of their personal information from service providers: https://accessmyinfo.ca/#/.

384 *R v Chehil*, 2013 SCC 49 at para 40-43; *R v Kang-Brown*, [2008] 1 SCR 456. This problem is discussed further below in Section 5.5.1 ("Algorithmic Policing and Generalized Suspicion").

385 "[T]the suspicion held by the police cannot be so broad that it descends to the level of generalized suspicion, which was described by Bastarache J., at para. 151 of A.M., as suspicion 'that attaches to a particular activity or location rather than to a specific person'." *R v Chehil*,

with broad-based statistical generalizations.[386] Reliance on inaccurate information in algorithmic policing technologies presents additional constitutional danger. An "arrest based on a source the reliability of which, in the end, is unknown cannot be said to be objectively reasonable."[387] Notably, in the context of CPIC cases, there are, in case law, conflicting treatment of individuals who have been arrested on the strength of an error in the CPIC database. In some cases, courts have declined to find that any *Charter* violation occurred as a result of the erroneous information so long as the officer who reviewed the CPIC data believed that it was valid at the time of arrest.[388]

The analysis of the CPIC database case law highlights some of the issues that arise when law enforcement seeks to use algorithmic policing technologies that rely on existing police databases that are out of date or inaccurate. This is an example of what is sometimes referred to as the "garbage in, garbage out" problem. If police data sets are prone to error and fed into algorithmic policing technologies, subsequent forecasts provided by those algorithms (i.e., predictions of criminal activity from person-focused or location-focused algorithmic policing tools) would be tainted by those errors. Law enforcement agencies' reliance on error-tainted algorithmic forecasts would risk unjustifiable interferences with *Charter*-protected interests such as privacy or liberty, if law enforcement authorities act on those algorithmic predictions. While it is less likely that courts will be quick to assume that reliance on novel technologies is objectively reasonable in the absence of independent evidence showing the reliability of such tools, the CPIC-related error cases also demonstrate the vulnerability that individuals have to being harmed by inaccurate data. Meaningful access to remedies for errors may be elusive.

Given that personal information derived through data processing is also protected by privacy legislation, applicable accuracy obligations are relevant not only to input data containing personal information, but also algorithmic outputs as well. In *Ewert v. Canada*, the Supreme Court of Canada found that the Correctional Service of Canada (CSC) failed in its obligation to "take all reasonable steps to ensure that any information about an offender that it uses is as accurate, up to date and complete as possible," by relying on certain risk assessment tools to make determinations about Mr. Ewert.[389] The CSC used these tools despite long-standing awareness that the tools possibly exhibited cultural bias and that their validity was seriously in question when applied to Indigenous offenders, of whom Mr. Ewert was one.[390]

---

2013 SCC 49 at para 28.

386 See e.g., "As Professor Frederick Schauer explains, decision makers that rely on statistically sound but nonuniversal generalizations 'are being simultaneously rational and unfair' because certain individuals are 'actuarially saddled' by statistically sound inferences that are nevertheless inaccurate." Solon Barocas & Andrew D Selbst, "Big Data's Disparate Impact" (2016) 104 California Law Review 671 at 688.

387 *See R v White*, 2006 ONCJ 147 at para 27.

388 *R v Clark*, [2003] OJ No 1323 (CJ); *R v Wilson*, [2003] OJ No 4465 (Sup Ct).

389 *Ewert v Canada*, 2018 SCC 30 at 3. In this case, the data accuracy obligation resulted from section 24(1) of the *Corrections and Conditional Release Act* (SC 1992, c 20), which closely resembles section 6(2) of the federal *Privacy Act*: "A government institution shall take all reasonable steps to ensure that personal information that is used for an administrative purpose by the institution is as accurate, up-to-date and complete as possible." Privacy Act, RSC, 1985, c P-21, s 6(2).

390 *Ewert v Canada*, 2018 SCC 30.

Using algorithms to analyze social media information for risks of future criminal activity raises similar concerns with respect to cultural context.[391] After reviewing the Hub program in Saskatchewan, Saskatchewan's Information and Privacy Commissioner concluded that social media data should not be subject to collection through an algorithmic technology by public bodies or a basis for a risk determination because social media is a source of inaccurate information.[392] The use of automated tools is difficult when analyzing language that is highly context-dependent and culturally specific, which may not be adequately reflected in the data sets used to train the algorithms.[393] For example, Professor Andrew Ferguson notes that keywords related to gangs and shootings ("hit", "run", "strike", "cap", and "park") can also relate to baseball.[394] An algorithm that cannot distinguish between the two contexts may draw police attention to individuals, based on innocuous communications, and subject those individuals to privacy violations. This risk was acknowledged by a representative of the SPPAL, who stated that researchers were aware of the risk associated with the concept of 'garbage in, garbage out' and the novel nature of the research that they are doing.[395] However, despite their awareness of this issue and of the Information and Privacy Commissioner's findings and recommendations in respect of social media data, the SPPAL has nonetheless indicated it intends to incorporate low-accuracy data sources such as social media inputs.[396]

Public policy interests, the goal of effective law enforcement, and privacy norms and applicable legislation all reinforce the need for appropriate safeguards to ensure that police databases and algorithmic processing methods provide law enforcement with accurate and reliable information. It is only from such information that the agencies should make decisions that will impact individuals, victims, and the public at large. Developing robust privacy safeguards requires investing resources

391 For example, in the United States, researchers who claimed to develop an algorithm that identified gang members based on their Twitter posts—in particular, based on their use of "tough talk", certain words and emojis, and links to rap music videos—were criticized for the potentially discriminatory assumptions underlying the tool: Jordan Pearson, "Researchers Claim AI Can Identify Gang Members on Twitter", *Vice* (1 November 2016), <https://www.vice.com/en_us/article/mg7kgx/researchers-claim-ai-can-identify-gang-members-on-twitter>.

392 Community Mobilization Prince Albert (Re), 2014 CanLII 81867 (SK IPC) at para 32-38.

393 See e.g., UN General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/73/348 (29 Aug 2018) <https://undocs.org/A/73/348> at para 15. See also the wide range of research demonstrating the unreliability of AI to distinguish nuance in the field of content moderation on social media platforms, e.g., Natasha Duarte, Emma Llanso & Anna Loup, "Mixed Messages? The Limits of Automated Social Media Content Analysis" (November 2017), Center for Democracy & Technology <https://cdt.org/wp-content/uploads/2017/11/Mixed-Messages-Paper.pdf>; Maarten Sap et al, "The Risk of Racial Bias in Hate Speech Detection" (Paper delivered at Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics, Florence, Italy, 28 July 2019) 1668; and Md Abul Bashar et al, "Misogynistic Tweet Detection: Modelling CNN with Small Datasets" in R Islam et al, eds, *Data Mining: 16th Australasian Conference, AusDM 2018, Revised Selected Papers (Communications in Computer and Information Science,* Volume 996).

394 Andrew Ferguson, The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement (New York: NYU Press, 2017), at 126.

395 The SPPAL representative also noted that the novel nature of algorithmic policing research in Canada is another reason to ensure researchers' and developers' models are as transparent as possible: "Is this data that's being used even correct? Given that this work is so new, we have nothing to compare it against. But if I publish something in a criminal justice journal, someone can look at it and say, 'Hey, CPIC is two years behind', or, 'Here's some things you didn't capture for violent offenders.'" Interview of a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) by Cynthia Khoo (23 July 2019).

396 Dr. Kiera Stockdale, Saskatoon Police Service, "Saskatchewan Police Predictive Analytics Lab Missing Persons Project: Year One", Defence Research and Development Canada (February 2019), <http://cradpdf.drdc-rddc.gc.ca/PDFS/unc335/p809812_A1b.pdf>.

in the proper maintenance of police databases that are relied on (as is already requested by police and prosecutors).[397] Further, law enforcement agencies must integrate and rely on the expertise of technologists who can provide objective guidance on the reliability and accuracy of data processing methods.

397 Brigitte Bureau, "RCMP database remains out of date, police and prosecutors say", *CBC News* (10 March 2015) <https://www.cbc.ca/news/politics/rcmp-database-remains-out-of-date-police-and-prosecutors-say-1.2989397>.

# Facial Recognition Technology and the Erosion of Privacy Rights

Facial recognition serves as an example of how algorithmic policing technologies can pose significant threats to the right to privacy.[398] Given that facial recognition technology is "a tool that could end [the] ability to walk down the street anonymously,"[399] there is a critical need for public dialogue, regulation, and clear limits surrounding its potential use.

Facial recognition technologies can enable law enforcement to track and de-anonymize individuals going about their daily activities and, as such, significantly heightens the privacy interests in one's facial image.[400] Legal protection under human rights and constitutional law applies as a result.[401] However, like other algorithmic policing technologies considered in this report, facial recognition tools involve data collection, data processing, and data sharing methods that have not yet been the extensive focus of case law, out of which will emerge detailed rules that law enforcement authorities must follow. Even in the absence of such rules, law enforcement authorities are required to adhere to human rights and constitutional protections (such as those applicable to the biometric information associated with facial images) regardless of how well those rights have been fleshed out in Canadian courts. Regulation through specific laws can address the existing uncertainty in this area by setting out clear and necessary limits.

As noted in Section 5.2.1 ("Data Collection: Mass Surveillance and Public Space"), law enforcement must obtain prior judicial approval to engage in electronic investigative techniques that attempt to track or de-anonymize individuals who are engaging in online or public environments.[402] Such techniques include placing GPS-tracking devices on cars or de-anonymizing an individual's online activities by obtaining the subscriber's identifying information that is linked to a particular IP address. The case for granting analogous protection in relation to facial images is similarly compelling. Using facial recognition technology, law enforcement can potentially track and de-anonymize individuals

398 See generally Clare Garvie, Alvaro Bedoya & Jonathan Frankle, "The Perpetual Line-Up: Unregulated Police Face Recognition in America" (18 October 2016) <https://www.perpetuallineup.org>.

399 Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It", *The New York Times* (18 January 2020), <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

400 The UN Human Rights Committee also recognized in its Draft General Comment No. 37 that the use of facial recognition and other technologies that can identify individual participants in public assemblies can infringe privacy rights and must be subject to independent scrutiny and oversight. UN Human Rights Committee, "Draft General Comment No. 37" (2019) <https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx>, at para 69. Office of the Privacy Commissioner of Canada, "Metadata and Privacy: A Technical and Legal Overview" (October 2014) <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/>; *R v Spencer*, [2014] 2 SCR 212; *R v Rogers Communications*, 2016 ONSC 70; *R v Wise*, [1992] 1 SCR 527. See also: *R v Vu*, [2013] 3 SCR 657; *Riley v California*, (2014) 573 US 373 (Supreme Court of the United States).

401 Research Group of the Office of the Privacy Commissioner of Canada, "Automated Facial Recognition in the Public and Private Sectors", *Office of the Privacy Commissioner of Canada* (March 2013), <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/fr_201303/#heading-005>; Office of the Information & Privacy Commissioner, "Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia" (16 February 2012) <https://www.oipc.bc.ca/investigation-reports/1245>.

402 *R v Spencer*, [2014] 2 SCR 212; *R v Wise*, [1992] 1 SCR 527.

who are moving freely in public and online spaces without the affected individuals being aware that their image has been collected, processed, or identified. De-anonymization, in particular, occurs by taking an image of an unknown face and then using an algorithm to cross-reference the image with other picture databases to obtain a potential match that leads to an identification.

The unregulated use of facial recognition technology presents at least three other challenges to protected privacy interests in addition to eroding anonymity in daily life.

First, the collection and retention practices of 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 emergence of new facial recognition technology, the expectation of privacy in facial images is attenuated. 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,[403] and law enforcement authorities are even authorized to use force if it is needed to obtain the photograph;[404] 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.[405] 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.[406] In particular, the unauthorized retention of images is unconstitutional.[407] 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.[408]

Second, facial recognition technology is unreliable, particularly in the case of racialized individuals and women, who are more likely to be misidentified by the technology.[409] Facial recognition algorithms

403 *Identification of Criminals Act*, RSC, 1985, c I-1.

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

405 See Section 4.3.3 ("Facial Recognition").

406 *R v Dore*, [2002] OJ No 2845 (CA).

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

408 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>.

409 Danielle Groen, "How We Made AI as Racist and Sexist as Humans", *The Walrus* (12 November 2019), <https://thewalrus.ca/how-we-made-

generate matches probabilistically. One search can generate multiple ranked hits.[410] However, researchers and governmental studies report that facial recognition systems vary in their accuracy rates. For example, researchers in the United States determined that commercial facial recognition software erred in identifying darker-skinned women more than one-third of the time, and only 0.8 percent of the time for white men.[411] Further, a 2018 report by Big Brother Watch indicated that NeoFace Watch, a facial recognition product by NEC Corporation—the company from which the CPS and the TPS procured their facial recognition technologies—was found to produce inaccurate matches 91 to 98 percent of the time, in usage by the Metropolitan Police and South Wales Police in the United Kingdom.[412] Detroit Police Chief James Craig admitted in June 2020 that the facial recognition technology used by the Detroit Police, developed by DataWorks Plus, misidentifies individuals 96% of the time.[413] Such findings raise questions about the reliability of a technique that can lead to arrests or criminal charges on the basis of misidentification.

> *Facial recognition: I can unlock my sister's phone, and we're not twins.*
>
> *- Black Legal Action Centre (BLAC)*[414]

Third, increasing levels of image collection and sharing between the private sector and law enforcement authorities calls for aggressive action to enforce transparency, oversight, and clear limits on usage. In January 2020, the *New York Times* revealed that the company Clearview AI had engaged in massive aggregation of public and semi-public images through scraping the Internet, and used these images to develop facial recognition technology that the company then made available as a product to law enforcement agencies.[415] Clearview AI later identified that it had contracts with Canadian law enforcement agencies but did not disclose which ones. It was only after a leak of Clearview AI's internal

---

ai-as-racist-and-sexist-as-humans/>; Drew Harwell, "Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use", *The Washington Post* (19 December 2019), <https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/>; and Russell Bramdon, "Amazon's facial recognition matched 28 members of Congress to criminal mugshots", *The Verge* (26 July 2018), <https://www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition>.

410 Ian Sample, "What is facial recognition – and how sinister is it?", *The Guardian* (29 July 2019), <https://www.theguardian.com/technology/2019/jul/29/what-is-facial-recognition-and-how-sinister-is-it>.

411 Steve Lohr, "Facial Recognition Is Accurate, if You're a White Guy", *New York Times* (9 February 2018) <https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html>; and Joy Buolamwini & Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification" (2018) 81 Proceedings of Machine Learning Research 1.

412 Big Brother Watch, "Face Off: The lawless growth of facial recognition in UK policing" (May 2018), at 3,4, 6, <https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf>.

413 Jason Koebler, "Detroit Police Chief: Facial Recognition Software Misidentifies 96% of the Time", *VICE Motherboard* (29 June 2020), <https://www.vice.com/en_ca/article/dyzykz/detroit-police-chief-facial-recognition-software-misidentifies-96-of-the-time>.

414 Interview of Black Legal Action Centre by Cynthia Khoo (12 July 2019).

415 Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It", *The New York Times* (18 January 2020), <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>; "Privacy watchdogs to probe Clearview AI's facial-recognition technology", *CBC News* (21 February 2020), <https://www.cbc.ca/news/canada/toronto/clearview-ai-police-use-1.5471493>.

data resulted in further news revelations that Canadian law enforcement authorities themselves provided minimal information regarding whether their respective police services had used the company's facial recognition product.

Information such as the fact that Canadian police services are testing controversial face recognition technology should not be made available to the public only following exposure by the news media, demonstrating the need for proactive transparency and oversight practices. The fact that Clearview AI later suspended its contract with the RCMP, and announced that it would cease operations in Canada, does not cure this democratic deficit.[416] Prior attempts to determine which agencies were using the Clearview AI technology were stymied: journalists received incorrect information from agencies; the company declined to explain the legality of its collection of information or provision of it to Canadian agencies; and the Canadian public and politicians were (at least temporarily) at a loss to assess what oversight or limits were or ought to be applied to the technology, all because of a catastrophic failure of agencies to provide transparency in their activities. Cases such as Clearview AI emphasize the critical need for governmental processes associated with algorithmic policing technologies to meaningfully guarantee sufficient transparency, oversight, and clear limits on the adoption and use of these technologies—up to and including preemptive bans, given the demonstrable dangers of facial recognition technology in particular. Further, the litany of bans and moratoriums that municipalities and industry entities have already implemented in the United States, as described in Section 4.3.3 ("Facial Recognition") of this report, is additional indication of the fundamental threat that facial recognition technology poses to the right to privacy and other human rights and freedoms, particularly those of historically marginalized groups disproportionately impacted by police surveillance.

416 Thomas Daigle, "Clearview AI stops offering facial recognition software in Canada amid privacy probe," *CBC* (6 July 2020) <https://www.cbc.ca/news/technology/clearview-ai-stops-facial-recognition-in-canada-1.5639380>.

### 5.2.5. Concluding Comments: Algorithmic Policing and the Right to Privacy

Algorithmic policing tools, such as algorithmic surveillance and person-focused 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. Human rights and constitutional jurisprudence that relate to the protection of privacy provide guidance on how privacy interests are likely to be engaged by the use of such novel technology. The jurisprudence recognizes the need for privacy protection with respect to personal information that is available in public locations. While section 8 jurisprudence in Canada has tended to relate to data collection methods by law enforcement, section 8 and privacy legislation also apply to data processing and sharing methods that distinctly engage privacy interests.

As law enforcement agencies seek access to new classes or unprecedented volumes of data about individuals and communities, often while using products provided by private companies, legal safeguards and constitutional protections must keep pace to uphold the rights of all individuals. In particular, these safeguards must ensure that individuals remain free from being subjected to unreasonable interference with protected privacy interests by law enforcement agencies, and ensure that protected zones of privacy are not eroded by expanding police data collection practices and surveillance capabilities.[417] The use of algorithmic policing technologies, which may infringe upon privacy, must be restricted to necessary and proportionate uses in order to protect a zone of privacy in public life that individuals are entitled to expect so that they can exercise fundamental liberties such as the freedom of expression. Securing such a zone should include judicial oversight mechanisms for forms of data processing and data sharing that create new privacy concerns that are not adequately addressed under Canada's existing search warrant and production order regime.

## 5.3. Rights to Freedom of Expression, Peaceful Assembly, and Association

The rights to freedom of expression, peaceful assembly, and association are protected under articles 19, 21, and 22 of the ICCPR[418] and section 2 of the *Charter*.[419] These freedoms are fundamental to a

417 The UN General Assembly, UN Human Rights Council, and UN High Commissioner for Human Rights have all recognized the dangers of mass surveillance and the need to re-examine the right to privacy in light of contemporary challenges arising from technological advances. See UN General Assembly, "Resolution adopted by the General Assembly on 18 December 2013: 68/167, The right to privacy in the digital age", (21 January 2014) <https://undocs.org/A/RES/68/167>; UN Human Rights Committee, "Resolution adopted by the Human Rights Council on 23 March 2017: 34/7, The right to privacy in the digital age", (7 April 2017) <https://undocs.org/A/HRC/RES/34/7>; 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>, and UN Human Rights Council, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29> at para 17.

418 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966 <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>, arts 19, 21, 22.

419 *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11, s 2.

democratic society and for the promotion and protection of a broad range of other human rights.[420] The rights to peaceful assembly and freedom of association are particularly valuable insofar as they enable marginalized individuals to come together to correct power imbalances and protect themselves against more powerful entities.[421]

Algorithmic policing technology 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.[422] 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.[423] This section of the report discusses, in particular, two issues associated with the negative impact of algorithmic policing technologies on the rights to freedom of expression, peaceful assembly, and association.

Section 5.3.1 analyzes how algorithmic policing technologies may undermine the anonymity of the crowd at public assemblies, representing an unprecedented level of technological incursion on the fundamental freedoms such anonymity protects. Section 5.3.2 examines how algorithmic policing technologies specifically impact marginalized communities through enabling algorithmic surveillance of protest activity and social movements. This kind of targeted monitoring raises particular human rights and *Charter* concerns given the historical context of disproportionate law enforcement surveillance against marginalized communities and human rights advocates. The importance of protecting these fundamental freedoms is underscored given their interconnected relationship with other *Charter* and human rights, such as the rights to equality and privacy.

## 5.3.1. Undermining the Anonymity of the Crowd at Public Assemblies

The deployment of new and rapidly developing surveillance technologies, such as facial recognition and automated licence plate readers, by law enforcement agencies threatens the anonymity that has served as a condition for the exercise of the fundamental freedoms of expression, peaceful assembly,

420 UNHRC, *General Comment No 34 on Article 19 (Freedoms of opinion and expression)*, 102nd Sess, adopted 12 September 2011, UN Doc CCPR/C/GC/34, at paras 2-3 <https://www2.ohchr.org/english/bodies/hrc/docs/GC34.pdf>; UNHRC, *General Comment No 37 on Article 21 (Right of peaceful assembly)*, 129th Sess, adopted 27 July 2020, UN Doc CCPR/C/GC/37, at paras 1-2 <https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx>; *Mounted Police Association of Ontario v. Canada (Attorney General)*, 2015 SCC 1 at para 48.

421 UNHRC, *General Comment No 37 on Article 21 (Right of peaceful assembly)*, 129th Sess, adopted 27 July 2020, UN Doc CCPR/C/GC/37, at para 2 <https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx>; *Mounted Police Association of Ontario v. Canada (Attorney General)*, 2015 SCC 1 at para 58.

422 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*.

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

and association. Historically, participants in mass demonstrations have been able to rely on the relative anonymity of the crowd to protect their identities from employers, law enforcement, or other authorities; anonymity enables the more fulsome exercise of fundamental freedoms with a reduced risk of reprisals.[424] Facial recognition technology, however, can potentially identify those individuals from images or videos captured at a public gathering with significantly greater ease compared to law enforcement attempts to identify individuals without such technology. Thus, facial recognition and similar capabilities can undermine the anonymity that has facilitated participants' exercise of their fundamental freedoms. Law enforcement agencies have begun to use this technology on protesters. In the United Kingdom, the South Wales Police has been accused of using its facial recognition system at a peaceful anti-arms protest.[425] In Canada, police officers in Toronto and Calgary can submit images of individuals taken at public gatherings to their own facial recognition programs to search for matches against their respective mug-shot databases.[426] These forms of algorithmic surveillance highlight the relationship between the protection of privacy as anonymity and other fundamental freedoms such as free expression and free association.[427]

Further, individuals who take measures to avoid being identified by facial recognition systems may be viewed as suspicious and potentially fined for their attempts to preserve their anonymity. Such fines have been assigned in the United Kingdom.[428] In Canada, a criminal offence was enacted in 2012 to criminalize wearing masks during riots and unlawful assemblies (now sections 65 and 66 of the *Criminal Code*).[429] Critics fear this prohibition could chill or prevent peaceful protest activity.[430] The UN Human Rights Committee's General Comment on the right of peaceful assembly states that participant's measures to protect their anonymity should not be the subject of a general ban.[431] Thus, algorithmic policing technologies—especially when combined with laws that preclude lawful efforts to inhibit such

424 Privacy International, "Privacy International's contribution to the half-day general discussion on Article 21 of ICCPR", <https://www.ohchr.org/Documents/HRBodies/CCPR/GCArticle21/PrivacyInternational.pdf>; UNHRC, *General Comment No 37 on Article 21 (Right of peaceful assembly)*, 129th Sess, adopted 27 July 2020, UN Doc CCPR/C/GC/37, at para 2 <https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx>.

425 Ed Bridges, "Why I'm Challenging Cardiff Police On Their Invasive Facial Recognition Technology", *Huff Post Blog* (14 June 2018) <https://www.huffingtonpost.co.uk/entry/facial-recognition_uk_5b227088e4b0bbb7a0e53760?guccounter=1>.

426 For further details about the use of facial recognition technology by Canadian police services, see Section 4.3.3 ("Facial Recognition") and IN FOCUS #5: Facial Recognition Technology and the Erosion of Privacy Rights, in Section 5.2.4 ("Data Accuracy: Inaccurate Data and Inaccurate Algorithms").

427 *R v Wise*, [1992] 1 SCR 527 at 558; *R v Spencer*, [2014] 2 SCR 212 at para 44.

428 Lizzie Dearden, "Police stop people for covering their faces from facial recognition camera then fine man £90 after he protested", *Independent* (31 January 2009) <https://www.independent.co.uk/news/uk/crime/facial-recognition-cameras-technology-london-trial-met-police-face-cover-man-fined-a8756936.html>.

429 Office of the Privacy Commissioner of Canada, "Automated Facial Recognition in the Public and Private Sectors" (March 2013) <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/fr_201303/#fn8-rf>; *Criminal Code*, RSC, 1985, c C-46, ss 65(1) and 66(1).

430 Office of the Privacy Commissioner of Canada, "Automated Facial Recognition in the Public and Private Sectors" (March 2013) <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/fr_201303/#fn8-rf>; "New Bill Refines Rules on Masks in Unlawful Protests", *The Globe and Mail* (1 November 2012) <https://www.theglobeandmail.com/news/politics/new-bill-refines-rules-on-masks-in-unlawful-protests/article4845550>.

431 UNHRC, *General Comment No 37 on Article 21 (Right of peaceful assembly)*, 129th Sess, adopted 27 July 2020, UN Doc CCPR/C/GC/37, at para 60 <https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx>.

government surveillance—may have the effect of significantly eroding privacy as anonymity, with the result of infringing upon the rights of freedom of expression, peaceful assembly, and association.

### 5.3.2. Surveillance of Social Movements and Marginalized Communities

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.[432] Similarly, individuals may avoid freely exercising their freedom of association if police algorithms are used to track social networks and group affiliations, such as through the CPS's algorithmic social network analysis system, or even if individuals only suspect that the police may be tracking such information.[433] Such chilling effects may impact marginalized communities particularly 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.

> *The technology gets used against us [Black people] when we're trying to advocate for our rights. Activist monitoring is really scary. It's silencing because you're so scared.*
>
> *- Black Legal Action Centre (BLAC)*[434]

Canadian law enforcement agencies' attention to protests and demonstrations gives rise to particularly significant chilling effects in marginalized communities, implicating their right to peaceful assembly,[435] in addition to their right to freedom of expression. In discussing "Project Wide Awake,"[436] the RCMP specifically referred to their "proactive" analysis of social media communications to predict whether a crime might occur at a demonstration and to assess if there was any need for increased police presence at peaceful protests on that basis.[437] This practice casts significant doubt on whether such surveillance is necessary or proportionate, given the surveillance is deployed preemptively and

432 Glenn Greenwald, "New Study Shows Mass Surveillance Breeds Meekness, Fear and Self-Censorship", *The Intercept* (28 April 2016) <https://theintercept.com/2016/04/28/new-study-shows-mass-surveillance-breeds-meekness-fear-and-self-censorship/>.

433 See J. W. Penney, "Internet surveillance, regulation, and chilling effects online: a comparative case study" (2017), 6:2 Internet Policy Review 22; A. Marthews and C. Tucker, "The Impact of Online Surveillance on Behavior" in D. Gray and S. E. Henderson, eds., *The Cambridge Handbook of Surveillance Law* (2017) 437; and Kaminski, Margot E. and Witnov, Shane, "The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech" (January 1, 2015). University of Richmond Law Review, Vol. 49, 2015.

434 Interview of Black Legal Action Centre by Cynthia Khoo (12 July 2019).

435 UNHRC, *General Comment No 37 on Article 21 (Right of peaceful assembly)*, 129th Sess, adopted 27 July 2020, UN Doc CCPR/C/GC/37, at paras 2 and 36 <https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx>.

436 Project Wide Awake was introduced in more detail under "Social Media Surveillance" in Section 4.3 ("Algorithmic Surveillance Tools").

437 Bryan Carney, "'Project Wide Awake': How the RCMP Watches You on Social Media", *The Tyee* (25 March 2019) <https://thetyee.ca/News/2019/03/25/Project-Wide-Awake/>.

the non-violent nature of the scrutinized events. The Ottawa Police Service has also monitored the social media activity of protesters during demonstrations.[438]

Monitoring equality-seeking social movements presents particular threats to groups that advocate for democratic rights and freedoms for historically disadvantaged or marginalized communities. For example, an Ontario-based company called Media Sonar came under fire in 2016 for marketing itself to law enforcement agencies in the United States as a way to monitor hashtags related to social movements protesting police brutality, including #BlackLivesMatter.[439] Police in Calgary and Toronto have both contracted with Media Sonar in the past; however, they appear to have discontinued their use of the software.[440] A member of law enforcement from Calgary suggested that the agency's decision to discontinue its use was due to the software's reduced utility after the software lost its ability to access major social media platforms,[441] which implies that the decision did not represent opposition in principle to targeted surveillance of particular social movements. The software had lost its access as a result of social media platforms such as Twitter and Instagram (a subsidiary of Facebook) banning Media Sonar for violating their privacy policy and platform use policy, respectively.[442] The Toronto Police Service has also reportedly monitored social media activity related to the Black Lives Matter movement, using methods which have not, as of writing, been publicly disclosed.[443]

Criminal justice laws, police practices, and surveillance activities must be examined in the context of the continuing legacy of discriminatory surveillance by Canadian law enforcement of individuals and social movements related to Indigenous rights, racial justice, and other human rights advocacy.[444]

438 Nathan Munn, "'Predictive Policing' Is Coming to Canada's Capital, and Privacy Advocates Are Worried", *VICE Motherboard* (13 February 2017) <https://www.vice.com/en_us/article/jpaew3/ottawa-police-strategic-operations-centre-canada-surveillance>.

439 ACLU Northern California, "This Surveillance Software is Probably Spying on #BlackLivesMatter" (15 December 2015) <https://www.aclunc.org/blog/surveillance-software-probably-spying-blacklivesmatter>. Both police services appear to have discontinued their use of the software, with a member of law enforcement in Calgary suggesting that the decision to discontinue its use was due to the software's reduced usefulness after it was banned from accessing major social media platforms.

440 See Toronto Police Services Board, "Public Meeting - Agenda, April 20 2017", <http://www.tpsb.ca/images/agenda_apr20_public_main.pdf>, at p 5; Email from CPS FOI office to YS, 19 December 2018.

441 Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).

442 Andrew Margison, "Twitter and Instagram ban London, Ont., company for helping police track protesters", *CBC News* (19 January 2017) <https://www.cbc.ca/news/canada/toronto/twitter-bans-firm-police-protesters-1.3942093>.

443 Stephen Davis, "Police monitored Black Lives Matter Toronto protesters in 2016, documents show", *CBC News* (3 May 2018) <https://www.cbc.ca/news/canada/toronto/police-monitored-black-lives-matter-toronto-protesters-in-2016-documents-show-1.4645628>.

444 See e.g., comments of Jonathan Rudin featured within "IN FOCUS #1: Community Perspectives on Algorithmic Policing", in Part 2 ("Social and Historical Context"). Interview of Jonathan Rudin by Cynthia Khoo & Yolanda Song (8 May 2019). Recent history has reflected these patterns in police monitoring of the Idle No More movement and other Indigenous demonstrations: Jorge Barrera, "Aboriginal Affairs shared wide range of information with spy agency to bolster Idle No More surveillance: documents", *National News* (18 March 2015). <https://aptnnews.ca/2015/03/18/aboriginal-affairs-shared-wide-range-information-spy-agency-bolster-idle-surveillance-documents/>; Hillary Beaumont, "Canadian police spied on Indigenous protesters on Parliament Hill", *VICE* (10 November 2017) <https://news.vice.com/en_ca/article/a3jjxa/canadian-police-spied-on-indigenous-protesters-on-parliament-hill>; Hillary Beaumont, "Canada's spy agency has been watching Standing Rock and thinks it has Canadian implications", *VICE* (15 March 2017) <https://news.vice.com/en_ca/article/evaw3w/canadas-spy-agency-has-been-watching-standing-rock-and-thinks-it-has-canadian-implications>. In 2014, the RCMP established Project SITKA to collect information about prominent Indigenous activists and assess their levels of "threat" (assessed as a likelihood that the individual has committed or will likely commit criminal activity): Sean Craig, "RCMP tracked 89 indigenous activists considered 'threats' for participating in protests", *The National Post* (13 November 2016) <https://nationalpost.com/news/canada/rcmp-tracked-89-indigenous-activists-considered-threats-for-participating-in-protests>. Researchers Miles

Given the importance of protest and democratic dissent to the exercise of fundamental freedoms, law enforcement surveillance should be subject to rigorous scrutiny, especially in cases where those monitored are speaking from a position of historical disenfranchisement or oppression. Journalist, author, and activist Desmond Cole stated:

> One of the most important features of surveillance is the way in which it alters our behaviour as the targets. It alters our mind, literally. It forces us to consider that we are being watched. Even if we aren't. It pushes us to self-regulate, and we have to resist that. For myself, I've become much more aware of the notion that I am being watched; I think it would be impossible not to allow that to impact me in any way and how I work but I try to be aware of it. I try actively to not be afraid and not silence myself.[445]

Disproportionate targeting in surveillance practices by law enforcement raises fundamental questions about discrimination. Restrictions on the right of peaceful assembly must be "content neutral" and not based on race, ethnicity, political opinion, sexual orientation, or other protected or adjacent factors; any restrictions must also be necessary and proportionate in the context of upholding democracy and human rights.[446] Individuals who engage in social movements that are more likely to be monitored by law enforcement, such as Indigenous rights or racial justice movements, are arguably being denied equal protection of the law under the *Charter* or the ICCPR. These same groups may also be unfairly over-represented in police data sets, which might eventually be used to train policing algorithms, thereby causing law enforcement to direct further disproportionate police attention and resources towards those particular groups and communities.

In interpreting the *Charter*, the Supreme Court of Canada has made clear that the human rights and fundamental freedoms enshrined in the *Charter* should be interpreted as a unified system that maintains its underlying values and is internally coherent throughout.[447] As such, any examination of the impacts of police practices that systematically surveil online activities, protests, and forms of activism through algorithmic data aggregation and analysis requires a consideration of the global effects of those practices upon human rights and freedoms that relate to privacy, expression, association, and equality together. The protection of privacy under section 8 of the *Charter* has, for example, been described as a "precursor" to the exercising of other rights and fundamental freedoms protected by the *Charter*,

---

Howe and Jeffrey Monaghan found that the RCMP investigation extended far beyond criminal activities and encompassed not only protests but also speaking tours and other events where "Aboriginal grievances may be part of the topic": Miles Howe & Jeffrey Monaghan, "Strategic Incapacitation of Indigenous Dissent: Crowd Theories, Risk Management, and Settler Colonial Policing" (2018) 40:4 *Canadian Journal of Sociology* at 334. The researchers found "the RCMP's understanding of risk [or threat] to be synonymous with the potential of a protest movement's success … suggest[ing] that the RCMP's mandate has warped toward working to undermine protest movements, regardless of their legality": Miles Howe & Jeffrey Monaghan, "Policing Indigenous Dissent: Trends Behind Wet'suwet'en Raid" (28 January 2015) 5 *Culturally Modified* <https://culturallymodified.org/policing-indigenous-dissent-trends-behind-the-wetsuweten-raid/>.

445 Interview of Desmond Cole by Cynthia Khoo & Yolanda Song (31 May 2019).

446 UNHRC, *General Comment No 37 on Article 21 (Right of peaceful assembly)*, 129th Sess, adopted 27 July 2020, UN Doc CCPR/C/GC/37, at paras 22 and 40 <https://www.ohchr.org/EN/HRBodies/CCPR/Pages/GCArticle21.aspx>.

447 *R v S* (RJ), [1995] 1 SCR 451 at 561; *Health Services and Support – Facilities Subsector Bargaining Assn v British Columbia*, [2007] 2 SCR 391 at paras 80-86.

such as the freedom of expression.[448] The Supreme Court of Canada has recognized this inherent connection between privacy (such as anonymity in public space) and the freedom of expression:

> The ability to move about freely without constant supervision by the government is an important source of individual liberty that must be addressed. A fear of systematic observation, even in public places, destroys this sense of freedom. Justice Douglas recognized the importance of this privacy value in a democratic society, commenting that free movement is as dangerous to a tyrant as free expression of ideas or the right of assembly and is, therefore, controlled in most countries.[449]

Given the importance of the rights at stake, the impact of algorithmic policing technologies on fundamental freedoms must be given appropriate weight even where there are legitimate law enforcement objectives. This weighing should include recognition that individuals do not ordinarily expect their online activities to be systematically and intensively monitored and analyzed by law enforcement, nor should individuals be expected to conduct their lives under the burden of such an assumption. As a result, where such rights are engaged, rigorous scrutiny of algorithmic policing methods is important to examine their proportionality, legality, and necessity relative to public interest goals.[450]

### 5.3.3. Concluding Comments: Algorithmic Policing and the Rights to Freedom of Expression, Peaceful Assembly, and Association

Having surveyed the issues that algorithmic policing raises in the context of the rights to freedom of expression, peaceful assembly, and association, it is apparent that the use of algorithmic policing technologies risks chilling the exercise of these fundamental freedoms.[451] Surveillance tools such as facial recognition technology threaten the anonymity of the crowd that has traditionally protected the identities of protesters. A growing body of empirical evidence shows that the use of social media surveillance software to monitor the communications and activities of protesters may also pose a chilling effect on protected freedoms. The monitoring of protest activity and social movements is concerning in the historical context of the disproportionate law enforcement surveillance against racial justice and Indigenous rights advocates. Racialized and marginalized communities may be impacted by chilling effects particularly acutely. Protection of fundamental freedoms is important in that context to ensure that historically disadvantaged or marginalized communities have equally meaningful access to the freedom to organize and participate in democratic debate and dissent.

448 Renee Pomerance, "Informational Privacy in the Digital Age," in Benjamin Berger, Emma Cunliffe, and James Stribopoulos, eds, *To Ensure that Justice is Done: Essays in Memory of Marc Rosenberg* (Toronto: Thomson Reuters, 2017), at p 183.

449 *R v Wise*, [1992] 1 SCR 527 at 558 per La Forest J., which was endorsed by the unanimous court in *R v Spencer*, [2014] 2 SCR 212 at para 44.

450 UN General Assembly, *Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association*, A/74/349 (11 September 2019) <https://undocs.org/A/74/349> at para 61.

451 *R v Khawaja*, 2012 SCC 69 at paras 79-80; *Canadian Broadcasting Corporation v Attorney General of Ontario*, 2015 ONSC 3131 at para 168.

## 5.4. Right to Equality and Freedom from Discrimination

The Canadian criminal justice system and law enforcement practices have been repeatedly criticized by various United Nations bodies and experts for their discriminatory impact on marginalized groups such as Indigenous and racialized persons.[452] This negative and disproportionate impact also extends to individuals who are homeless, who live with mental illness, or who belong to the LGBTQ community, including those who exist at the intersection of multiple grounds of vulnerability or oppression.[453] Although the Canadian government has engaged in some efforts to prevent discrimination in criminal justice,[454] members of historically marginalized communities have overwhelmingly borne the brunt of human rights violations and disproportionate targeting by law enforcement authorities.[455] Such discrimination is made worse given that algorithmic policing technologies may draw on the biased and inaccurate data currently held or relied on by law enforcement agencies—such as data from police stops, gang databases, public reports, arrests, guilty pleas, and wrongful convictions.[456] These technologies risk perpetuating or amplifying existing inequalities in ways that amount to violating the right to equality and the right to freedom from discrimination of marginalized groups who are protected under section 15 of the *Canadian Charter of Rights and Freedoms* ("the *Charter*").[457]

Section 5.4 broadly analyzes how algorithmic policing techniques raise issues that engage the right to equality and the right to freedom from discrimination. Section 5.4.1 outlines the scope of the right to equality and freedom from discrimination in Canadian and international human rights law. Section 5.4.2 examines algorithmic bias and how algorithmic policing technology can lead to "feedback loops of injustice"[458] that can subject marginalized communities to increased suspicion and to a higher risk that law enforcement will use force or excessive force. Such feedback loops may also impair

452 In 2004, the UN Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia, and related intolerance expressed extreme concern about the high rate of incarceration of Indigenous, Black, and Asian persons in Canada: *Report by Mr. Doudou Diène, Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance*; the Committee on the Elimination of Racial Discrimination also noted the overrepresentation of African Canadians in the criminal justice system and the disproportionate rate at which police questioning and data collection affects people of African descent: United Nations Committee on the Elimination of Racial Discrimination, Summary Record of the 2600th Meeting, CERD/C/SR.2600 at para 34; and the UN OHRC Independent Expert on Minority Issues has likewise written, "Persons belonging to African Canadian, Muslim, Arab and Latino communities reported feeling subject to unjustified police surveillance and experiencing negative interactions with the police, which they consider to be consistent with a practice of racial profiling": *Report of the independent expert on minority issues: Addendum: Mission to Canada* (8 March 2010), A/HRC/13/23/Add.2, at para 53 <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/118/60/PDF/G1011860.pdf?OpenElement>.

453 See discussion in Section 5.4.2. ("Algorithmic Bias and "Feedback Loops of Injustice").

454 See e.g., United Nations, Committee on the Elimination of Racial Discrimination, "Consideration of reports submitted by States parties under article 9 of the Convention" CERD/C/CAN/21-23 (8 June 2016) <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G16/114/64/PDF/G1611464.pdf?OpenElement>.

455 See Section 2.1 ("Criminal Justice and Systemic Discrimination in Canada").

456 See Section 2.2 ("Bias and Inaccuracies in Police Data").

457 *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11, s 15.

458 This term is taken from Virginia Eubanks, *Automating Inequality*: *How High-Tech Tools Profile, Police, and Punish the Poor* (New York: St. Martin's Press, 2018) at 7.

community autonomy, well-being, and dignity. Section 5.4.3 analyzes how the data-driven nature of algorithmic policing makes those with socio-economic disadvantage particularly vulnerable to being wrongly and disproportionately captured by the criminal justice system. Such capture arises due to data 'hypervisibility' that, itself, results from more frequent engagement with government systems; this hypervisibility is also a consequence of the criminalization of poverty and homelessness. Section 5.4.4 discusses how algorithmic policing technologies may involve "inequality by design" while they simultaneously obscure systemic injustices with a veneer of scientific and mathematical legitimacy. Section 5.4.5 concludes with a brief discussion and recommendations drawn from the findings and analysis in Sections 5.4.1 through 5.4.4.

## 5.4.1. An Intersectional Approach to Equality and Freedom from Discrimination

The right to equality and freedom from discrimination is a cornerstone of international human rights law. The ICCPR provides that "all persons are equal before the law and are entitled without any discrimination to the equal protection of the law."[459] States also must respect and ensure that the rights enshrined in the Convention are guaranteed to all individuals "without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status."[460] Canada has ratified a number of additional international human rights instruments that provide similar protections for equality and freedom from discrimination.[461]

The right to equality and right to freedom from discrimination is also guaranteed by the *Charter* and by quasi-constitutional federal and provincial human rights codes, as well as by the provincial *Charte des droits et libertés de la personne* (*Charter of Human Rights and Freedoms*) in Quebec.[462] Section 15 of the *Charter* states, "Every individual is equal before and under the law and has the right to the equal protection and equal benefit of the law without discrimination and, in particular, without discrimination based on race, national or ethnic origin, colour, religion, sex, age or mental or physical disability."[463] The *Charter* protects individuals on the basis of the characteristics set out in the provision above, known

459 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966 <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>, art 26.

460 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966 <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>, art 2.1.

461 See the *International Covenant on Economic, Social and Cultural Rights* (ICESCR), 19 December 1966, ratified by Canada 1976, 993 UNTS 3, Can TS 1976 No 46, 6 ILM 360, entered into force 3 January 1976, ratified by Canada 1976, <https://www.ohchr.org/en/professionalinterest/pages/cescr.aspx>; *International Convention on the Elimination of All Forms of Racial Discrimination*, December 21, 1965, 660 UNTS 195 ratified by Canada in 1970, <https://www.ohchr.org/en/professionalinterest/pages/cerd.asx>; *Convention on the Elimination of All Forms of Discrimination against Women* (CEDAW), adopted December 18, 1979, GA res 34/180, 34 UN GAOR Supp (No 46) at 193, UN Doc A/34/46, entered into force September 3, 1981, ratified by Canada 1981, <https://www.ohchr.org/en/professionalinterest/pages/cedaw.aspx>; *Convention on the Rights of Persons with Disabilities* (CRPD), adopted December 13, 2006, GA Res 61/106, Annex I, UN GAOR, 61st Sess, Supp (No 49) at 65, UN Doc A/61/49 (2006), entered into force May 3, 2008, <https://www.ohchr.org/en/hrbodies/crpd/pages/crpdindex.aspx>; *Convention relating to the Status of Refugees*, 189 UNTS 150, entered into force April 22, 1954, ratified by Canada on 4 June 1969.

462 See e.g., *Canadian Human Rights Act*, RSC 1985, c H-6; *Human Rights Code*, RSBC 1996, c 210; *Human Rights Code*, RSO 1990, c H.19; *Alberta Human Rights Act*, RSA 2000, c A-25.5; *Charte des droits et libertés de la personne*, RLRQ c C-12.

463 *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11, s 15(1).

as enumerated grounds, and on the basis of analogous grounds.[464] The Supreme Court of Canada has recognized the following characteristics as analogous grounds for constitutional protection under section 15: citizenship status, marital status, sexual orientation, and Aboriginality-residence.[465] This list is not necessarily exhaustive, and new analogous grounds may be added in future cases.

Government activity violates section 15 of the *Charter* if it has the purpose or effect of creating a distinction based on an enumerated or analogous ground and the distinction perpetuates disadvantage.[466] Proof of intent to discriminate is not necessary; section 15 protection is engaged as long as a law or government activity has a discriminatory impact, regardless of intent.[467] Unlawful discrimination can occur indirectly through a process known as "adverse effects discrimination" or "adverse impacts discrimination." Adverse impacts discrimination is defined as "neutral rules with adverse consequences for certain groups."[468] Such rules are neutral in theory, but not in their application or outcomes.

The core animating principle of section 15 is substantive equality. Substantive equality recognizes that "every difference in treatment between individuals under the law will not necessarily result in inequality and, as well, that identical treatment may frequently produce serious inequality."[469] Substantive equality considerations are especially pertinent when it comes to the misleading notion that algorithms are "neutral" when, in fact, algorithms have provided prominent examples of adverse effects discrimination.[470] The rigid, formal equality of mathematical formulas is unlikely to operate justly

464 Analogous grounds are those that are not explicitly listed in the *Charter*, but which similarly "serve as the basis for stereotypical decisions made not on the basis of merit but on the basis of a personal characteristic that is immutable or changeable only at unacceptable cost to personal identity": *Corbiere v Canada (Minister of Indian and Northern Affairs)*, [1999] 2 SCR 203 at para 13.

465 Government of Canada, Department of Justice, "Section 15 - Equality Rights" <https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art15.html>.

466 *Kahkewistahaw First Nation v Taypotat*, 2015 SCC 30 at para 16; *R v Kapp*, [2008] 2 SCR 483; *Andrews v Law Society of British Columbia*, [1989] 1 SCR 143; *Law v Canada (Minister of Employment and Immigration)*, [1999] 1 SCR 497.

467 *R v Kapp*, [2008] 2 SCR 483; *Andrews v Law Society of British Columbia*, [1989] 1 SCR 143; *Law v Canada (Minister of Employment and Immigration)*, [1999] 1 SCR 497.

468 *Stewart v Elk Valley Coal Corp*, 2017 SCC 30, at paras 80-81. For example, a law that (hypothetically) mandated submission to facial recognition to access government services—"neutrally", because it applies to all individuals—would, in reality, perpetuate harmful disadvantage for racialized individuals with darker skin, whose faces research has shown may not be detected accurately or at all depending on how the facial recognition technology was developed: Joy Buolamwini, "When the Robot Doesn't See Dark Skin", *New York Times* (21 June 2018) <https://www.nytimes.com/2018/06/21/opinion/facial-analysis-technology-bias.html>. For examples of adverse discrimination cases, see e.g., *Symes v Canada*, [1993] 4 SCR 695 (child care expenses); *Bliss v Attorney General of Canada*, [1979] 1 SCR 183 (pregnancy); *Brooks v Canada Safeway Ltd*, [1989] 1 SCR 1219 (pregnancy); *Kahkewistahaw First Nation v Taypotat*, 2015 SCC 30 (education level); and *Eldridge v British Columbia* (Attorney General), [1997] 3 SCR 624 (hearing disability).

469 *Andrews v Law Society of British Columbia*, [1989] 1 SCR 143 at 164; *Law v Canada (Minister of Employment and Immigration)*, [1999] 1 SCR 497; *Kahkewistahaw First Nation v Taypotat*, 2015 SCC 30, at para 17.

470 See e.g., Jeffrey Dastin, "Amazon scraps secret AI recruiting tool that showed bias against women", *Reuters* (9 October 2018) <https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G>; Adi Robertson, "Facebook's ad delivery could be inherently discriminatory, researchers say", *Verge* (4 April 2019), <https://www.theverge.com/2019/4/4/18295190/facebook-ad-delivery-housing-job-race-gender-bias-study-northeastern-upturn> ("A new study says that Facebook's ad delivery algorithm discriminates based on race and gender, even when advertisers are trying to reach a broad audience. The research backs up a similar claim that the US Department of Housing and Urban Development made last week when it sued Facebook for breaking housing discrimination laws."); and Claire Cain Miller, "When Algorithms Discriminate", *New York Times* (9 July 2015) <https://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html>.

in contexts of substantive inequality, such as within a criminal justice system that is already scarred by historic and systemic discrimination. Thus, in assessing algorithmic policing tools, "[t]o approach the ideal of full equality before and under the law … the main consideration must be the impact of the law on the individual or the group concerned."[471]

Evaluating this impact in the context of algorithmic policing technology requires an intersectional approach.[472] Such an approach recognizes that "categories of discrimination may overlap… [and] individuals may suffer historical exclusion [based on and] confront multiple grounds of disadvantage." Intersecting grounds of discrimination may result in "particularly complex" life situations.[473] "Categorizing such discrimination as [for example] primarily racially oriented, or primarily gender-oriented, misconceives the reality of discrimination as it is experienced by individuals."[474] Intersectional analysis "places the focus on society's response to the individual as a result of the confluence of grounds, and it does not require the person to slot themselves into rigid compartments or categories."[475] Addressing technology-facilitated violations of equality rights and ensuring freedom from discrimination, with a nuanced intersectional perspective, is necessary to establish effective responses—legal, regulatory, or otherwise—that account for the root causes of discrimination and systemic oppression in Canada's criminal justice system. Such a perspective includes recognizing that "discrimination has evolved and tends to no longer be overt, but rather more subtle, multi-layered, systemic, environmental and institutional."[476] Intersectionality is thus particularly necessary when analyzing the individualized and systemic impacts of institutional adoption of algorithmic policing technology.

Section 15 of the *Charter* applies to algorithmic policing because police are government actors, and police activity, officers' conduct, and law enforcement policies fall under "the application or operation of law," which the *Charter* prohibits from being discriminatory.[477] The individuals and communities who have already been most negatively affected by the criminal justice system and who will presumably

471 *Andrews v Law Society of British Columbia*, [1989] 1 SCR 143 at 165; *R v Kapp*, [2008] 2 SCR 483 at para 15.

472 The Supreme Court of Canada has recognized that some grounds of discrimination are embedded in, or intersect with others: *Law v Canada*, [1999] 1 SCR 497 at para 94.

473 *Canada (Attorney General) v Mossop*, [1993] 1 SCR 554 at 645-646 (L'Heureux-Dubé J, in dissent).

474 Justice L'Heureux-Dubé writing for the minority in *Canada (AG) v Mossop*, [1993] 1 SCR 554 at 645-646 (Mossop), cited in Ontario Human Rights Commission, "An intersectional approach to discrimination: Addressing multiple grounds in human rights claims" (9 October 2001) <http://www.ohrc.on.ca/en/intersectional-approach-discrimination-addressing-multiple-grounds-human-rights-claims/move-towards-intersectional-approach>.

475 Ontario Human Rights Commission, "An intersectional approach to discrimination: Addressing multiple grounds in human rights claims" (9 October 2001) <http://www.ohrc.on.ca/en/intersectional-approach-discrimination-addressing-multiple-grounds-human-rights-claims/move-towards-intersectional-approach>.

476 Ontario Human Rights Commission, "An intersectional approach to discrimination: Addressing multiple grounds in human rights claims" (9 October 2001) <http://www.ohrc.on.ca/en/intersectional-approach-discrimination-addressing-multiple-grounds-human-rights-claims/move-towards-intersectional-approach>.

477 See e.g., *Elmardy v Toronto Police Services Board*, 2017 ONSC 2074 (finding section 15 violation based on the actions of an individual police officer, including racial profiling and physically attacking the plaintiff); and *Doe v Metropolitan Toronto (Municipality) Commissioners of Police*, 39 OR (3d) 487, 160 DLR (4th) 697, 126 CCC (3d) 12 (finding section 15 violation based on the police service's decision not to warn women who were at risk of being attacked by a serial rapist, due to belief in rape myths and sexist stereotypes about women).

continue to be most affected, including by algorithmic policing, are those from section 15 protected groups that have been historically over-policed and disproportionately criminalized, silenced, surveilled, and monitored by the state. These communities are defined by protected characteristics—based on the enumerated or analogous grounds—such as race, sexual orientation, Indigenous identity, or mental disability. Human rights legislation also captures law enforcement activities[478] and protects marginalized groups from discrimination, thus would also apply where algorithmic policing impacts the right to equality or freedom from discrimination.[479] For instance, section 15 and human rights legislation would likely apply where a policing policy relies on a biased algorithm, or where an algorithmic "prediction" contributes to an officer discriminating against a member of a marginalized community.

Ultimately, algorithmic policing technology may give rise to section 15 violations in at least three overarching ways: first, through perpetuating discriminatory feedback loops and confirmation bias, which concentrates further disproportionate police scrutiny on section 15 protected communities; second, through making section 15 protected groups particularly susceptible to law enforcement action by virtue of "data hypervisibility"; and third, through institutionalizing and obscuring underlying causes of systemic discrimination in criminal justice, while impeding the ability to directly address them. The following sections of the report (5.4.2 through 5.4.4) take up each of these issues in turn, with concluding comments in Section 5.4.5.

## 5.4.2. Algorithmic Bias and "Feedback Loops of Injustice"

Law enforcement authorities' use of algorithmic policing technology potentially violates section 15 where the technology's use results in protected groups being subjected to unequal protection of the law or losing equal benefit of the law. Just like with traditional policing methods, in the case of algorithmic policing, the "application or operation of law" occurs through police activities, policies, and conduct. Algorithmic bias in policing technologies can result in inequality and can perpetuate disadvantage against section 15 protected groups. Such perpetuation results from increased confirmation bias and discriminatory feedback loops, which occur when problematic police data is used to train policing algorithms.[480] This form of algorithmic bias can unjustly increase already heightened scrutiny, police suspicion, and aggression with respect to members of marginalized communities, exacerbating pre-existing discrimination. As a result, section 15 protected groups lose "equal benefit" and "equal protection" of the law, including other *Charter* rights, such as the presumption of innocence,[481] the right

478 "The consensus of several cases spanning over three decades of anti-discrimination law is that the law enforcement activities of municipal and regional police forces are 'public services' or 'facilities' [as defined for human rights legislation]." Justice Walter Surma Tarnopolsky, *Discrimination and the Law*, 1st ed (Toronto: Carswell, 2004) (loose-leaf updated 2020) at ch 11 at 11.6(c) ("Municipal Police").

479 For examples of police activities being found discriminatory under human rights legislation, see e.g., *Hum v Royal Canadian Mounted Police*, 8 CHRR D/3748; *Johnson v Halifax Regional Police Service*, [2003] NSHRBID No 2, 48 CHRR D/307; and *Dawson v Vancouver Police Board*, 2015 BCHRT 54.

480 See the discussion in Section 2.2 ("Bias and Inaccuracies in Police Data").

481 *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11, section 11(d).

to be free from unreasonable search and seizure,[482] and the right to be free from arbitrary detention.[483] Left unchecked, this state of affairs would impair the autonomy and dignity of those communities and the individuals within them. The remainder of this subsection will elaborate on each of the above points in turn.

Algorithmic bias and discriminatory feedback loops occur when discriminatory patterns in police data are embedded in and perpetuated by policing algorithms that were trained on such data.[484] The historical disadvantage and targeting of section 15 protected groups is embedded in the data and, consequently, embedded into the algorithms themselves. As Osoba and Welser write, "[a]pplying procedurally correct algorithms to biased data is a good way to teach artificial agents to imitate whatever bias the data contains."[485] Algorithms that are trained on police data, often composed of dirty data,[486] will thus likely identify, incorporate, and replicate historical patterns of discrimination, to the effect of violating protected groups' section 15 rights by providing them with lesser legal protections against state conduct.

For example, in a 2019 study, Rashida Richardson, Jason Schultz, and Kate Crawford demonstrated that at least nine jurisdictions across the United States likely trained predictive policing models with police data generated during times that gave rise to "government investigations, consent decrees, or other documentation of corrupt, racially biased, or otherwise illegal police practices."[487] Richardson et al. found "strong evidence" and an "extremely high likelihood" that Chicago's and New Orleans' predictive policing systems, respectively, were built atop this "dirty data."[488] The authors of the study stated that, in addition to other "research that empirically demonstrates that the mathematical models of predictive policing systems are susceptible to runaway feedback loops,"[489] their own findings suggested that "feedback loops are also a byproduct of the biased police data."[490] Both research groups found that feedback loops meant that police were "repeatedly sent back to the same neighborhoods regardless

482 See Section 5.2 ("Right to Privacy").

483 See Section 5.5 ("Right to Liberty and to Be Free from Arbitrary Detention").

484 See the discussion in Section 2.2 ("Bias and Inaccuracies in Police Data").

485 Osonde Osoba & William Welser IV, "An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence", RAND Corporation (2017) at 17 <https://pdfs.semanticscholar.org/b7be/0be36706c30a76312b34d60ff02d97698191.pdf>.

486 See Section 3.1 ("A Technical Primer"): "Where a policing algorithm has been contaminated by corrupted, distorted, incomplete, or biased data (whether inadvertently or intentionally), it has been trained on dirty data".

487 Rashida Richardson, Jason M Schultz & Kate Crawford, "Dirty Data, Bad Predictions: How civil rights violations impact police data, predictive policing systems, and justice" (May 2019) 94:192 *New York University Law Review* 192 at 197 <https://www.nyulawreview.org/wp-content/uploads/2019/04/NYULawReview-94-Richardson-Schultz-Crawford.pdf>.

488 This evidence emerged, among others, as a result of "extensive dirty policing practices and recent litigation." Neighbouring jurisdictions were also affected, in the case of Maricopa County, due to jurisdictions sharing the same police data and tools which included or were based on the dirty data. *Ibid* at 204.

489 *Ibid* at 218. Richardson, Schultz, and Crawford cite Danielle Ensign et al, "Runaway Feedback Loops in Predictive Policing" (2018) 81:1 Proceedings of Machine Learning Research <https://arxiv.org/pdf/1706.09847.pdf>; see also Kristian Lum & William Isaac, "To predict and serve?" (2016) 13:5 Significance 14.

490 *Ibid*.

of the actual crime rate."[491] In a separate study, Lum and Isaac's assessment of PredPol's algorithm, as applied to drug-related offences in Oakland, California, revealed that "[B]lack people would be targeted by predictive policing at roughly twice the rate of whites" despite "roughly equivalent" drug use.[492] The algorithm also targeted low-income households at "disproportionately high rates."[493]

Dirty data may also appear in the Canadian policing context. Such data may be generated through institutional or unconscious bias, directly or indirectly discriminatory policies and practices, or police misconduct. Multiple studies, inquiries, court decisions, and investigations have found that Black and Indigenous people, for instance, are overrepresented in Canadian carding, street check, arrest, pre-trial detention, sentencing, and incarceration data, and that this overrepresentation is a result of biased criminal justice practices or systemic discrimination.[494] Further, biased data exists about and impacts other marginalized groups such as LGBTQ individuals,[495] those with mental illnesses,[496] and low-income communities.[497]

491 *Ibid.*

492 Kristian Lum & William Isaac, "To predict and serve?" (2016) 13:5 Significance 14 at 18; for critiques and defence of this study, see William Isaac & Kristian Lum, "Setting the Record Straight on Predictive Policing and Race", *The Medium* (3 January 2018) <https://medium.com/in-justice-today/setting-the-record-straight-on-predictive-policing-and-race-fe588b457ca2>.

493 *Ibid.*

494 See e.g., Section 2.1 ("Criminal Justice and Systemic Discrimination in Canada"). See also: "Between 2008 and 2013, [Black people] were three times more likely to appear in the contact card dataset than their representation in the population.": Ontario Human Rights Commission, *Under Suspicion: Research and consultation report on racial profiling in Ontario* (April 2017) at 37 <http://www.ohrc.on.ca/en/under-suspicion-research-and-consultation-report-racial-profiling-ontario>.

495 For example, John Fisher details how certain *Criminal Code* provisions, such as indecency-related or obscenity-related offences, were frequently applied in a way that had the effect of discriminating against LGBTQ individuals and their communities, practices, and establishments. John Fisher, "Outlaws or In-laws?: Successes and Challenges in the Struggle for LGBT Equality", (2004) 49 McGill Law Journal 1183 at 1201-1202 (footnotes omitted) <https://lawjournal.mcgill.ca/wp-content/uploads/pdf/449577-4fishe.pdf> ("Much like the 'obscenity' provisions in the Customs regime, the 'indecency' test in the bawdy house provisions is neutral on its face, subjective in its application, depends on 'community standards of tolerance', and has been used to target LGBT establishments and practices. [...] There is no question that police raids on 'queerspaces' such as a gay bathhouse constitute a fundamental assault on our identity and consensual expression of our sexuality."). Police institutions have also historically played a significant role in the persecution of LGBTQ communities in Canada, such as in the 1981 Toronto bathhouse raids. See e.g., Jamie Bradburn, "Historicist: Raiding the Bathhouses", *Torontoist* (23 May 2015) <https://torontoist.com/2015/05/historicist-raiding-the-bathhouses>; and Michael Gold and Derek M Norman, "Stonewall Riot Apology: Police Actions Were 'Wrong,' Commissioner Admits", *New York Times* (6 June 2019) <https://www.nytimes.com/2019/06/06/nyregion/stonewall-riots-nypd.html>.

496 See generally Glen Luther & Mansfield Mela, "Mental Illness and Sentencing: Blaming the Mentally Ill for their Lack of Cooperation with Inadequate Treatment in *R v Maier*", *ABlawg* (30 March 2015) <https://ablawg.ca/wp-content/uploads/2015/03/Blog_GL_MM_Maier_March2015.3.pdf>; The Honourable Justice Richard D Schneider, "The Mentally Ill: How They Became Enmeshed in the Criminal Justice System and How We Might Get Them Out", *Department of Justice: Research and Statistics Division* (March 2015) <https://www.justice.gc.ca/eng/rp-pr/jr/mental/mental.pdf>; Roslyn Shields, "Mental Health and Criminal Justice Policy Framework", *Centre for Addiction and Mental Health* (October 2013) <https://www.camh.ca/-/media/files/pdfs---public-policy-submissions/mh_criminal_justice_policy_framework-pdf.pdf>; and Tanya Dupuis, Robin MacKay & Julia Nicol, "Current Issues in Mental Health in Canada: Mental Health and the Criminal Justice System", *Library of Parliament Background Paper* (16 December 2013) <https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/BackgroundPapers/PDF/2013-88-e.pdf>.

497 See Section 5.4.3 ("Socioeconomic Disadvantage and Hypervisibility to Algorithmic Policing").

Police data may also reflect that systemic discrimination results in under-policing,[498] including a lack of police presence where there is need (and noting that increased police presence is distinct from increased imposing of police stops in a community), of historically marginalized communities where they are victims of crime. For example, Jonathan Rudin wrote in a report prepared for the Ipperwash Inquiry, "Aboriginal people are not only overrepresented in the criminal justice system as accused persons, but as victims as well. [They] are often seen as less worthy victims by the police, and thus requests for assistance are often ignored or downplayed. [...] Under-policing and over-policing are really two sides of the same coin."[499] The Ontario Human Rights Commission recognizes under-policing of racialized individuals as a form of racial discrimination that occurs both individually among specific members of law enforcement and institutionally in systemic responses to crimes that affect members of Black, Indigenous, or racialized communities in particular.[500] The LGBTQ community has also historically received unequal and lesser "protection of the law", such as in 2018, when police services appeared slow to investigate a serial killer targeting Toronto's Gay Village.[501]

Algorithms trained on dirty data reflect the dynamics that underlie the data's original collection and, thus, perpetuate disadvantage against the affected individuals and groups with protected characteristics. For instance, systemic bias through under-policing may result in dirty data that is used to train policing algorithms, which perpetuate the bias by systematically and significantly underestimating the extent to which members of marginalized communities are victimized criminally. Policing algorithms that are trained on dirty data may also reflect preferential under-policing,[502] where offenders from dominant social classes are treated more leniently or favourably by law enforcement—both the COMPAS risk assessment tool and PredPol's algorithm in Lum and Isaac's study resulted in disproportionately

498 "Under-policing generally refers to inadequate law enforcement responses to the victimization or probable victimization of an individual or group of individuals. For example, there have been longstanding concerns of under-policing related to sexual assaults against women and violence against LGBTQ2+ communities." Ontario Human Rights Commission, "Policy on eliminating racial profiling in law enforcement" (20 June 2019), at 2.2 (footnotes omitted) <http://www.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement>.

499 Jonathan Rudin, *Aboriginal Peoples and the Criminal Justice System* (Toronto: Ipperwash Inquiry, 2005) at 1-2, Ipperwash Inquiry <www.attorneygeneral.jus.gov.on.ca/inquiries/ipperwash/policy_part/research/pdf/Rudin.pdf>. Additionally, the Ontario Human Rights Commission has stated, "The final report of the *National Inquiry into Missing and Murdered Indigenous Women and Girls* outlines the historical, cultural and political dimensions of under-policing. Racial dehumanization is a recurring theme, and on multiple occasions the term 'disposable' is used to convey how the dominant society often regards Indigenous women and girls." Ontario Human Rights Commission, "Policy on eliminating racial profiling in law enforcement" (20 June 2019), at 2.2.1 <http://www.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement>.

500 Ontario Human Rights Commission, "Policy on eliminating racial profiling in law enforcement" (20 June 2019), at 2.2 <http://www.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement>.

501 See e.g., "Vijayanathan, who is one of the most outspoken critics of how Toronto let its gay community down, insists that police only took the investigations seriously when Andrew Kinsman, one of two white victims, was reported missing. But he also points to racism within the gay community – comparing the massive local search mounted after the reported disappearance of the other white victim... with the slower and less cohesive response to the disappearances of the brown-skinned victims." David Graham, "How alleged Toronto serial killer Bruce McArthur went unnoticed", *Guardian* (23 June 2018) <https://www.theguardian.com/world/2018/jun/23/bruce-mcarthur-toronto-gay-serial-killer>. The article later quotes historian Tom Hooper: "'For both gay men in the 1970s and queer people of colour today, the police have been enforcers but not protectors. Isolation, combined with a fear of police, has marginalized members of our community and made them more vulnerable to violence.'"

502 "Beyond practices of neglect in relation to Indigenous and racialized crime victims, under-policing can take a very different form – 'favoritism toward an offending class.' Given limited law enforcement resources, racial profiling, as a manifestation of over-policing directed toward Indigenous and racialized populations, can entail the under-policing of [w]hite people who are engaged in criminal activity. The OHRC describes these race-specific patterns of law enforcement as preferential under-policing. This is perhaps most often illustrated in the area of drug enforcement...." Ontario Human Rights Commission, "Policy on eliminating racial profiling in law enforcement" (20 June 2019), at 2.2 (footnotes omitted) <http://www.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement>.

favourable treatment towards white offenders. Ultimately, police data that does not screen out the layers of bias against all impacted section 15 protected groups would constitute dirty data, and it should not be used to train algorithms for the purpose of policing, law enforcement, corrections, or other functions of the criminal justice system.

Canadian police services' use of facial recognition poses particular feedback loop concerns. In Calgary and Toronto, for instance, police facial recognition systems facilitate the identification of unknown individuals by searching their images against police mug-shot databases. As a result, individuals who have been previously charged but are legally innocent or those who have been convicted of a criminal offence may be more easily identified—or misidentified, given the high error rates of facial recognition technology[503]—in the future than those who have not been previously charged or convicted.[504] Facial recognition programs may expose *Charter*-protected groups to disproportionate levels of suspicion and police scrutiny compared to individuals who have not been captured in mug-shot databases, or who belong to groups who historically have not been targeted and continue to not be targeted for police scrutiny on the basis of protected characteristics.[505] This disproportionate and unjustified scrutiny would constitute perpetuation of disadvantage based on an enumerated or analogous ground, in violation of the *Charter* equality right.

Some members of Canadian law enforcement have recognized the potential for predictive policing to perpetuate discriminatory feedback loops. A member of law enforcement in Calgary stated, "We can see if we're doing proactive work in certain areas, that will skew the data. We will get more calls there, that's because we sent people there."[506] The Vancouver Police Department (VPD) has tried to mitigate potential bias by excluding incidents that are reported by police officers from its algorithmic crime forecasts, and it trains the GeoDASH algorithms exclusively on data from verified break-and-enters reported by members of the public.[507] However, some forms of bias, including the fact that

503 See Section 5.2.4 ("Data Accuracy: Inaccurate Data and Inaccurate Algorithms").

504 "Once in a database, a suspect can repeatedly be surveilled; law enforcement can retroactively search ALPR data and identify individuals, vehicles, times, and places, rather than starting to gather information on them only once they come under suspicion." Sarah Brayne, "Big Data Surveillance: The Case of Policing" (2017) 82:5 American Sociological Rev 977 at 1000. This is even before taking into account facial recognition systems such as Clearview AI, which scrapes photos from social media data across the entire web, and which has been tested by police services in Toronto, Peel, and Halton, Ontario. *Kashmir Hill*, "The Secretive Company That Might End Privacy as We Know It", *New York Times* (18 January 2020) <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>; "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>; and Wendy Gillis & Kate Allen, "Peel and Halton police reveal they too used controversial facial recognition tool", *Toronto Star* (14 February 2020) <https://www.thestar.com/news/gta/2020/02/14/peel-and-halton-police-reveal-they-too-used-controversial-facial-recognition-tool.html>.

505 See "IN FOCUS #5: Facial Recognition Technology and the Erosion of Privacy Rights", in Section 5.2.4 ("Data Accuracy: Inaccurate Data and Inaccurate Algorithms").

506 Interview of a member of law enforcement in Calgary by Yolanda Song & Cynthia Khoo (6 May 2019).

507 "I did not want to have any data that could be perceived as having police bias in terms of generating the calls. There's always perceptions that the police could predominantly deploy to areas where they have preconceived notions that there's a higher degree of criminality because of ethnic, socioeconomic status, or any of those underlying issues that could predispose police officers to go to certain areas. And then based on that, it could be a self-fulfilling prophecy. And then they detect crime because if you're focusing all your resources by pre-deploying based on your own biases you're going to find things if you're looking for it. [...] Whether I believe it's true or not that that happens at the Vancouver Police, I didn't want the spectre that that could even be entering into the data bias. Based on that, I made a decision that we would only use public-initiated reported property crime." Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019).

some communities are more likely to report crimes to the police than others or are more likely to be taken seriously by the police when reporting criminal activity, can remain despite such efforts.[508] Warning block watches that their neighbourhood has been identified by an algorithm as a potential site of criminal activity may also trigger the "out of place" effect, where residents or law enforcement authorities discriminate against racialized individuals in predominantly white or wealthier neighbourhoods.[509]

Algorithmic bias can occur even if explicit markers of protected characteristics such as race, national origin, or disability are removed from data sets.[510] Such bias can transpire because the characteristics can be encoded in proxy data, which is data that may not appear to be the type that would give rise to discrimination, but which is correlated with information that does give rise to section 15 protections. For instance, ZIP codes in the United States are often correlated with race[511] due to racially discriminatory historical practices.[512] Relying on ZIP codes can thus function as a proxy for race, which raises section 15 protections. Other examples of proxy data include using an individual's online search activity to infer race, age, and gender;[513] using "liked" brands or pages on Facebook to infer race;[514] and using

508 See Section 2.2 ("Bias and Inaccuracies in Police Data").

509 "Specific policing activities related to monitoring traffic may be seen as forms of systemic racial profiling. One is stopping and questioning people who are perceived to be "out of place" and not residents of the neighbourhood they are in. Higher income neighbourhoods tend to be populated by White residents. This, coupled with stereotypes linking racialized people with criminality, may lead to racialized people in the neighbourhood being more likely to be stopped because they are perceived to be suspicious.": Ontario Human Rights Commission, "OHRC Response to the Race Data and Traffic Stops in Ottawa Report" (28 November 2016) <http://www.ontla.on.ca/library/repository/mon/30012/337641.pdf>, at 3 (footnotes omitted); see also: "The Star analysis of the police stop data shows blacks are more likely than whites to be documented in areas where fewer black people live." Jim Rankin and Patty Winsa, "Known to police: Toronto police stop and document black and brown people far more than whites", *Toronto Star* (9 March 2012) <https://www.thestar.com/news/insight/2012/03/09/known_to_police_toronto_police_stop_and_document_black_and_brown_people_far_more_than_whites.html>.

510 See e.g., Andrew D Selbst, "Disparate Impact in Big Data Policing", (2017) 52 *Georgia Law Review* 109 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2819182>; and Solon Barocas and Andrew D Selbst, "Big Data's Disparate Impact", (2016) 104 *California Law Review* 671, <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2477899>.

511 In Canada, marketing data draws similar correlations, such as Environics Analytics's PRIZM5 tool, which sorts every Canadian postal code into one of 68 "lifestyle types", with neighbourhood profiles that sometimes indicate race and socioeconomic status. These neighbourhood profiles include names such as "Arts & Affluence", "Asian Sophisticates", "Newcomers Rising", "South Asian Society", "Nouveaux Riches", "First Nations Families", "Enclaves Multiethniques", "Low-Rise Renters", and "South Asian Achievers". As far as the authors of this report could ascertain, this kind of marketing data is not used to inform policing algorithms in Canada. "PRIZM5 Segment Snapshots 2015", <http://assets.cengage.com/training/AOD_PRIZM5_Snapshots.pdf>; see also "PRIZM5", Environics <downloads.esri.com/esri_content_doc/dbl/int/Environics-PRIZM5-Segment-Side.pdf>.

512 See e.g., Alexis Madrigal, "The Racist Housing Policy That Made Your Neighborhood", *The Atlantic* (22 May 2014) <https://www.theatlantic.com/business/archive/2014/05/the-racist-housing-policy-that-made-your-neighborhood/371439/>; Digital Chicago, "Racial Restriction and Housing Discrimination in the Chicagoland Area", <https://digitalchicagohistory.org/exhibits/show/restricted-chicago/other/redlining>; and Camila, Domonoske, "Interactive Redlining Map Zooms In On America's History Of Discrimination", *NPR* (19 October 2016) <https://www.npr.org/sections/thetwo-way/2016/10/19/498536077/interactive-redlining-map-zooms-in-on-americas-history-of-discrimination>. Moreover, some have explicitly taken advantage of such correlations, such as the SAT test preparation company The Princeton Review, which quoted a higher price for its "24-hr Online Tutoring" service for American zip codes with a disproportionately higher Asian population compared to other zip codes, which were quoted lower prices for the same service: Jeff Larson, Surya Mattu & Julia Angwin, "Unintended Consequences of Geographic Targeting", (September 2015) *Technology Science* <https://techscience.org/a/2015090103/>.

513 Sara Wachter-Boettcher, "Google Thought I Was a Man", *Nautilus* (28 September 2017) <nautil.us/issue/52/the-hive/google-thought-i-was-a-man>.

514 Julia Angwin & Terry Parris Jr, "Facebook Lets Advertisers Exclude Users by Race", *Pro Publica* (28 October 2016) <https://www.propublica.org/article/facebook-lets-advertisers-exclude-users-by-race>.

purchasing history or social media posts to infer health conditions.[515] In the Canadian policing context, data that may not have seemed problematic when it was collected is used to draw inferences that can lead policing agencies to incorrect conclusions, which may be acted upon to the detriment of affected individuals. One example of this is determining whether a student is part of a gang, based on their friends at school.[516]

Algorithmic bias and discriminatory feedback loops that can arise from algorithmic policing technology can lead to two additional consequences that further perpetuate disadvantage for marginalized groups protected under section 15 of the *Charter*.

First, the characterization of neighbourhoods as "high crime" or of individuals as "high risk" raises concerns that algorithmic policing could encourage undue suspicion and more aggressive policing towards identified individuals or individuals within identified neighbourhoods. Officers who patrol algorithmically highlighted areas or are alerted to particular individuals by an algorithm may be more likely to perform stops or to use force or excessive force, as compared to the same circumstances without an algorithmic "tip."[517] Unconstitutional detentions already occur in Canada without algorithmically encouraged suspicion, fear, or aggression among police officers.[518] Serious consequences may follow from neighbourhoods or individuals being preemptively tagged with algorithmic "red flags," particularly where pre-existing tension exists between law enforcement and the tagged parties. Excessive use of force by law enforcement already disproportionately harms section 15 protected groups, in particular, Black and Indigenous communities[519] and individuals with

515 "As Pole's computers crawled through the data, he was able to identify about 25 products that, when analyzed together, allowed him to assign each shopper a "pregnancy prediction" score. More important, he could also estimate her due date to within a small window, so Target could send coupons timed to very specific stages of her pregnancy." Charles Duhigg, "How Companies Learn Your Secrets", *New York Times Magazine* (16 February 2012) <https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>; and Olga Khazan, "What Your Facebook Posts Say About Your Mental Health", *Atlantic* (6 November 2019) <https://www.theatlantic.com/health/archive/2019/11/what-your-tweets-say-about-your-mood/601510/>.

516 See discussion regarding gang databases, under Section 2.2 ("Bias and Inaccuracies in Police Data").

517 Andrew Guthrie Ferguson, "Predictive Policing and Reasonable Suspicion" (January 2013) 62:2 Emory Law Journal 259 at 305-308.

518 See e.g., *Elmardy v Toronto Police Services Board*, 2015 ONSC 2952; *R v Ohenhen*, 2016 ONSC 5782; *R v Schuhknecht*, 2005 BCPC 161; and *R v K(A)*, 2014 ONCJ 374.

519 See e.g., Scot Worley, "Police Use of Force in Ontario: An Examination of Data from the Special Investigations Unit: Final Report" (Research Project Conducted on behalf of the African Canadian Legal Clinic for Submission to the *Ipperwash Inquiry*) <https://www.attorneygeneral.jus.gov.on.ca/inquiries/ipperwash/policy_part/projects/pdf/AfricanCanadianClinicIpperwashProject_SIUStudybyScotWortley.pdf>; Ontario Human Rights Commission, *A Collective Impact: Interim report on the inquiry into racial profiling and racial discrimination of Black persons by the Toronto Police Service* (November 2018) <ohrc.on.ca/sites/default/files/TPS%20Inquiry_Interim%20Report%20EN%20FINAL%20DESIGNED%20for%20remed_3_0.pdf#overlay-context=en/news_centre/ohrc-interim-report-toronto-police-service-inquiry-shows-disturbing-results> at 30-32; Farida Deif, "Submission to the Government of Canada on Police Abuse of Indigenous Women in Saskatchewan and Failures to Protect Indigenous Women from Violence" (June 2017) *Human Rights Watch* <https://www.hrw.org/sites/default/files/supporting_resources/canada_saskatchewan_submission_june_2017.pdf>; The Honourable Michael H. Tulloch, *Report of the Independent Police Oversight Review* (2017) at 26-27 and 223-25 <http://www.policeoversightreview.ca/ReportoftheIndependentPoliceOversightReview.pdf>; Ontario Human Rights Commission, *Under Suspicion: Research and consultation report on racial profiling in Ontario* (April 2017), at 42-43, 65, 104 <http://www.ohrc.on.ca/en/under-suspicion-research-and-consultation-report-racial-profiling-ontario>; Anastassia Bystrova, "Does Suspect Race Influence Use of Force by Police?" (2016) 5:1 Sociological Imagination: Western's Undergraduate Sociology Student Journal 1 <https://ojs.lib.uwo.ca/index.php/si/article/view/5310/4455>; and Andrew Russell, "Sask., Quebec arrest videos show 'startling' examples of excessive police force: experts", *Global News* (4 July 2019) <https://globalnews.ca/news/5456773/sask-quebec-arrest-videos-excessive-police-force-experts/>.

mental disabilities.[520] Even if being algorithmically flagged does not increase the likelihood of physical violence, studies have shown that "increased scrutiny and surveillance resulting from the disproportionate patrolling of historically over-policed communities ha[ve] been linked to worsening mental and physical health."[521] Algorithmic technologies that have the potential to continue or to amplify historical patterns of violence against members of marginalized communities would likely constitute a discriminatory impact, violating section 15 equality rights.

Second, predictive policing and algorithmic surveillance that has the perceived or actual effect of baselessly or disproportionately targeting historically marginalized communities may degrade community autonomy, dignity, well-being, and community relations with police services. Such degradation, regardless of whether algorithmic policing technologies are used, impairs community autonomy and well-being, exacerbates pre-existing tensions between police and disproportionately criminalized communities, and brings the administration of justice into disrepute. Deploying algorithmic policing technology to focus patrol forces on neighbourhoods that are predominantly inhabited by section 15 protected groups; to flag marginalized individuals for closer scrutiny before any wrongdoing has occurred; or to monitor their online conversations and social networks (particularly in view of the *Charter* rights to freedom of expression and assembly[522]) would reproduce common and longstanding patterns of systemic discrimination. Deployment in such a manner also continues the historical predisposition of treating vulnerable and marginalized communities as societal laboratories and guinea pigs, wherein they disproportionately or exclusively suffer the consequences of working out the "glitches" before a given technology is either more widely implemented or is abandoned.[523]

520 "There is also a socially significant intersection between race and mental health that may affect officer decisions about use of force. There are stereotypes about Black people regarding violence and criminality, and concerns that police are more likely to use force in their interactions with Black people. Furthermore, people with mental health disabilities may be more likely to be subject to officer use of force because of responses to police instructions or behaviours that may seem unusual, unpredictable or inappropriate, or due to police reliance on stereotypical assumptions about dangerousness or violence. [...] " Ontario Human Rights Commission, *A Collective Impact: Interim report on the inquiry into racial profiling and racial discrimination of Black persons by the Toronto Police Service* (November 2018) <ohrc.on.ca/sites/default/files/TPS%20Inquiry_Interim%20Report%20EN%20FINAL%20DESIGNED%20for%20remed_3_0.pdf#overlay-context=en/news_centre/ohrc-interim-report-toronto-police-service-inquiry-shows-disturbing-results> at 8 (footnote omitted). See also "Further analysis reveals that Black civilians are grossly over-represented in use of force cases in which no mental health crisis was flagged. ... Black civilians are also over-represented in SIU use of force cases where mental health issues were identified. ... White civilians, by contrast, are over-represented in use of force cases that involve civilians who were identified as being in mental health crisis, and under-represented in cases in which no mental health issues were noted..." *Ibid* at 94-95. See also *R v Forcillo*, 2018 ONCA 402; and Katherine Wilton, "Video captures Montreal police fatally shooting mentally ill man", Montreal Gazette (1 March 2019) <https://montrealgazette.com/news/local-news/video-captures-montreal-police-fatally-shooting-mentally-ill-man>.

521 Hannah Couchman, "Policing by Machine: Predictive policing and the threat to our rights," Liberty (January 2019), at 17 (footnotes omitted). The report continues, "This is corroborated by other studies, which show that living in areas where pedestrian stops are more likely to become invasive is associated with worse health, and that reports of trauma and anxiety from young men in New York City increased as the frequency of police contact rose, especially among those reporting intrusive and/or unfair police stops. The increased police contact also created additional opportunities for police violence in over-policed areas."

522 See Section 5.3 ("Rights to Freedom of Expression, Peaceful Assembly, and Association").

523 Virginia Eubanks, "Want to Predict the Future of Surveillance? Ask Poor Communities", The American Prospect (15 January 2014) <https://prospect.org/power/want-predict-future-surveillance-ask-poor-communities./>; Joy Buolamwini, Written Testimony at the Hearing on Artificial Intelligence: Societal and Ethical Implications, United States House Committee on Science, Space and Technology (26 June 2019), at 11-12 <https://science.house.gov/imo/media/doc/Buolamwini%20Testimony.pdf>; See also, in the case of the LGBTQ+ community: Jordan Pearson, "Canadian Internet Filtering Company Says It's Stopped 'Alternative Lifestyles' Censorship", *VICE Motherboard* (21 January 2019), <https://www.vice.com/en_us/article/3kgznn/netsweeper-says-its-stopped-alternative-lifestyles-censorship>; Geoff White, "Use of facial recognition tech 'dangerously irresponsible'", *BBC Click* (13 May 2019) <https://www.bbc.com/news/technology-48222017>; and Blaise Agüra y Arcas, Margaret Mitchell & Alexander Todorov, "Physiognomy's New Clothes" (6 May 2017) <https://medium.com/@blaisea/physiognomys-new-clothes-f2d4b59fdd6a>.

Jonathan Rudin, lawyer and Program Director at Aboriginal Legal Services, provided the following personal views—speaking on behalf of himself only—regarding algorithmic policing and its potential impact on marginalized communities:

> If things are going to be done, there needs to be a level of transparency, sharing of information, and discussion of why things are being done. When Indigenous people don't have trust in systems, it's because they shouldn't have trust in systems. You can't start things by saying, forget all the past stuff and let's move forward. If that's the basis of roll out, they're going to fail. [...] If [involving the community] doesn't happen, the distrust will always be there. That's not paranoia, that's just reality.[524]

Concerns about the community impact of algorithmic policing technologies were not lost on the law enforcement representatives who were interviewed for this report. For example, S/Constable Ryan Prox of the VPD stated, "I'm very sensitive to the fact [that predictive policing risks further targeting of marginalized communities]. If we're going to go down this road and be the first police department in Canada to do this, we have to do our due diligence. This is a high-risk undertaking that we've taken as much proactive steps to prevent violations of people's civil rights as possible."[525] Similarly, a representative of the SPPAL stated, "If the tech or the algorithms or any results don't yield to improved outcomes for kids or people who are vulnerable or make the community safer, then there's no reason to use any of this tech."[526] It is apparent that there is, ostensibly, consensus among the Canadian law enforcement representatives interviewed for this report, with respect to not desiring to put historically marginalized and vulnerable communities at risk of being harmed by algorithmic policing technologies. Given such consensus, police services must meaningfully consult with and listen to those same communities prior to, during, and after implementation of any such technologies, especially groups that are protected under section 15 of the *Charter* and most subjected to or affected by algorithmic policing.

### 5.4.3. Socio-economic Disadvantage and Hypervisibility to Algorithmic Policing

Algorithmic discrimination may occur by virtue of simply existing in society in a way that makes a person more visible to law enforcement monitoring and to state and police data collection apparatuses. Professor Virginia Eubanks explains, "[m]arginalized groups face higher levels of data collection when they access public benefits, walk through highly policed neighborhoods, enter the health-care system, or cross national borders. That data acts to reinforce their marginality when it is used to target them for suspicion and extra scrutiny."[527] Beyond the immediate privacy and liberty concerns,[528] such increased "data visibility" of marginalized groups may itself amount to a

524 Interview of Jonathan Rudin by Cynthia Khoo & Yolanda Song (8 May 2019).

525 Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019).

526 Interview of a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) by Cynthia Khoo (23 July 2019).

527 Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (New York: St. Martin's Press, 2018) at 7. Eubanks also points out that means-testing social welfare programs have "rationalized all manner of surveillance and policing of applicants and beneficiaries." *Ibid* at 28.

528 For a full discussion of algorithmic policing and the right to privacy, see Section 5.2 ("Right to Privacy"); for analysis of algorithmic policing

section 15 violation. The phenomenon perpetuates disadvantage for section 15 protected groups by exposing them to unequal and more relentless application of the law (as exercised through police officers), while weakening the protection of the law to which they are entitled. Specifically, this unequal and unfair application of law may infringe upon their rights to privacy, to be free from unreasonable search and seizure, and to be free from arbitrary detention. These rights are protected under sections 8 and 9 of the *Charter*, respectively, as well as under human rights legislation.

In her in-depth analysis of how algorithmic decision-making harms impoverished individuals, Eubanks connects the dots between the poor being historically criminalized and the state using that imputed criminality to justify invasive data collection demands, in exchange for access to government services to meet basic needs. She writes:

> This kind of blanket access to deeply personal information makes little sense outside of a system that equates poverty and homelessness with criminality. As a point of contrast, it is difficult to imagine those receiving federal dollars through mortgage tax deductions or federally subsidized student loans undergoing such thorough scrutiny, or having their personal information available for access by law enforcement without a warrant. Moreover, the pattern of increased data collection, sharing, and surveillance reinforces the criminalization of the unhoused, if only because so many of the basic conditions of being homeless—having nowhere to sleep, nowhere to put your stuff, and nowhere to go to the bathroom—are also officially crimes.[529]

The "[c]riminalization of the unhoused" also occurs throughout Canada.[530] Such criminalization has the effect of making those who are homeless more susceptible to being drawn into the criminal justice system than those who engage in illegal activities from within the walls of private property. Sarah Brayne elaborates on the dangers that result from this form of algorithmic bias when she explains that "[t]he retroactive nature of policing in an era of dragnet data collection means information is routinely accumulated and files are lying in wait. In that sense, individuals [who are poor, homeless, or racialized] lead incriminating lives—daily activities, now codified as data, can be marshaled as evidence ex post facto."[531] Brayne further notes that "[u]nchecked predictions … may justify the over-policing of minority

---

and the right to liberty and freedom from arbitrary detention, see Section 5.5 ("Right to Liberty and to Be Free from Arbitrary Detention").

529 *Ibid* at 116-117.

530 See e.g., Justin Douglas, "The Criminalization of Poverty: Montreal's Policy of Ticketing Homeless Youth for Municipal and Transportation By-Law Infractions" (2011) 16 Appeal 49; Damian Collins & Nicholas Blomley, "Private Needs and Public Space: Politics, Poverty, and Anti-Panhandling By-Laws in Canadian Cities" in Law Commission of Canada, *New Perspectives on the Public-Private Divide* (Vancouver: UBC Press, 2003) at 56 <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.119.4772&rep=rep1&type=pdf#page=56>; Jackie Esmonde, "Criminalizing Poverty: The Criminal Law Power and the Safe Streets Act" (2002) Journal of Law and Social Policy 63; "The city where it's against the law to be poor", *CBC Radio* (4 January 2015) <https://www.cbc.ca/radio/thesundayedition/law-against-poverty-michael-s-essay-talking-to-terrorists-socks-for-the-homeless-documentary-1.2943464/the-city-where-it-s-against-the-law-to-be-poor-1.2943469>; and Stephen Gaetz, "The Criminalization of Homelessness: A Canadian Perspective" (2013) European Journal of Homelessness 357 <https://www.feantsa.org/download/sg_response7772916537698278481.pdf>.

531 Sarah Brayne, "Big Data Surveillance: The Case of Policing" (2017) 82:5 American Sociological Review 977 at 1000-01. Andrew Ferguson also discusses the dangers of facial recognition in particular, for those who are homeless or otherwise forced to spend more time on the streets: "[T]he real ground-breaking shift will be when facial recognition technology can be used to match individuals on the street to risk-scores in a computer. While currently such real-time facial recognition technology does not exist—being limited to stationary video cameras—the technology is being developed to deploy facial recognition on police cameras and even police body-worn cameras. In this new world, the

communities and potentially take away resources from individuals and areas invisible to data collection sensors or subject to systematic underreporting."[532]

> *One of the biggest tricks about all the algorithmic and predictive policing technology is it only seems to be good to expose the crimes of the poor. [...] There's no* Minority Report, *as it were, for the wealthy.*
>
> *- Desmond Cole (Author, Journalist, and Racial Justice Activist)*[533]

What Eubanks and Brayne discuss is a form of the adage 'what gets measured, gets managed': because those who live near or below the poverty line and the otherwise marginalized are more often subjected to a kind of measurement through state monitoring, quantification, and reduction to crude data points, they become systematically more susceptible to so-called management—and mismanagement—by law enforcement, in a way that more privileged members of society are not.[534] The concern with algorithmic policing technologies in this context is that they overwhelmingly focus on certain types of crimes and offenders (e.g., street-level property crime or gang violence) while neglecting to train the same algorithmic eye on other kinds of crimes and offenders (e.g., environmental crime or criminal harassment). To be clear, this is not to say that algorithmic surveillance should be expanded to include a broader swath of crimes, given the privacy considerations expounded on in Section 5.2 ("Right to Privacy"). Rather, these trends constitute another form of inequality that is attached to algorithmic policing where marginalized groups are concerned.

Specifically, the selectivity of focus may constitute a form of adverse effects discrimination under section 15 if using algorithmic policing technology for certain types of crime means that

---

combination of facial recognition and the heat list will mean that each person on the street can be scored and tracked." Andrew Guthrie Ferguson, "Illuminating Black Data Policing" (2018) 15 Ohio State Journal of Criminal Law 503 at 521 (footnotes omitted).

532 Sarah Brayne, "Big Data Surveillance: The Case of Policing" (2017) 82:5 American Sociological Review 977 at 998 (footnotes omitted). Brayne's statement draws attention to the fallacy that what a system can measure happens to be an appropriate, let alone the best, metric by which to assess outcomes, when this may not be the case. See also Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (New York: Crown Publishing Group, 2016). In fact, such indicators may simply have been the most easily measured and, thus, incorrectly treated as the most important indicators of effective law enforcement or of community safety. To the authors' knowledge, there have been no studies that have determined that focusing exclusively on developing predictive policing for street crimes would lead to greater total community safety and well-being compared to focusing instead on preventing certain other kinds of crimes with the same amount of resources.

533 Interview of Desmond Cole by Cynthia Khoo & Yolanda Song (31 May 2019).

534 In another example of the adage, empirical research conducted by Scot Wortley and other researchers centres racism and racial profiling by police services as the phenomenon to be measured, and thus more given to be "managed", or addressed as a serious public policy problem and justice system concern. See e.g., Scot Wortley, "Police Use of Force in Ontario: An Examination of Data from the Special Investigations Unit: Final Report" (Research Project Conducted on behalf of the African Canadian Legal Clinic for Submission to the *Ipperwash Inquiry*) <https://www.attorneygeneral.jus.gov.on.ca/inquiries/ipperwash/policy_part/projects/pdf/AfricanCanadianClinicIpperwashProject_SIUStudybyScotWortley.pdf>; Scot Wortley & Akwasi Owusu-Bempah, "The usual suspects: police stop and search practices in Canada" (2011) 21:4 Policing and Society 395; Steven Hayle, Scot Wortley, & Julian Tanner, "Race, Street Life, and Policing: Implications for Racial Profiling" (2016) 58:3 Canadian Journal of Criminology and Criminal Justice 322.

disproportionate focus is directed towards members of communities who are defined by protected grounds (as opposed to instead turning the state's formidable surveillance apparatus upon predicted suspects and potential offenders with sociopolitical and socioeconomic advantage).[535] Further, socio-economic disadvantage is intertwined with, and often a direct intergenerational result of, the historic and ongoing systemic disadvantage experienced on the basis of other protected grounds.[536] Poverty, homelessness, and socio-economic status must, therefore, be taken into account before adopting any new technologies where criminal jeopardy is at stake.

The presence and activities of marginalized individuals may be simply more visible to algorithmic policing technology and related law enforcement tools that purport to detect signs of criminality; visibility alone, however, does not indicate anything about actual criminality. Yet, this disproportionate exposure to being seen, scrutinized, and processed by the criminal justice system involves particularly high stakes for communities that are already over-policed and unjustly overrepresented throughout subsequent stages of the system. A Black or Indigenous individual, for example, is at higher risk of surveillance, monitoring, and suspicion to begin with and, once monitored, is then at higher risk of being searched or detained and arrested. Once detained, they are at higher risk of being subjected to unnecessary use of force. Once arrested, they are at higher risk of being charged. Once charged, they are at higher risk of being incarcerated, with more or harsher conditions, and for longer periods, compared to white individuals. And, finally, once incarcerated, they are at higher risk of being subjected to more punishing treatment and abuse, compared to white individuals under the same or similar circumstances.

Therefore, initial encounters with law enforcement, which may be considered "low stakes" by members of groups (such as the affluent or the politically powerful) that have historically enjoyed good relations with criminal justice institutions, "can lead to more serious police interventions" in the case of historically overpoliced groups.[537] Every encounter risks violating a marginalized individual's right to liberty and equality, right to be free from discrimination, and right to be free from unreasonable search and seizure. Any one of these initial violations may easily snowball into layers of subsequent abuses and unjust treatment at every subsequent stage in the criminal justice system, even where the impacted individual did nothing to warrant scrutiny in the first instance. What may have begun as a

535 For a satirical and pointed proof-of-concept, see Brian Clifton, Sam Lavigne, & Francis Tseng, "Predicting Financial Crime: Augmenting the Predictive Policing Arsenal", *The New Inquiry* (2017) <https://arxiv.org/pdf/1704.07826.pdf>; "White Collar Crime Risk Zones", Brian Clifton, Sam Lavigne, & Francis Tseng, "White Collar Crime Risk Zones", *The New Inquiry* <https://whitecollar.thenewinquiry.com>; and Katharine Schwab, "Proof That Algorithms Pick Up Our Biases, In A Single Map", *Fast Company* (26 April 2017) <https://www.fastcompany.com/90111752/proof-that-algorithms-pick-up-our-biases-in-a-single-map>.

536 See e.g., Bourassa et al, "Understanding the Intergenerational Effects of Colonization: Aboriginal Women with Neurological Conditions—Their Reality and Resilience" (2015) 10:2 *International Journal of Indigenous Health* (revised references 2016) 3 at 9-11; Savannah Hope et al, "Intergenerational Trauma and Aboriginal Homelessness" (September 2017), online (pdf): Social Planning and Research Council of Hamilton <http://www.sprc.hamilton.on.ca/wp-content/uploads/2017/09/Intergenerational_Trauma_and_Aboriginal_Homelessness_2017.pdf>; Valerie J Pruegger, Derek Cook & Sybille Richter-Salomons, "Inequality in Calgary: The Racialization of Poverty" (2009), online (pdf): *City of Calgary* <https://www.calgary.ca/csps/cns/publications-guides-and-directories/inequality-in-calgary.html>; and Paul J Kim, "Social Determinants of Health Inequities in Indigenous Canadians Through a Life Course Approach to Colonialism and the Residential School System" (2019) 3:1 Health Equity 378.

537 Ontario Human Rights Commission, Under Suspicion: *Research and consultation report on racial profiling in Ontario* (April 2017), at 38 <http://www.ohrc.on.ca/en/under-suspicion-research-and-consultation-report-racial-profiling-ontario>.

mistake or misconduct based on racial profiling, a biased data set, a poorly designed algorithm, or all of the above, can result in algorithmically altered fates with severe and far-reaching repercussions for marginalized individuals and communities that are protected under section 15 of the *Charter*.

# The Evolving Law of Socio-economic Status as a Protected Human Rights Ground of Equality and Freedom from Discrimination

The constitutionality of discrimination on the basis of low-income socio-economic status is an evolving issue in Canada. Canadian courts do not yet generally recognize poverty or socio-economic status as falling under an analogous ground under section 15. Legal scholars have called for the acceptance of poverty as a defining characteristic that gives rise to section 15 protection under the *Charter*.[538] Multiple appellate decisions have begun to trace the contours of an emergent acknowledgement of the link between socio-economic status and discrimination. Full recognition of this link would ensure that individuals who lack socio-economic status have equally meaningful access to *Charter* rights in Canada.[539]

For example, in the 2018 decision in *R v Meads*,[540] the Ontario Court of Appeal struck down legislation that denied individuals enhanced credit for pretrial custody on the ground that they had failed to show cause why they should not be held in pretrial detention (as opposed to being released on bail). The Court held that one reason the law violated section 7 of the *Charter* was that well-heeled individuals are more likely to demonstrate why they should make bail. This analysis is significant in the context of predictive policing tools because being able to make bail is essentially a question about risk (or lack thereof) and, in that way, is analogous to a predictive tool. The Court's reasoning has implications for an equality rights analysis of algorithmic policing because the Court said that disproportionately disadvantaging accused persons who are indigent violates the *Charter*. *Meads* was decided under section 7 (the law was overbroad), but it is relevant to section 15 because the law was overbroad based on principles of equality and freedom from discrimination. The Court found that "poor and socially isolated individuals," due to poverty, mental health, or addiction, would not have access to the resources required to prove they met the criteria for pretrial release. Detention would thus result from "social and economic disadvantage" rather than any misconduct. The law thus bore "no rational connection to the objective of deterring misconduct on release."[541]

Examples of the relevance of poverty as an analogous ground appear in decisions from lower courts and tribunals that have recognized narrower related characteristics—such as public-housing

538 See e.g., the history tracing jurisprudence of an "effort to disappear the poor within section 15(1)" in Kerri Froc, "Immutability Hauntings: Socioeconomic Status and Women's Right to Just Conditions of Work under Section 15 of the *Charter*" in Martha Jackman and Bruce Porter, eds, Advancing Social Rights in Canada (Toronto: Irwin Law, 2014) 187.

539 *R v Boudreault*, 2018 SCC 58; *Quebec (Attorney General) v Alliance du personnel professionnel et technique de la santé et des services sociaux*, 2018 SCC 17; and *R v Le*, 2019 SCC 34 at para 59.

540 *R v Meads*, 2018 ONCA 146.

541 *Ibid* at para 46.

tenants; racialized, single, immigrant mothers or women; and single mothers receiving social welfare—as analogous grounds.[542] Provincial human rights law in Quebec,[543] New Brunswick, and the Northwest Territories also recognize "discrimination against those suffering from social and economic disadvantage, such as social assistance recipients and workers in precarious and low-paying positions, who face discriminatory assumptions regarding, for example, their ability to pay for rent or goods and services."[544]

In the criminal justice context, *R v. Le* is a landmark constitutional liberty and privacy case involving racialized individuals and the socio-economically disadvantaged. In this decision, the Supreme Court of Canada established that "we have arrived at a place where the research now shows disproportionate policing of racialized and low-income communities."[545] This developing equality jurisprudence will have consequences in future case law and, thus, needs to be monitored given the mounting recognition that poverty itself has long been a basis of wrongful discrimination.

542 *Sparks v Dartmouth/Halifax (County) Regional Housing Authority*, 119 NSR (2d) 91 (NSCA); *Kearney v Bramalea Ltd.* (No. 2) (1998), 34 CHRR D/1 (Ont Bd Inq); and *Falkiner et al v Ontario (Director of Income Maintenance, Ministry of Community & Social Services)* (2002), 159 OAC 135 (CA).

543 "According to the Commission, social profiling is a form of discrimination pursuant to section 10 of the *Quebec Charter of Human Rights and Freedoms*... including 'social condition.' Social condition has been a prohibited ground of discrimination under the Quebec *Charter* since its adoption in 1975. ... Homelessness has been accepted by human rights tribunals, courts, and the Quebec Human Rights Commission as a form of 'social condition.'" Marie-Eve Sylvestre and Céline Bellot, "Challenging Discriminatory and Punitive Responses to Homelessness in Canada" in Martha Jackman and Bruce Porter, eds, *Advancing Social Rights in Canada* (Toronto: Irwin Law, 2014) 155 at 172-73.

544 "Both Quebec and New Brunswick also adopt an objective-subjective test for social condition in the guidelines of their respective human rights commissions. ... This test has evolved over time in Quebec to address discrimination against those suffering from social and economic disadvantage, such as social assistance recipients and workers in precarious and low-paying positions, who face discriminatory assumptions regarding, for example, their ability to pay for rent or goods and services." Wayne MacKay & Natasha Kim, "Adding Social Condition to the *Canadian Human Rights Act*", *Canadian Human Rights Commission* (February 2009) at 3 <http://publications.gc.ca/collections/collection_2012/ccdp-chrc/HR4-14-2009-eng.pdf>.

545 *R v Le*, 2019 SCC 34 at para 97.

## 5.4.4. Inequality by Design and "Math-washing" Injustice

Adverse effects discrimination in algorithmic policing can result from how an algorithm is designed.[546] Software programmers make a number of consequential choices when developing code that will be used for criminal justice. These choices can be laden with pre-existing biases, value judgments, lack of domain expertise or lived experience, or ignorance with respect to the real consequences of certain mathematical decisions for marginalized individuals and their communities.

For example, Equivant (formerly Northpointe) designed the recidivism prediction algorithm, the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) according to a certain understanding of what they considered it meant for an algorithm to be fair.[547] Yet COMPAS enshrined, in code, bias against Black defendants—locking in inequality by design. According to computer scientist Arvind Narayanan, there are at least 21 different definitions of fairness that could be used in designing an algorithm, each of which promotes certain values and politics over others.[548] Those who develop an algorithm such as COMPAS may have to choose (or may unknowingly decide) between, for example, prioritizing equal predictive accuracy for all groups, prioritizing minimizing false negatives over minimizing false positives,[549] or prioritizing the maximization of true positives at the expense of increasing false positives. Many design choices involve a trade-off in one way or another, but those who are most impacted by police algorithms—such as individuals who are brought into the criminal justice system or wrongfully criminalized by law enforcement authorities that rely on algorithmic assessments—have little say in which trade-offs are made.

Algorithms that are used for policing and law enforcement purposes and that, by design, perpetuate disadvantage for individuals in a protected group would be, or ought to be, considered a violation of section 15. In *Ewert v. Canada*, for instance, the impugned risk assessment tools were designed, developed, tested, and validated without Indigenous defendants in mind and without their involvement, even though these tools are now used disproportionately on Indigenous individuals—which is, itself, a result of their general over-representation in the criminal justice system, due to factors described in Section 2.1 ("Criminal Justice and Systemic Discrimination in Canada"). The Supreme Court of Canada did not find that the Correctional Service of Canada's use of these tools violated Mr. Ewert's section 15 rights, on the basis that there was insufficient evidence that the tools "in fact overestimate the

546 "Given the flexible and malleable way in which ML [machine learning] algorithms learn and develop, training the algorithm can be fraught with hazards as regards the characterisation and weighting given to the input data." Royal United Services Institute, *Machine Learning Algorithms and Police Decision-Making: Legal, Ethical and Regulatory Challenges* (September 2018) at 24-25 <https://rusi.org/sites/default/files/201809_whr_3-18_machine_learning_algorithms.pdf.pdf>.

547 Specifically, Northpointe calibrated the algorithm so that it would have the same predictive accuracy rate for both white and Black defendants across the board, but this resulted in the algorithm having a higher false positive rate for Black defendants and higher false negative rate for white defendants. Matthias Spielkamp, "Inspecting Algorithms for Bias", *MIT Technology Review* (12 June 2017) <https://www.technologyreview.com/s/607955/inspecting-algorithms-for-bias/>.

548 Arvind Narayanan, "Tutorial: 21 fairness definitions and their politics" (1 March 2018), YouTube <https://www.youtube.com/watch?v=jIXIuYdnyyk>; Arvind Narayanan, "Tutorial: 21 fairness definitions and their politics" (23 February 2018), Google Docs <https://docs.google.com/document/d/1bnQKzFAzCTcBcNvW5tsPuSDje8WWWY-SSF4wQm6TLvQ/edit>.

549 Hannah Couchman, "Policing by Machine: Predictive policing and the threat to our rights," (January 2019) *Liberty*, at 50-51 <https://www.libertyhumanrights.org.uk/sites/default/files/LIB%2011%20Predictive%20Policing%20Report%20WEB.pdf>.

risk posed by Indigenous inmates or lead to harsher conditions of incarceration or to the denial of rehabilitative opportunities because of such an overestimation."[550] This finding suggests that where there is evidence of such overestimation, harsher consequences, or denial of benefits for a protected group—as is the case with COMPAS—it would be open to a court to find that reliance on such a tool does violate section 15.

Algorithmic policing technologies may not only encode inequality and discrimination into the criminal justice system, but they also mask this injustice by virtue of their reliance on algorithms; the adoption of these tools can provide algorithmic policing systems a veneer of scientific and mathematical "infallibility", "neutrality", or "objectivity". This phenomenon of "math-washing"[551] situations simultaneously obscures the root causes of inequality and related socio-political injustices, which algorithms are put forth to ostensibly "solve," while redirecting time, attention, and resources away from genuine reforms of underlying structural or institutional systems and patterns of harm.[552] According to Ruha Benjamin, algorithmic band-aids for deep-seated societal ills "offer pragmatic inclusion in place of political and social transformation. [...] New Jim Code fixes are a permanent placeholder for bolder change."[553]

As an example, the Stop LAPD Spying Coalition points to systemic racism as the core issue that law enforcement agencies, governments, and broader society must address. Rather than trying to improve algorithmic policing, "critical race theorists contend that ... the complete dismantling of racism in one context necessitates concomitant consideration of other forms of oppression in other contexts... A more equitable application of the LASER program, if it were even possible, should not be the goal then. Such colorblind policies are not sufficient to adequately address institutionalized racism, which the LASER program is but one manifestation of."[554] Put another way, problems related to inequality in the criminal justice system existed before and outside of algorithms; their solutions are beyond the purview and constraints of algorithms as well.

550 *Ewert v Canada*, 2018 SCC 30 at para 79.

551 "Mathwashing" is "the assumption that algorithmic models don't have subjectivity baked into them because they involve math": Elizabeth E Joh, "Feeding the Machine: Policing, Crime Data, & Algorithms" (2017) 26:2 William & Mary Bill of Rights Journal 287 at 292 <https://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1835&context=wmborj>. The term was coined by a former data scientist at Kickstarter, Fred Benenson, who described it as follows: "Mathwashing can be thought of using math terms (algorithm, model, etc.) to paper over a more subjective reality." Tyler Woods, "'Mathwashing,' Facebook and the zeitgeist of data worship", *Technical.ly* (8 June 2016) <https://technical.ly/brooklyn/2016/06/08/fred-benenson-mathwashing-facebook-data-worship/>.

552 "ADS [automated decision systems] are often adopted to avoid or obfuscate broader structural and systemic problems in society – problems that are often beyond the capacity of cash-strapped agencies to address meaningfully." Meredith Whittaker et al, "AI Now Report 2018" (December 2018), *AI Now Institute*, at 40 <https://ainowinstitute.org/AI_Now_2018_Report.pdf>.

553 Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code* (Cambridge: Polity Press, 2019) at 156-57.

554 Stop LAPD Spying Coalition, "Before the Bullet Hits the Body: Dismantling Predictive Policing in Los Angeles" (8 May 2018) at 19 <https://stoplapdspying.org/wp-content/uploads/2018/05/Before-the-Bullet-Hits-the%20-Body-May-8-2018.pdf>. "LASER" refers to the Los Angeles' Strategic Extraction and Restoration Program, the LAPD's predictive policing initiative, which was introduced in Section 4.2 ("Person-Focused Algorithmic Policing").

## 5.4.5. Concluding Comments: Algorithmic Policing and the Right to Equality and Freedom from Discrimination

Equality and discrimination concerns are at the heart of many issues with algorithmic policing technologies. Such technologies combine two fields that have historically discriminated against section 15 protected groups: criminal justice and algorithmic decision-making (as a subset of the technology sector more broadly). In addition to the specific equality issues discussed above, two additional cross-cutting considerations are core to assessing algorithmic policing technologies with regard to section 15 rights.

First, section 15 violations that may occur through algorithmic policing can disproportionately impair marginalized individuals' other *Charter* rights, such as the right to privacy and to be free from unreasonable search and seizure,[555] the right to liberty and to be free from arbitrary detention,[556] and the right to a presumption of innocence.[557] As such, where the state engages with, uses, or relies on algorithmic policing technologies to the particular detriment of marginalized communities—such as collecting private-sector data from commercial entities, seeking data from social services agencies that primarily serve marginalized communities, using data-mining techniques to identify individuals based on protected characteristics, or more frequently conducting police stops on marginalized individuals or within their communities based on algorithmic indicators—the state may be violating its domestic and international human rights obligations to uphold equality and freedom from discrimination.

Second, given the opaque and often privatized nature of algorithmic policing technology, the deep-seated prevalence of systemic discrimination and the historical difficulties of proving adverse effects discrimination in court,[558] lawmakers should consider implementing a reverse onus in section 15 claims concerning algorithmic bias. Teresa Scassa has pointed out that in *Ewert v. Canada*, it "took [the defendant] 18 years [and] a dedicated team of lawyers"[559] to advance the litigation. She has suggested that a requirement "to demonstrate discriminatory impacts or effects, or to show how the algorithm itself and/or the data used to develop it incorporate biases or discriminatory assumptions [...] will impose a significant evidentiary burden"[560] on future parties, who will likely be already marginalized individuals. Legal scholars have also previously suggested implementing a reverse onus in the context

555 See Section 5.2 ("Right to Privacy").

556 See Section 5.5 ("Right to Liberty and to Be Free from Arbitrary Detention").

557 *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11, s 11(d).

558 "To date, few decisions of the Supreme Court have dealt with adverse effect discrimination, perhaps because of the significant practical difficulties involved in adducing sufficient evidence to demonstrate adverse impacts on particular groups, such as women (*Symes v. Canada*, [1993] 4 S.C.R. 695). Where adverse impact claims have succeeded under the *Charter*, they have been based on self-evident societal patterns amenable to judicial notice..." "Section 15 – Equality rights", Department of Justice (17 June 2019) <https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art15.html>.

559 Teresa Scassa, "Supreme Court of Canada Decision Has Relevance for Addressing Bias in Algorithmic Decision-Making", Teresa Scassa (14 June 2018) <www.teresascassa.ca/index.php?option=com_k2&view=item&id=278:supreme-court-of-canada-decision-has-relevance-for-addressing-bias-in-algorithmic-decision-making&Itemid=80>.

560 *Ibid*.

of racial profiling and arbitrary detention under section 9 of the *Charter*, based on similar equitable considerations.[561] Shifting this burden would recognize the formidable challenges facing equality-seeking and marginalized individuals who are trying to prove that an algorithmic policing technology is discriminatory. Such individuals' lack of access to a given algorithm, combined with other areas of stark information asymmetry, will almost undoubtedly put state actors and private sector businesses in the best position to provide the relevant evidence in nearly every case.

Lastly, several policy recommendations flow from analyzing bias in design, data, policing, and community impact in the context of algorithmic policing technology. These recommendations would mitigate the risks or impacts of section 15 violations associated with such technology, and should begin with ensuring that historic police data sets are not used to train or operate law enforcement algorithms. Preventing and mitigating section 15 violations also requires meaningful involvement and consultation of marginalized and historically over-criminalized communities be integrated into any design, development, or implementation process of an algorithmic policing technology. While training police officers plays a role, to mitigate unconscious bias and automation bias where they are sent to algorithmic "hot spots" or where they engage with "heat list" or algorithmically risk-assessed individuals, studies have shown that such training is often not effective and thus cannot weigh against substantive reasons to ban or severely limit the use of algorithmic policing technologies where they introduce risks to equality and freedom from discrimination. Further prevention or mitigation measures include tracking output data of policing algorithms on an ongoing basis to monitor for problematic trends that appear to target marginalized communities or display bias against section 15 protected groups; establishing a firewall to prevent or minimize data-sharing between social service providers and law enforcement agencies; and reconsidering whether an algorithmic policing technology is truly an appropriate solution, as opposed to directing resources and attention to underlying substantive societal issues and root causes such as systemic racism or classism.

## 5.5. Right to Liberty and to Be Free from Arbitrary Detention

Canadian constitutional law and international human rights law guarantee the right to life, liberty, and security of the person, including the right not to be detained arbitrarily. The Universal Declaration of Human Rights and ICCPR both establish "the right to liberty and security of person" and the right

561 See e.g., "In light of this evidence [of racial profiling of Black drivers] and the evidence of systemic racism in Canada, the evidentiary burden under section 9 should shift to the Crown to establish, on a balance of probabilities, that a so-called routine vehicle stop of a Black driver was not motivated by race. [...] Not only is this burden consistent with equality and fairness principles, but also, with precedent and policy. [...] Since the police are part of the administration of justice, the Crown should be held accountable for police misconduct such as racial profiling." David M Tanovich, "Using the *Charter* to Stop Racial Profiling: The Development of an Equality-Based Conception of Arbitrary Detention" (2002) 40:2 Osgoode Hall Law Journal 145 at 181-82. Regarding the establishing of investigative detention in *R v Mann*, 2004 SCC 52: "[G]iven the evidence of amenability to abuse, the odd fit between investigative detentions and ss. 10(a-c) of the *Charter*, and the novel nature of the power, had it been alive to the racial aspect of this issue, the Supreme Court might have held that the Crown should bear the burden of showing that an investigative detention is reasonable and justified." Benjamin L Berger, "Race and Erasure in *R. v. Mann*" (2004) 21 Criminal Reports (Articles) 58 (WL). See also Gabriella Jamieson, "Using Section 24(1) *Charter* Damages to Remedy Racial Discrimination in the Criminal Justice System" (2017) 22 Appeal 71 at 85-86 ("A Shifting Burden in the Future?").

not to be "subjected to arbitrary arrest or detention."[562] Similarly, section 9 of the Canadian *Charter* provides every individual with "the right not to be arbitrarily detained or imprisoned," while section 7 guarantees that everyone "has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice."[563]

Algorithmic policing technologies engage section 9 and section 7 liberty rights because they increase the risk that an individual may be arrested or detained arbitrarily or deprived of their liberty in a manner that is not in accordance with the principles of fundamental justice. The following subsections of this report analyze two central concerns with algorithmic policing technologies in this regard. Section 5.5.1 demonstrates how relying on an algorithmic policing technology to arrest or detain an individual may not satisfy the "reasonable suspicion" or "reasonable grounds" standard in Canadian law. Reliance on algorithmic predictions does not satisfy the requisite standard because algorithmic predictions involve generalized predictions that may result in generalized suspicion, supplanting individualized assessments of someone's personal characteristics and behaviour, thus potentially rendering the arrest or detention unconstitutional. Section 5.5.2 discusses the problem of unconscious bias among law enforcement officers and other actors in the criminal justice system, specifically as manifested in racial bias and racial profiling. Algorithmic policing technologies may contribute to increased racial profiling, which Canadian courts have established renders a detention or arrest arbitrary and thus unconstitutional.

Due to some overlap in subject matter, the legal and policy analysis in this section will focus on section 9 and arbitrary arrest and detention, while section 7 issues will be discussed later in Section 5.6 ("Right to Due Process").

## 5.5.1. Algorithmic Policing and Generalized Suspicion

In Canadian criminal and constitutional law, the standard of reasonable suspicion is what prevents a detention from being arbitrary and thus unconstitutional. The standard "prevents the indiscriminate and discriminatory exercise of police power."[564] Algorithmic policing may threaten the right to be free from arbitrary detention based on the ways in which algorithmic predictions may interact with police officers' suspicions in practice, and how those predictions may influence the legal analysis for reasonable suspicion in law.[565]

For suspicion to be "reasonable," section 9 jurisprudence requires the suspicion to be specific to an individual's characteristics and behaviours. The grounds for detention must be reasonable and

562 The UDHR states, "Everyone has the right to life, liberty and security of the person" and "No one shall be subjected to arbitrary arrest, detention or exile:" *Universal Declaration of Human Rights*, adopted December 10, 1948, GA Res 217A(III), UN Doc A/810 at 71 (1948), arts 3 and 9. Article 9 of the ICCPR states, "Everyone has the right to liberty and security of person. No one shall be subjected to arbitrary arrest or detention. No one shall be deprived of his liberty except on such grounds and in accordance with such procedure as are established by law."

563 *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11, ss 7 and 9.

564 *R v Mann*, [2004] 3 SCR 59; *R v Chehil*, 2013 SCC 49 at para 3.

565 See generally Andrew Guthrie Ferguson, "Predictive Policing and Reasonable Suspicion" (2013) 62:2 Emory Law Journal 259 at 309-310.

objectively established.[566] Determining reasonable suspicion involves assessing "the totality of the circumstances, based on objectively discernible facts, and is subject to independent and rigorous judicial scrutiny."[567] As such, the grounds for a detention cannot be formed on the basis of unreliable information—such as faulty or inaccurate data—or for biased or discriminatory inferences. Using algorithmic predictions to justify a deprivation of liberty (e.g., an investigative detention on the street) thus raises section 9 concerns should the police service not have established the reliability of the algorithm or its underlying data.

Algorithmic policing methods tend to rely on generalized inferences by definition. As such, these methods contravene established law that reasonable suspicion cannot rely on generalized suspicion,[568] such as suspicion based on beliefs about an ethnic group or on the location where an individual was found. Relying on algorithmic policing technologies as grounds for suspicion may violate section 9 where the algorithmic prediction(s) are based on statistical trends as opposed to being particularized to a specific individual.

Officers may subconsciously rely on a risk prediction generated by an algorithm to form grounds for suspicion that they consider to be "reasonable" even if "the actions of [a suspected or detained individual] have not changed at all. Objectively, what the suspect has done is no more or less suspicious or criminal than an individual who was not subject to an elevated risk prediction. Yet the prediction, in combination with a profile of generalized criminal activity," may be relied on by the officer to formulate suspicions or justify a detention—even if there had been no other cause for suspicion in the absence of the algorithmic tool.[569] Algorithmic predictions may thus result in detentions that are rooted in generalized suspicion or questionable reliability in either the algorithm or its underlying data. The result is a potential increase in unconstitutional detentions (including police stops) than may have occurred in the absence of algorithmic policing technologies.

Research in this field has widely recognized the problem of 'automation bias', defined as the tendency of humans "to rely on the judgments of automated decisions as superior to their own, even when they have reason to believe the technology is flawed."[570] Acknowledging these concerns in an interview for this report, S/Constable Ryan Prox of the VPD responded that officers are trained explicitly against relying on algorithmic predictions as grounds for suspicion.[571] However, neither the interview nor research for this report identified formal written policies that would reinforce this training. In

566 *R v Chehil*, 2013 SCC 49.

567 *Ibid* at para 3.

568 *R v Kang-Brown*, 2008 SCC 18.

569 Andrew Guthrie Ferguson, "Predictive Policing and Reasonable Suspicion" (2013) 62:2 Emory Law Journal 259.

570 Lindsey Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border" (2017) 41 *NYU Review of Law & Social Change* 327 at 342-43 <https://socialchangenyu.com/wp-content/uploads/2017/09/barrett_digital_9-6-17.pdf>.

571 Prox stated, "In terms of training, we make it very clear that if the police officers are deployed at forecasted locations, you cannot use the forecasting system as grounds for a street check. […] Just because you see somebody walking down the street, the forecasting doesn't give you licence to do a street check. You still need to form your grounds to engage in any capacity with a member of the public." Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019).

addition, training alone is likely insufficient to remove the risk of automation bias among officers.[572] Moreover, training is only one component of broader police culture and practices, and the VPD is only one of more than 140 municipal police services in Canada.[573] Without establishing effective training, technological literacy, cultural competence, and related best practices throughout all law enforcement agencies across the country, individuals remain at an elevated risk of having their section 9 rights violated by way of automation bias and other biases in algorithmic policing. Clear written policies, directives, and meaningful accountability mechanisms are recommended and discussed further in Part 6 ("Recommendations and Conclusion") of this report.

### 5.5.2. Unconscious Bias and Racial Profiling

Algorithmic policing technologies are highly susceptible to incorporating and perpetuating the unconscious biases of their developers, reflecting biases embedded in their training data, and exacerbating any unconscious bias in the humans who use such technology. Their outputs about suspicious persons or places can perpetuate bias. Factors grounding reasonable suspicion "must respect *Charter* principles [and] must relate to the actions of the subject of an investigation, and not his or her immutable characteristics."[574] Relying on algorithmic tools may thus create significant constitutional and human rights issues where the algorithm generates predictions on the basis of an individual's immutable characteristics (or known proxies for immutable characteristics) or demonstrates bias against particular groups.

For example, section 9 of the *Charter* renders it unconstitutional to engage in racial profiling as a basis for a detention. Racial profiling can occur through algorithms and be tacitly legitimized as a result of "math-washing."[575] Canadian courts have expressly held that racial profiling can be proven through the existence of numerous factors, and they do not require explicit proof of overt bias in the mind of the police officer at the time of the detention. This principle stems from recognizing that "the attitude underlying racial profiling is one that may be consciously or unconsciously held, and racial profiling can be the product of overt, subconscious, or institutional racial bias."[576] Further, racial profiling may occur when "race is used in conjunction with other factors."[577]

• • • • • • • • • • •

572 See e.g., "Other studies cited by the authors, albeit in the context of automation bias, indicate that even explicit briefings about risk factors in HCI [human-computer interaction] do not mitigate the strength of automation bias, and this seems to be true in both multitasking and singletasking environments. An idle mind is not an empty mind, but rather a wandering mind, and when the stakes are high, the risk of complacency is still too great to be managed by rubber-stamp training interventions that make only a questionable difference to deep-seated psychological propensities." John Zerilli, Alistair Knott, James Maclaurin & Colin Gavaghan, "Algorithmic Decision-Making and the Control Problem" (2019) 29 Minds and Machines 555 at 575.

573 Patricia Conor, "Police resources in Canada, 2017", *Statistics Canada* (28 March 2018) <https://www150.statcan.gc.ca/n1/pub/85-002-x/2018001/article/54912-eng.htm>.

574 *R v Chehil*, 2013 SCC 49 at para 43.

575 See Section 5.4.4 ("Inequality by Design and 'Mathwashing' Injustice").

576 *R v Neyazi*, 2014 ONSC 6838 at para 195.

577 *Ibid.*

The historic context and present-day reality of race relations and racial profiling in Canada creates possibly insurmountable constitutional hurdles to law enforcement authorities' reliance on either police-generated data sets or systematically biased data sets of any kind to generate algorithmically derived predictions that are used to justify a deprivation of liberty. The Supreme Court of Canada has unanimously taken judicial notice[578] of the accuracy of a significant body of research that has established that disproportionate policing of racialized and low-income communities occurs.[579] Further, courts have also taken judicial notice that "racial minorities are both treated differently by the police and that such differential treatment does not go unnoticed by them."[580] The majority in *R. v. Le* held that "on a go-forward basis, these reports will clearly form part of the social context when determining whether there has been an arbitrary detention contrary to the *Charter*."[581]

Such findings support the fundamental need to place limits on the use of police-generated data sets to predict whether a presumed-innocent individual has committed or is likely to engage in a criminal offense and to justify detentions. This need is even greater in the context of systemic racism. Police services that seek to use algorithmic policing technologies that depend on underlying police data will thus face challenges in demonstrating the reliability and lack of bias in such systems as well as demonstrating that generalized suspicion does not play a role in subsequent decisions to detain or arrest someone.[582] Notoriously unreliable information cannot reasonably serve to justify an interference with liberty through a detention or arrest.[583]

Being subjected to heightened police scrutiny and additional stops and detentions as a result of algorithmic policing technologies can compound racialized individuals' pre-existing negative experiences.[584] Violations of the right to be free from arbitrary detention are often significant and humiliating experiences that strike at the core of individual dignity. These violations can unfold in a matter of seconds or minutes, and they can take a toll on a person's physical and mental health, impact the individual's ability to pursue employment and education opportunities, contribute to the continuing socio-political exclusion of racial minorities, cause a loss of trust in the fairness of the Canadian criminal justice system, and perpetuate the wrongful and disproportionate criminalization of individuals who often have not committed any unlawful activities.[585]

578 R v Le, 2019 SCC 3, at para 260.

579 *Ibid* at para 97.

580 *Ibid* at para 90.

581 *Ibid* at para 96.

582 For example, Lum and Isaac demonstrated that PredPol's algorithm would result in biased and disproportionate policing of racialized individuals for drug offences, despite similar rates of drug use between racialized and white individuals, due to bias in police-recorded data. Kristian Lum & William Isaac, "To predict and serve?" (2016) 13:5 Significance 14.

583 *R v Nuttall*, 2018 BCCA 479, at para 244; *R v Bernshaw*, [1995] 1 SCR 254.

584 *R v Le*, 2019 SCC 34, at para 95.

585 *Ibid*.

### 5.5.3. Concluding Comments: Algorithmic Policing and the Right to Liberty and to Be Free from Arbitrary Detention

To comply with human rights and constitutional standards, law enforcement agencies that rely on algorithmic policing technologies cannot use them to justify interferences with liberty (e.g., arrests or detentions). By definition, algorithmic predictive policing is based on generalized statistical inferences. Canadian law requires an officer to have reasonable suspicion that a specific individual is implicated in criminal activity to justify their detention or arrest. The suspicion must be linked to the given person's specific characteristics and behaviour. Further, suspicion is not reasonable if it is based on immutable characteristics such as race. Law enforcement actors that adopt algorithmic policing technologies must ensure that such methods do not, in practice, expand the scope of what is considered "reasonable" suspicion, particularly in the case of racialized or other marginalized communities that are already subjected to unreasonable suspicion in the form of unconscious bias and racial profiling in the criminal justice system.

## 5.6. Right to Due Process

The right to due process is a foundational principle in the criminal justice system and is enshrined in international human rights law and in the *Charter*. Article 14 of the ICCPR protects specific due process rights, such as the right to be presumed innocent until proven guilty in a fair hearing by an impartial arbiter in a court of law.[586] Section 7 of the *Charter* guarantees that all individuals have the right to life, liberty, and security of the person, which cannot be limited "except in accordance with the principles of fundamental justice".[587] The principles of fundamental justice are the foundational, organizing principles and values that form the bedrock of how the justice system must operate.[588] One specific principle of fundamental justice under section 7, for example, is the right to make full answer and defence to a criminal charge. The protection for due process rights in section 7 is reinforced by other rights in the *Charter* that relate to *habeas corpus* (a determination of whether an arrest or detention was lawful), the right to reasonable bail, the right to be free from arbitrary detention and arrest, and the right to a fair trial.[589]

The use of algorithmic policing technology by law enforcement authorities raises several constitutional and human rights issues under the right to due process, which the following subsections of this report will analyze. Section 5.6.1 discusses the concept of algorithmic transparency and the connection between access to information and the ability for an individual to exercise their due process rights. Due process rights are engaged where individuals who are affected by algorithmic policing

586 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966 <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>, art 14.

587 *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11, s 7.

588 *Canada (Attorney General) v. Bedford*, 2013 SCC 72, at para. 94-96.

589 *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11, ss 9, 10(c), and 11(e).

technology are not able to obtain necessary information to evaluate the technology's reliability, so they can determine whether their rights have been infringed or not by its use. Section 5.6.1 also presents concerns regarding the influence of private sector vendors over access to information and due process rights.

Section 5.6.2 examines how algorithmic policing technologies may impact the right to make full answer and defence, including the role of disclosure (i.e., law enforcement disclosing that such technology was used in an individual's case, and related details). Where full disclosure of relevant information about an algorithmic policing technology is not possible, the use of that technology by law enforcement in a manner that affects an individual's liberty or other *Charter*-protected rights is incompatible with the right to due process.

## 5.6.1. Informational Barriers to Due Process: Algorithmic Transparency and Private Sector Influence

Law enforcement agencies' use of algorithmic policing technology engages due process concerns where there are barriers to the disclosure of information about the technology. Information asymmetry between law enforcement authorities who use algorithmic policing technologies and the individuals and communities who are disproportionately and negatively impacted by them raises the issue of algorithmic transparency. The concept of algorithmic transparency is part of a broader framework of principles that are generally referred to as algorithmic fairness, accountability, transparency, and ethics (FATE).[590] While it has become widely recognized that algorithmic transparency, alone, does not necessarily amount to algorithmic accountability without further action,[591] transparency is frequently a precondition to achieving accountability, and the absence of transparency warrants particular attention.

Providing transparency with algorithmic policing technologies may be challenging, if not impossible, due to the nature of the technology itself. Machine-learning methods "vary considerably in the level of transparency they are able to provide," as some "forms of machine learning provide far less information in terms of how the model computes an outcome."[592] In some cases, even the developer

590 These broad principles have been established and advanced through a significant body of literature, advocacy, government and industry initiatives, and two major annual conferences. See e.g., "Fairness, Accountability, and Transparency in Machine Learning", <https://www.fatml.org>; European Parliamentary, European Parliamentary Research Service, "A governance framework for algorithmic accountability and transparency", (April 2019) <https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624262/EPRS_STU(2019)624262_EN.pdf>; Robert H Sloan & Richard Warner, "When Is an Algorithm Transparent? Predictive Analytics, Privacy, and Public Policy", (May/June 2018) 16:3 IEEE Security & Privacy 18 <https://ieeexplore.ieee.org/document/8395116>.

591 See e.g., Maayan Perel & Niva Elkin-Koren, "Black Box Tinkering: Beyond Disclosure in Algorithmic Enforcement" (2017) 69:1 Florida Law Review 181; and Janelle Berscheld & Francois Roewer-Despres, "Beyond Transparency: A Proposed Framework for Accountability in Decision-Making AI Systems" (2019) 5:2 AI Matters 13.

592 Alexander Babuta, Marion Oswald and Christine Rinik, "Machine Learning Algorithms and Police Decision-Making Legal, Ethical and Regulatory Challenges" (September 2018) RUSI Whitehall Report 3-18, <https://rusi.org/sites/default/files/201809_whr_3-18_machine_learning_algorithms.pdf.pdf>. See also, UN General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/73/348 (29 Aug 2018) <https://undocs.org/A/73/348> at para 40; "Can we open the black box of AI?", https://www.nature.com/news/can-we-open-the-black-box-of-ai-1.20731. The black box problem includes, for example, not being able to tell or explain what factors an algorithm relied on to make a decision, or not knowing how much or how little weight the algorithm assigned to different

of an algorithmic technology may not be able to explain how the algorithm arrived at the decision it generated. For example, in discussing the Vancouver Police Department's (VPD) GeoDASH algorithmic forecasting system, S/Constable Ryan Prox shared that VPD officers run their "algorithm in its machine-learning retraining mode at 3-week intervals; every 3-week interval it rewrites its algorithmic code. That's why we do the independent audits. Because I can't tell you what factors it's weighting according to making the determinations for the boxes. I can tell you if it's doing it accurately, based on where the incidents are taking place, but I can't tell you the 'why', and what weighting it's putting on what factors."[593]

The increasing partnership between private businesses and law enforcement presents specific challenges regarding transparency and due process rights. Private companies often resist, or refuse to provide, full and meaningful disclosure about their algorithmic policing tools, including information about the underlying algorithmic models, variables, data sets used, and testing that speaks to the tool's level of reliability and accuracy. At the same time, police technology vendors contribute to reduced transparency in the initial procurement process through lobbying government agencies behind the scenes to purchase, adopt, or promote their products.[594] Trade secrets and other intellectual property laws also pose substantial barriers to the FATE principles in algorithmic decision making.[595] For example, when the VPD first implemented the GeoDASH APS, it was presented to the VPD's oversight board *in camera* to protect the private commercial interests involved.[596] Concerns about proprietary software contributed to the SPPAL's decision to develop their algorithmic policing technology in-house:

> Not speaking for all the partners, but initially when we started out, because we were concerned about the black-box nature of proprietary software. With consultation with the university and our sense we

---

factors in its determination. A growing field has emerged that attempts to "solve" the black box problem by developing "explainable AI" (XAI); however, it remains to be seen to what extent this line of inquiry delivers on such a promise. See e.g., Amina Adadi & Mohammed Berrada, "Peeking Inside the Black-Box: A Survey on Explainable Artificial Intelligence (XAI)", (2018) IEEE Access <https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8466590>; AJ Abdallat, "Explainable AI: Why We Need To Open The Black Box", *Forbes* (22 February 2019) <https://www.forbes.com/sites/forbestechcouncil/2019/02/22/explainable-ai-why-we-need-to-open-the-black-box/#75d712771717>; however, see, e.g., Cassie Kozyrkov,."Explainable AI won't deliver. Here's why.", *Hackernoon* (16 September 2018) <https://hackernoon.com/explainable-ai-wont-deliver-here-s-why-6738f54216be>.

593 Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019).

594 For example, a lobbyist hired by Shotspotter, the vendor of an algorithmic gunshot detection system, has been registered with the City of Toronto since 2013 and had multiple communications with two city councillors and Mayor John Tory and their staff between 2013 and 2016. Subsequently, Shotspotter CEO Ralph Clark and three other senior executives registered as lobbyists just a few days following Mayor Tory's motion to the Toronto Police Services Board for funding to licence Shotspotter software in Toronto. City of Toronto, <http://app.toronto.ca/lobbyistsearch/searchInput.do> (available by searching with keyword "ShotSpotter", accessed 1 October 2019); "Could a Controversial Gun Surveillance System Help Tackle Toronto Crime?", *The Globe and Mail*, <https://www.theglobeandmail.com/news/toronto/technology-offers-police-more-than-a-shot-in-the-dark/article30773005/>; and Jessica Patton, What is 'ShotSpotter'? Controversial gunshot detector technology approved by Toronto police", *Global News* (20 July 2018). In Massachusetts, a facial recognition company called Suspect Technologies offered to provide its product to the local police department for free, in exchange for the department's support on a government grant application. Joseph Cox, "'They Would Go Absolutely Nuts': How a Mark Cuban-Backed Facial Recognition Firm Tried to Work With Cops", *VICE Motherboard* (6 May 2019) <https://www.vice.com/en_ca/article/xwny7d/mark-cuban-facial-recognition-suspect-technologies>.

595 However, see Andrew Selbst's explanation that trade secrets may not always necessarily hinder algorithmic transparency in the context of algorithmic impact assessments; but where they do, "there is no reason, as a matter of policy, why trade secrets should have preferential status over something as important as fairness in criminal justice." Andrew D. Selbst, "Disparate Impact in Big Data Policing" (2017) 52 Georgia Law Review 109 at 190. See also

596 *Ibid*.

> could develop something in a more transparent and maybe even more cutting-edge way, we opted against it. That's currently where we're at, especially for this project. That's not to say in the future certain things couldn't be considered. But, as of now, it was a conscious effort to do this in-house, so we could be as transparent as possible, and so we could review and defend it.[597]

Litigation in the United States regarding the COMPAS risk assessment technology serves as a cautionary example of how due process principles have not always been guarded or prioritized from the earliest stages of potential procurement or use. In *State v. Loomis*, the State of Wisconsin did not provide disclosure about how the COMPAS risk assessment tool had been used in the defendant's case,[598] including information about "how the risk scores [were] determined, or how the factors [were] weighed."[599] Disclosure was not provided because the COMPAS vendor, Northpointe, Inc. (now Equivant) asserted proprietary claims.[600] The Wisconsin Supreme Court held that using an algorithmic risk assessment in criminal sentencing did not violate the defendant's right to due process despite this lack of disclosure[601] and despite acknowledging that studies testing COMPAS predictions "raise concerns regarding how a COMPAS assessment's risk factors correlate with race."[602] One study showed that "[B]lack defendants 'were far more likely than white defendants to be incorrectly judged to be at a higher risk of recidivism'... [while] white defendants were more likely than [B]lack defendants to be incorrectly flagged as low risk."[603]

Even if Canada were to establish laws that required disclosure from vendors, trade agreements may block the ability to apply conditions at the procurement or importation stage.[604] Exceptions apply only in the context of specific investigations and cases and, even then, they remain "subject to safeguards against unauthorized disclosure."[605] This situation means that where an algorithmic policing technology is based in the United States or Mexico, the Canadian government may be barred from requiring full algorithmic transparency at the procurement stage. Rather, the technology's underlying algorithms could not be examined until harm had occurred and an actual proceeding was underway—perhaps not even then and, almost certainly, not without encountering further obstacles in obtaining

597 Interview of a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) by Cynthia Khoo (23 July 2019).

598 The Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) is a risk-assessment tool designed to provide "decisional support" for the Department of Corrections when making placement decisions, managing offenders, and planning treatment.

599 *State v Loomis*, 881 NW 2d 749 (Wis 2016) at para 51.

600 *State v Loomis*, 881 NW 2d 749 (Wis 2016) at para 51.

601 *State v Loomis*, 881 NW 2d 749 (Wis 2016).

602 *State v Loomis*, 881 NW 2d 749 (Wis 2016).

603 *State v Loomis*, 881 NW 2d 749 (Wis 2016) at para 63.

604 Article 19.16.1 of the Canada-United States-Mexico Agreement (CUSMA) bars member countries from being able to require "access to" software source code or software algorithms based in the other countries as a condition of "import, distribution, sale or use" of that software in the country. *Canada-United States-Mexico Agreement*, 30 November 2018 (ratified 13 March 2020), Art 19.16, para 1, <https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19-Digital-Trade.pdf>.

605 Article 19.16.2 provides that a regulatory body or judicial authority may require the owner to "preserve and make available the source code of software, or an algorithm expressed in that source code, to the regulatory body for a specific investigation, inspection, examination, enforcement action, or judicial proceeding." *Canada-United States-Mexico Agreement*, 30 November 2018 (ratified 13 March 2020), Art 19.16, para 2.

the required information. These considerations must be taken into account in the regulation and potential implementation of algorithmic policing, such as by prohibiting the procurement of commercial off-the-shelf algorithmic policing technologies from vendors based in the United States or Mexico or from any vendors who are unwilling or unable to meet a level of transparency required to protect constitutional and human rights in their use in Canada.

When considering whether to procure or use an algorithmic policing technology, Canadian governments, lawmakers, and criminal justice actors must be vigilant in prioritizing the due process rights of individuals who are subjected to the criminal justice system. As the federal Department of Justice recognizes, "it may be assumed that if [procedural protections] apply outside the criminal context, they apply with greater force in the criminal context."[606] Public interest legal standards must apply to commercial vendors that enter into contracts with government or law enforcement for algorithmic policing tools whenever criminal jeopardy is at stake. It is not justifiable to prioritize proprietary interests or profit at the expense of individuals' human and constitutional rights, such as the right not to be deprived of liberty except in accordance with the principles of fundamental justice.[607]

# Open Source Algorithms and Source Code Review

As a matter of public accountability and public funding, government and law enforcement agencies that develop algorithmic policing technologies—whether in-house or in partnership with private vendors—should make the source code and related details of such technologies publicly available in machine-readable and human-readable forms. Doing so would serve to make the right to due process and right to a remedy meaningful. Making the source code of an algorithmic policing technology publicly available would also support informed public participation in meaningful democratic dialogue regarding whether to adopt a particular technology for law enforcement purposes. One potential mechanism through which open-source code policies could be accomplished is to apply open-source software licensing, such as the GNU General Public License (GPL), to the software behind algorithmic policing technologies.[608] Open software licensing would be appropriate in cases where technologies are publicly funded and, thus, should be available to members of the public for purposes of review or research.

There may be some kinds of algorithmic policing technologies for which it would be contrary to the public interest to release the source code to the public or make it open source. Where that circumstance can be demonstrated, the source code and related details must still be made available to the relevant public bodies and independent experts, on a confidential basis. This availability is necessary for the purposes of conducting algorithmic impact assessments, preprocurement reviews, and tests for security vulnerabilities. Similarly, where any such technology has been developed or adopted and put into use, the source code must be made confidentially available for auditing, investigations, and judicial proceedings. The broad rationale for such confidentiality should be made public and confirmed by oversight groups, such as the relevant information or privacy commissioner. The agencies and individuals who are granted access to the source code for review and auditing purposes may be bound to confidentiality with respect to the contents of the source code itself, but they should not be bound to confidentiality with respect to their *findings* based on the source code.

Government and law enforcement agencies that acquire off-the-shelf algorithmic policing technologies but are not involved in the development of any of the acquired technologies should include as a condition of all procurement contracts that vendors waive trade secrets and related proprietary rights. These rights should be waived for all released versions of proprietary software components to the extent that allows for access to and testing of the algorithmic technology by public bodies and independent experts. Such waivure includes waiving proprietary rights for the relevant government or law enforcement agency, which will allow them to conduct independent audits, investigations, inspections, examinations, enforcement actions, or judicial proceedings. This process would also be subject to safeguards against unauthorized disclosure should non-disclosure to the public be found to override public interest considerations.

608 "GNU General Public License", GNU Operating System (18 November 2016) <https://www.gnu.org/licenses/gpl-3.0.en.html>; and "About The Licenses", Creative Commons <https://creativecommons.org/licenses/>.

Putting this recommendation into practice could, as an example, involve the Office of the Privacy Commissioner, the Canadian Centre for Cyber Security, or federal research agencies as the public bodies responsible for reviewing algorithmic policing technology as a part of the procurement process. They, in turn, could retain independent experts to assist in review and auditing.

## 5.6.2. Non-Disclosure and the Right to Make Full Answer and Defence

The right to make full answer and defence to a criminal charge—a component of due process protection—is one of the principles of fundamental justice under section 7 of the *Charter*.[609] This principle imposes a duty on the prosecuting Crown to disclose all relevant information in its possession or control to defendants in criminal proceedings.[610] Without full disclosure of such information or if full disclosure is not possible, the use of algorithmic policing technology that leads to interference with an individual's liberty risks wrongful convictions in the criminal justice system and would contravene the right to due process.

Whether the non-disclosure of information about an algorithmic policing technology violates due process rights is a context-specific determination. The scope of due process rights is informed by the nature of the individual's jeopardy (i.e., what type of *Charter*-protected interests have been affected or are at stake); what potential defences or *Charter* claims may be in play; and whether law enforcement's use of an algorithmic policing technology is relevant to the issues in dispute (i.e., whether a *Charter* or human right has been violated or can be justifiably restricted).

Delineating an individual's right to due process and to make full answer and defence with regard to the use of specific technologies will entail highly contextual inquiries. To illustrate the tensions that inform whether the use of algorithmic policing technology is compliant with due process rights, this subsection focuses on one of the main sources of due process protection: the right to make full answer and defence where the state seeks to limit an individual's liberty in criminal proceedings.

When it comes to algorithmic policing technology, any assessment of the right to disclosure necessarily implicates the principle of algorithmic transparency. In the context of a criminal case, algorithmic transparency requires determining what type of information must be disclosed to protect the right to make full answer and defence of an individual who has been affected by an algorithmic policing technology. The Crown should be required to disclose the following types of information, so the defendant can assess a technology's reliability as well as any applicable *Charter* issues and defences surrounding the tool's use:

- How the tool and its underlying algorithmic models work (if the developers cannot say how the tool or its algorithms work, they must indicate that explicitly);
- What data sets the algorithms were trained on;

609 The right to make full answer and defence is a companion to the right to a fair trial, which is itself also guaranteed under section 11(d) of the *Charter*.

610 The Crown must disclose all information in the possession of the prosecuting Crown (except to the extent that it is clearly irrelevant, privileged, or its disclosure is otherwise governed by law), as well as the fruits of the investigation in the possession of the police: *R v Stinchcombe*, [1991] 3 SCR 326; *R v McNeil*, [2009] 1 SCR 66. Relevant information includes information that speaks to the merits of the allegations; exculpatory information or information that may assist the defence in its own investigation or preparation for trial; and information relevant to *Charter* issues or remedies arising in the case: *R v Stinchcombe*, [1991] 3 SCR 326; *R v Jackson*, 2015 ONCA 832.

- How the algorithm weighs different factors (if the developers cannot identify how the algorithm weighs different factors, they must say so explicitly);
- What input data was used;
- Information about the relationship and any contracts, memoranda of understanding, or agreements between law enforcement and third-party private sector actors who were involved in data collection or data analytics that law enforcement relied on prior to the criminal charge;
- Information about the relationship and any contracts, memoranda of understanding, or agreements between law enforcement and third-party vendors of algorithmic policing tools that law enforcement purchased off-the-shelf or developed in collaboration with the private vendor; and
- Information about the testing and maintenance methods and practices used by the developer, including all available information regarding the reliability or accuracy rate of predictions or decisions generated by the tool in testing and/or prior in use cases (e.g., accuracy rate of recidivism prediction tools, accuracy rate of facial recognition tools).

As outlined in Section 5.6.1 ("Informational Barriers to Due Process: Algorithmic Transparency and Private Sector Influence"), barriers to the disclosure of information may arise depending on the nature of the technology or the existence of proprietary claims by private vendors. Where full disclosure of all relevant information is impossible (e.g., due to a third-party vendor's assertion of a proprietary claim, or the developer's inability to identify, on a technical level and in plain language, how an algorithm works or how it weighs various factors), law enforcements' use of that technology in a manner that affects an individual's liberty or other *Charter*-protected interests is incompatible with the right to make full answer and defence.

A key feature of due process rights relates to the overarching *Charter* principle that if the state interferes with an individual's liberty, it can only do so in a reasonable manner.[611] If an algorithmic tool is relied upon to form grounds for a deprivation of liberty and is unreliable or biased, it cannot reasonably serve as a justification for the deprivation of liberty or other affected rights. The Crown bears the burden to demonstrate whether limits on liberty are reasonably justified. As a result, for the Crown to meaningfully meet its burden, and for defendants, defence counsel, courts, and the public to be able to scrutinize the reliability and use of algorithmic policing technology by law enforcement, access to meaningful disclosure is a critical due process safeguard. When the Crown seeks to introduce evidence that was obtained through an algorithmic policing technology, access to disclosure must be provided.

611 The right to liberty protected by section 7 is reinforced by a range of protections that ensure that all deprivations of liberty must be reasonably justified. These protections appear at the various stages of the criminal process from an individual's first encounter with police until the imposition and completion of sentence if found guilty. For example, after the front-line policing stage, section 11(e) guarantees that all persons charged with an offence have the right not to be denied reasonable bail without just cause, and the presumption of innocence protected by section 11(d) of the Charter means that an individual cannot be imprisoned for a crime unless the Crown establishes guilt beyond any reasonable doubt in a fair trial. *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11, ss 9, 11(d), and 11(e).

In these situations, lack of disclosure would likely impair the Crown's ability to satisfy its burden of showing that any limits on individual liberty were or would be reasonably justified. The failure to meet this burden would infringe the defendant's right to make full answer and defence by depriving that individual and their counsel of relevant information regarding whether any deprivation of liberty is justified.

Any violation of the right to make full answer and defence, where algorithmic policing technology has been used, has significant consequences for those who have been targeted by the technology and for public trust in the administration of justice. Algorithmic policing technology is an ongoing, evolving field, and the reliability of these technologies across the board is not a matter of fact or scientific consensus.[612] In fact, the Chicago Police Department ended its Strategic Subject List (SSL) in January 2020, after the city's Office of Inspector General released an advisory questioning its reliability,[613] and the Los Angeles Police Department ended its L.A. Strategic Extraction and Restoration (LASER) Program in March 2019,[614] after its Inspector General completed an audit that found "a lack of clear, reliable data that could be used to measure both the inputs and outcomes" of the program.[615] Questions about the reliability of such technologies are material, particularly in light of problems that have been raised by academics, disproportionately impacted communities, and human rights researchers. Concerns about the appropriateness of data sets used include questions about the source of the data, the age of the data, the sample size of the data, the demographics of those reflected in the data, and the accuracy of the data sets themselves.[616] Concerns also surround the potential presence of systemic biases in data sets that are subsequently used to train or as input data for the algorithmic policing technology in question.[617]

612 For example, a 2019 review of the existing literature identified only four empirical studies of predictive policing methods and concluded that "the current thrust of predictive policing initiatives is based on convincing arguments and anecdotal evidence rather than on systematic empirical research." Further, the authors identified that the empirical literature was focused on evaluating the benefits of algorithmic policing and neglected to measure for adverse effects. Albert Meijer & Martijn Wessels, "Predictive Policing: Review of Benefits and Drawbacks" (2019) 42:12 *International Journal of Public Administration*, 1031-1039 at 1037 <https://www.tandfonline.com/doi/full/10.1080/01900692.2019.1575664>.

613 Jeremy Gorner & Annie Sweeney, "For years Chicago police rated the risk of tens of thousands being caught up in violence. That controversial effort has quietly been ended", *Chicago Tribune* (24 January 2020), <https://www.chicagotribune.com/news/criminal-justice/ct-chicago-police-strategic-subject-list-ended-20200125-spn4kjmrxrh4tmktdjckhtox4i-story.html>; and "Advisory Concerning the Chicago Police Department's Predictive Risk Models", City of Chicago Office of Inspector General (23 January 2020) <https://igchicago.org/wp-content/uploads/2020/01/OIG-Advisory-Concerning-CPDs-Predictive-Risk-Models-.pdf>.

614 Mark Puente, "LAPD to scrap some crime data programs after criticism", *Los Angeles Times* (5 April 2019) <https://www.latimes.com/local/lanow/la-me-lapd-predictive-policing-big-data-20190405-story.html>.

615 Mark P Smith, "Review of Selected Los Angeles Police Department Data-Driven Policing Strategies", Office of the Inspector General, Los Angeles Police Commission (12 March 2019), at 23. <https://a27e0481-a3d0-44b8-8142-1376cfbb6e32.filesusr.com/ugd/b2dd23_21f6fe20f1b84c179abf440d4c049219.pdf>. The report also raised concerns about the LAPD's use of PredPol, including discrepancies in data collection which "made it difficult to draw conclusions about the effectiveness of the system in reducing vehicle or other crime". *Ibid*, at 29.

616 Logan Koepke & David Robinson, "Danger Ahead: Risk Assessment and the Future of Bail Reform" (2019) 93 Washington Law Review 1725; *Innocence at Stake: The Need for Continued Vigilance to Prevent Wrongful Convictions in Canada* (2018) <https://www.ppsc-sppc.gc.ca/eng/pub/is-ip/is-ip-eng.pdf>, at p 169-172 (recognizing the phenomenon of false guilty pleas in criminal courts, which will taint criminal record data).

617 Danielle Groen, "How We Made AI As Racist and Sexist As Humans", *The Walrus* (4 October 2019) <https://thewalrus.ca/how-we-made-ai-as-racist-and-sexist-as-humans/>.

Analogizing algorithmic policing technologies to the use of expert opinions in the criminal justice system may provide a framework and guiding questions for courts to refer to in assessing the reliability of such technologies. With expert evidence, courts exercise a critical gatekeeper function, ensuring that the admitted evidence is sufficiently reliable, will not usurp the judge or jury, and will not risk undue bias towards the expert. Given the risks of wrongful convictions associated with the presentation of expert evidence, in addition to other issues that may impact procedural fairness in a criminal law proceeding, a large body of law has emerged to govern the use of such evidence.[618] The relevant law recognizes that expert evidence must be qualified (i.e., the expert must be deemed to have the appropriate expertise to provide their opinion to the court on the matter at hand) and evaluated accordingly to determine its admissibility in criminal proceedings.

In many respects, relying on algorithmic policing technologies in criminal proceedings is akin to relying on a form of unqualified expert evidence. Access to meaningful and full disclosure about the technology is critical for the court to be able to exercise its gatekeeper role over the use of expert evidence. Like experts who may usurp the judge's role or garner undue weight to their testimony in the eyes of the court, algorithmic policing tools can be given undue weight given the significant risks of automation bias[619] that are associated with algorithmic technology.[620] To mitigate such bias, there should be full disclosure regarding how different tools function and to reveal hidden reliability problems within a particular algorithmic technology. Such disclosures are also required to avoid leaving justice system participants with a false sense of security about the ability or appropriateness of deferring to such technology in making decisions that impact the civil liberties and constitutional rights of individuals.

Furthermore, the individuals who actually create the algorithmic policing technology may constitute potentially unqualified experts. Chan and Bennett Moses have described how the rise of big data has led some enthusiasts to embrace correlation over causation, foreshadowing "an emerging 'jurisdictional conflict' between social scientists and Big Data analysts,"[621] including in criminology. Kelly Hannah-Moffat has examined the shift in criminal risk assessment tools from "psychology informed risk" to "big data informed risk"[622] and further observed that "new players or experts are entering the risk game:

618 Commissions of inquiry have time and again emphasized the importance of due process protections in the aftermath of high-profile wrongful convictions. It is where these protections break down that defendants are at greater risk of a wrongful conviction: "Thomas Sophonow Inquiry Report", <https://digitalcollection.gov.mb.ca/awweb/pdfopener?smd=1&did=12713&md=1>; *Truscott (Re)*, 2007 ONCA 575.

619 Hannah Couchman, "Policing by Machine: Predictive policing and the threat to our rights," (January 2019) *Liberty*, at 34 <https://www.libertyhumanrights.org.uk/sites/default/files/LIB%2011%20Predictive%20Policing%20Report%20WEB.pdf>.

620 Automation bias is discussed in Section 5.5.1 ("Algorithmic Policing and Generalized Suspicion"), and is defined as the human tendency to "to rely on the judgments of automated decisions as superior to their own, even when they have reason to believe the technology is flawed." Lindsey Barrett, "Reasonably Suspicious Algorithms: Predictive Policing at the United States Border", (2017) 41 *NYU Review of Law & Social Change* 327 <https://socialchangenyu.com/wp-content/uploads/2017/09/barrett_digital_9-6-17.pdf> at 342-43. See also Danielle Keats Citron, "Technological Due Process" (2008) 85:6 Washington Law Review 1249 at 1271-1272, <https://openscholarship.wustl.edu/cgi/viewcontent.cgi?article=1166&context=law_lawreview>.

621 Janet Chan & Lydia Bennett Moses, "Is Big Data challenging criminology?" (2016) 20:1 Theoretical Criminology 21 at 23.

622 The former is developed through purpose-specific design, established social science methodologies, and disciplinary expertise and standards while the latter involves "methodological uncertainties" and "data that are assembled and disassembled for a range of purposes and is developed without being linked to a specific discipline." Kelly Hannah-Moffat, "Algorithmic risk governance: Big data analytics, race and information activism in criminal justice debates" (2018) 23:4 Theoretical Criminology 453 at 458.

technologists (e.g., concerned citizens, computer scientists, software engineers and hackers—usually not trained in social science) who make data public and accessible to a range of stakeholders."[623]

The involvement of technology companies and developers from outside criminology, criminal law, and the criminal justice system raises long-standing concerns regarding the impact of technocentric or techno-solutionist views on criminal justice.[624] Increasingly, policing systems and methods and law enforcement decision making are being advanced through the technology sector, data sciences industry, and private enterprise, which are not necessarily equipped with domain expertise or driven by the same values that underlie criminal justice objectives. Such fields and their actors may also not be subject to or trained in the necessary professional regulations, ethical standards, or analytical demands associated with criminological research or public policy expertise in the area of policing and criminal justice.[625] Lack of expertise is likely to be a greater issue where law enforcement agencies purchase off-the-shelf products or services from private companies, as opposed to, for example, how the VPD developed their GeoDASH algorithmic prediction system in collaboration with university academics and a private vendor.[626] Similarly, the SPPAL's predictive policing projects are conducted according to protocols established with the University of Saskatchewan Research Ethics Board.[627]

Including independent and credible academic and domain experts in the development of algorithmic policing technologies is a critical first step to increasing the chances of the technology being reliable. However, the direct involvement of such experts with criminological, legal, or public policy expertise in criminal justice is a necessary, but by no means sufficient, condition to justify deference towards an

623 *Ibid,* at 456.

624 See e.g., "This trend [toward automated decision-making] is a part of 'algorithmic governmentality' (Rouvroy and Berns, 2013) and the increased influence of mathematics on all spheres of our lives (O'Neil, 2016). It is a part of 'solutionism', whereby tech companies offer technical solutions to all social problems, including crime (Morozov, 2013)." Aleš Završnik, "Algorithmic justice: Algorithms and big data in criminal justice settings" (2019) European Journal of Criminology 1 at 2. See generally Evgeny Morozov, *To Save Everything, Click Here: The Folly of Technological Solutionism* (New York: PublicAffairs, 2013) and Meredith Broussard, *Artificial Unintelligence: How Computers Misunderstand the World* (Cambridge, MA: MIT Press, 2018).

625 One particularly troubling result of engaging in technological development separate from ethical considerations and historical and socio-political context, including in the area of criminal justice, is individuals attempting to develop algorithmic technologies that purport to predict sensitive personal information about an individual based on their facial features alone, such as whether they are a criminal offender, or what their sexual orientation is—potentially "reviving an old belief with a bad history: that you can intuit character from appearance. This pseudoscience, physiognomy, was fuel for the scientific racism of the 19th and 20th centuries, and gave moral cover to some of humanity's worst impulses". James Vincent, "The invention of AI 'gaydar' could be the start of something much worse", *The Verge* (21 September 2017) <https://www.theverge.com/2017/9/21/16332760/ai-sexuality-gaydar-photo-physiognomy>; see also Sahil Chinoy, "The Racist History Behind Facial Recognition", *New York Times* (10 July 2019) <https://www.nytimes.com/2019/07/10/opinion/facial-recognition-race.html> ("The technological frontiers being explored by questionable researchers and unscrupulous start-ups recall the discredited pseudosciences of physiognomy and phrenology, which purport to use facial structure and head shape to assess character and mental capacity.") As an example of one such concerning technological endeavour, see Parabon NanoLabs: "Algorithmic DNA Sketches", <https://parabon-nanolabs.com/>; Emerging Technology from the arXiv, "Neural Network Learns to Identify Criminals by Their Faces", *Technology Review* (22 November 2016) <https://www.technologyreview.com/s/602955/neural-network-learns-to-identify-criminals-by-their-faces/>.

626 According to Prox, the private vendor met needs for technology that was "industry acceptable and standardized", but also noted, "It got a lot more complicated when we got the private sector involved," compared to the initial partnership between the VPD and academics alone. Interview of Ryan Prox by Cynthia Khoo & Yolanda Song (7 May 2019).

627 Interview of a representative for the Saskatchewan Police Predictive Analytics Lab (SPPAL) by Cynthia Khoo (23 July 2019). The representative also stated, "We like to validate [the SPPAL's algorithmic models] on other samples or have other people take a look, see how they [the models] perform, use other methods, see if they approve or not. You want to make sure what you're finding is robust but also open to scrutiny".

algorithmic policing technology. These individuals may themselves unintentionally convey unconscious bias through their work, or they may fail to identify others' unconscious biases or other flaws. Also, their involvement does not eradicate the risk that such technology lacks reliability for reasons outside of their purview or the risk that law enforcement authorities use the technology in a manner that does not comply with human rights law or the *Charter*. As such, even where independent and qualified experts with the appropriate domain knowledge have been involved in developing an algorithmic policing technology, full disclosure of the technology's use and all relevant details must still occur, so defendants in criminal justice proceedings can assess the technology's reliability, including the identification of any unconscious bias or inadvertent discrimination in the technology's development or use leading to a potentially unlawful restriction on liberty.

### 5.6.3. Concluding Comments: Algorithmic Policing and the Right to Due Process

Criminal courts in Canada exercise an essential gatekeeping function, including the assessment of expert evidence, such as scientific, psychiatric, or forensic evidence. Examining this role makes clear that courts must have the ability to obtain meaningful disclosure about algorithmic policing technologies, their functionalities, source code, training, and input data. Ensuring such disclosure provides a necessary constitutional safeguard, where law enforcement relies on algorithmic policing technology in circumstances that restrict or otherwise engage an individual's *Charter*-protected rights, such as the right to liberty.

Further, any law enforcement authorities that are considering the adoption of algorithmic policing technologies should first ensure that the right to due process will not be infringed by the use of such technologies. Questions about the reliability, intelligibility, and auditability of such technologies should be asked—and responses to them obtained—at the outset, prior to any procurement or associated public spending on such tools. Such questions are particularly necessary where the technologies are used in a way that impacts real individuals (i.e., not procured solely for the purpose of internal trial runs or simulations that have no outside impact on the lives and human rights of any individuals or their communities). Where law enforcement has relied on an algorithmic policing technology to justify depriving someone of their liberty, the technology must be reliable and unbiased, among other requirements. Where an algorithmic tool cannot be shown to meet established requirements such as, at minimum, reliability and lack of bias, the tool cannot reasonably serve as justification for the deprivation of liberty in accordance with the principles of fundamental justice or in accordance with other related constitutional due process rights.

# Algorithmic Impact Assessments

Algorithmic accountability experts in the United States have proposed that governments and public agencies use "algorithmic impact assessments" (AIAs) to facilitate transparency, accountability, and human rights compliance when deploying algorithmic technologies.[628] 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,[629] and to challenge the proposed or continued use of a technology where it risks infringing upon constitutional or human rights.[630]

Any established AIA framework for algorithmic policing technologies should include obligations and procedures to facilitate public comment; external scrutiny of proposed and ongoing algorithmic policing systems; internal institutional capacity-building on issues that relate to fairness and disparate impacts; strong due process mechanisms for negatively affected individuals or communities; and identification and fulsome evaluation of all reasonable alternative solutions for the given objective—including the alternative of not pursuing the examined technology at all. Further substantive components should include the requirement for the relevant government agency or law enforcement authority to:[631]

- Disclose to independent experts, to historically over-policed communities, and to the public proposed and existing algorithmic policing technologies, including their purposes, scope, operation, training, and input data details, and relevant internal policies and legal obligations;
- Articulate any net benefits that the technology is expected to provide to communities;
- Articulate potential harmful impacts—including human rights impacts, sociological impacts, and material on-the-ground impacts—of the proposed technologies'

628 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. Selbst refers to "algorithmic impact statements" (AISs) in his paper; for ease of reference, this report uses "algorithmic impact assessments" to refer to both AIAs and AISs.

629 Andrew D Selbst, "Disparate Impact in Big Data Policing" (2017) 52 Georgia Law Review 109 at 178-179.

630 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.

631 In fulfilling the requirements of these components, the AIA may reference or incorporate separate mandatory impact assessment, accountability, and public transparency obligations, where they have been imposed through legislation or binding directives, for example.

use on the public and on likely impacted communities with particular focus on historically over-policed communities;

- Outline mitigation strategies for each of the identified potential harms;
- Outline oversight and redress mechanisms to challenge algorithmic outputs or use; and
- Identify a plan for providing external researchers, auditors, courts, commissioners, or investigative bodies with meaningful, ongoing access to scrutinize the proposed technologies, both before adoption and afterwards where applicable.

Where an algorithmic policing technology has undergone an AIA and been deployed, the AIA should be subject to regular updates and renewal, based on the latest information and research, including information regarding the technology's impact on affected communities.[632] The AIA process should also include procedures for stakeholders to challenge a particular agency if it fails to comply with AIA requirements or any subsequent obligations that result from the AIA.[633]

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 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.[634] To facilitate this process, the Treasury Board provides an online tool titled "Algorithmic Impact Assessment," which is a questionnaire designed to assist federal departments to internally assess and mitigate the risks associated with using algorithmic technologies.[635]

At the outset, it is important to note 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, as demonstrated throughout this report, many algorithmic policing technologies are adopted and implemented on a provincial or municipal level. As enacting a similar Directive for provinces or municipalities is outside the jurisdiction of the Treasury Board, this report recommends that provinces and territories enact their own directives and AIA requirements with robust transparency, accountability, and oversight mechanisms where provincial or municipal public bodies—such as law enforcement agencies and police services—are considering implementing algorithmic decision-making technologies.

632 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 10.

633 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 10.

634 Government of Canada, "Directive on Automated Decision-Making", <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592>.

635 "Algorithmic Impact Assessment" (29 March 2019) Government of Canada <https://open.canada.ca/aia-eia-js/?lang=en>.

Beyond jurisdictional limitations, the Treasury Board's provided impact assessment tool (hereinafter referred to as "the questionnaire") contains serious deficiencies that prevent it from being an effective oversight, transparency, or accountability instrument. The questionnaire is a far cry from what has been set out by researchers, such as Selbst and those at the AI Now Institute as constituting an AIA, and further, it does not match the general understanding of similar kinds of impact assessments, such as privacy impact assessments (PIAs) that are already required in other contexts in Canada.[636] The questionnaire is estimated to take 35 minutes to complete and asks approximately 60 questions,[637] nearly all of which are multiple choice format or answered on a yes/no basis. The questionnaire has no requirement to provide supporting details or documentation to substantiate responses with respect to potential impacts, risk mitigation measures, or explanations about how the proposed program works on both a technical and operational level.[638] Moreover, the Treasury Board questionnaire does not define what constitutes "high" or "low" risks, impacts, or stakes for affected or vulnerable communities. It relies on respondents to self-evaluate or to bring the appropriate expertise to provide answers that would lead to an accurate assessment.

While the Treasury Board questionnaire may provide a helpful preliminary internal assessment tool to test ideas before investing further resources in them, the tool in its current form will not fulfill the function of what has generally been understood to constitute a meaningful AIA, such as that proposed by Selbst and the AI Now Institute. Any AIA adopted in Canada should follow the latter model, which would, appropriately, require more of government agencies or law enforcement authorities who wish to use algorithmic policing technologies on members of the public.

636 A privacy impact assessment (PIA) is "a risk management process that helps institutions ensure they meet legislative requirements and identify the impacts their programs and activities will have on individuals' privacy." Completing a PIA in given circumstances is a legal obligation under various Canadian privacy laws, such as the federal *Privacy Act*, various institutions' enabling legislation, or government policies and directives. "Expectations: OPC's Guide to the Privacy Impact Assessment Process", Office of the Privacy Commissioner of Canada (Marcy 2020) <https://www.priv.gc.ca/en/privacy-topics/privacy-impact-assessments/gd_exp_202003/#toc4-1>.

637 *Ibid*.

638 In contrast, the draft Privacy Impact Assessment that the Calgary Police Service conducted on its adoption of Palantir's products and services in 2014 runs to nearly fifty pages of substantive details and analysis regarding the technology, its implementation, and associated legal and policy issues for privacy and data protection alone. Calgary Police Service, "Calgary Police Service Palantir Implementation Privacy Impact Assessment: June 1, 2014 Draft" at 29-30, (obtained through freedom of information request 18-G-1921). For further context, while distinguishing other forms of impact assessments in the United States, such as "racial impact statements" and surveillance impact reports, Selbst notes, "While there is value in the transparency that these documents provide, these versions of impact statements are not as robust as the proposed AIS [algorithmic impact statement]. They can run a mere handful of pages, whereas regulations were required to limit EISs [environmental impact statements, on which AIAs were based] to 150 pages, except in cases of 'unusual scope or complexity,' which are afforded 300." Andrew D Selbst, "Disparate Impact in Big Data Policing" (2017) 52 Georgia Law Review 109 at 186.

## 5.7. Right to a Remedy

The right to a remedy, as provided for by the ICCPR and by the *Charter*, guarantees that those whose human rights or constitutional rights have been violated are able to obtain meaningful redress for such violations.[639] The ICCPR requires signatory states to ensure that "any person whose rights or freedoms [established in the ICCPR] are violated shall have an effective remedy"; that any claims for a remedy shall be "determined by competent judicial, administrative, or legislative authorities"; and that competent authorities shall enforce any remedies that are granted.[640] The *Charter* provides a similar guarantee in section 24(1): "Anyone whose rights or freedoms, as guaranteed by this charter, have been infringed or denied may apply to a court of competent jurisdiction to obtain such remedy as the court considers appropriate and just in the circumstances."[641] In the criminal justice context, section 24(2) provides the specific remedy that evidence may be excluded from being admissible in some cases if it was obtained in a way that "infringed or denied" any *Charter* rights or freedoms.[642]

Algorithmic policing technologies raise multiple complications for an impacted individual's ability to exercise their right to an effective remedy. The UN Special Rapporteur on the protection and promotion of freedom of expression and the High Commissioner for Human Rights have recognized that algorithmic systems and privacy violations from surveillance, respectively, pose particular challenges in this regard,[643] which will be discussed in the subsections following. Section 5.7.1 analyzes the lack of a requirement in Canadian law to provide notice of general or specific surveillance, including algorithmic surveillance, by law enforcement. It also discusses how this lack of notice impacts the ability to challenge the use of algorithmic policing technology where it has violated a constitutional or human right. Section 5.7.2 discusses what it means for a remedy to be effective and why relying on case litigation to remedy constitutional or human rights infringements by algorithmic policing may be an insufficient safeguard.

639 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966 <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>, art 2.3; *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11, s 24. See also, UN General Assembly, "Resolution adopted by the General Assembly on 16 December 2005: Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of International Humanitarian Law", (21 March 2006) <https://www.ohchr.org/EN/ProfessionalInterest/Pages/RemedyAndReparation.aspx>.

640 UN General Assembly, *International Covenant on Civil and Political Rights*, 16 December 1966 <http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx>, art 2.3.

641 *Canadian Charter of Rights and Freedoms*, s 7, Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act* 1982 (UK), 1982, c 11, s 24(1).

642 *Ibid*, s 24(2).

643 UN General Assembly, R*eport of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/73/348 (29 Aug 2018) <https://undocs.org/A/73/348> para 40; UN Human Rights Council, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at para 54.

### 5.7.1. Notice Requirement and Ability to Challenge Algorithmic Policing

International human rights experts have expressed concern about the lack of notice to individuals whose rights may have been affected by algorithmic processing and about the resulting interference with their right to a remedy.[644] The UN High Commissioner for Human Rights has stated that providing notice of general or specific surveillance measures (usually *ex post facto*, or notice provided after the fact) and ensuring that impacted individuals have legal standing to challenge those measures are "critical issues in determining access to effective remedy".[645]

Currently, Canadian law enforcement agencies are required to provide notice to individuals who have been the subject of electronic surveillance through an interception of private communications.[646] In considering the notice requirement regarding wiretap surveillance, the Supreme Court of Canada affirmed that the "right to privacy implies not just freedom from unreasonable search and seizure, but also the ability to identify and challenge such invasions, and to seek a meaningful remedy. Notice [enhances] all these interests."[647] Notice is thus a vehicle for facilitating meaningful access to remedies for *Charter* and human rights violations that are occasioned by a given law enforcement agency.

Despite this recognition of the importance of notice, domestic privacy laws routinely exempt law enforcement agencies from requirements to provide notice to individuals about data collection activities, outside of the wiretap surveillance context.[648] These exemptions may include data collection from algorithmic policing technologies, and the scope of the legal duty to provide notice to targets of electronic surveillance has not been fully determined because courts have not considered this issue closely yet. As such, a fundamental split can exist between what human rights law requires and what is, in fact, provided or not provided to individuals through the practices of Canadian law enforcement agencies and the criminal justice system.

The importance of notice to individuals and the public regarding how policing agencies have conducted technological surveillance is reinforced by the further importance of disclosure to accused individuals. By receiving notice, defendants in criminal courts can take steps to ensure they receive all

644 UN General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/73/348 (29 Aug 2018) <https://undocs.org/A/73/348> at para 40.

645 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 40; UN Human Rights Council, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at paras 41 and 54.

646 *Criminal Code*, s 196.

647 *R v Tse*, 2012 SCC 16 at para 83.

648 See *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, s 27(3)(a); *Freedom of Information and Protection of Privacy Act*, RSO 1990, c F.31, s 39(3); *Municipal Freedom of Information and Protection of Privacy Act*, RSO 1990, c M.56, s 29(3)(a), which contain explicit exemptions from the general notice requirement for personal data collected for law enforcement purposes. In other privacy legislation, such as the *Privacy Act* and the Alberta FIPPA, law enforcement exemptions are captured in provisions that state that notice is not required if providing it could result in the collection of inaccurate data: see *Privacy Act*, RSC 1985, c P-21, s 5(3); *Freedom of Information and Protection of Privacy Act*, RSA 2000, c F-25, s 34(3).

further information necessary to enable full answer and defence. However, the notice requirement is also important for individuals who have experienced potential privacy or free expression violations or discrimination, but where the Crown has not filed criminal charges after engaging in the activities that resulted in such violations. For example, where individuals are wrongly identified by facial recognition systems, such as those used by the Calgary Police Service and the Toronto Police Service, the CPS and TPS documents released through FOI requests do not indicate that these individuals would be notified.[649] Individuals whose images are captured by facial recognition technology may suffer a number of civil liberties violations, including harms associated with being detained or arrested, or invasions of privacy occasioned by other police investigative techniques (e.g., searches of an individual's home, accessing the private contents of a confiscated computer, or strip searches on arrest). Such harms may occur even if the ensuing investigation does not ultimately lead to a criminal charge.

Further, unreasonable violations of civil liberties cause individual and societal harm to the fundamental freedoms that are protected by constitutional safeguards of privacy and free expression. It is for this reason that civil damages for *Charter* violations are intended to provide compensation, vindication, and deterrence against future similar violations.[650] Vindication "as an object of constitutional damages focuses on the harm the *Charter* breach causes to the state and to society."[651] Similarly, individuals who may be caught up in social media surveillance algorithms based on their communications, associations, or location may have their data stored in law enforcement systems without their knowledge.[652] Yet, Canadian law enforcement agencies have not historically provided such notice when monitoring the online or offline activities of protesters.[653] In short, while substantive harms to individuals' constitutional and human rights may result from being directly or indirectly targeted by algorithmic policing technology, there is currently no guarantee of notice to individuals in Canadian law when they are subjected to such technology, and therefore, there is no guarantee that they will be able to obtain remedies for associated violations.

A requirement for notice is directly related to the ability to exercise the right to an effective remedy. In order to seek access to a remedy, the affected person(s) must actually realize that their rights have been

649 Mark Saunders, "Facial Recognition System", 17 May 2019, pages 2-3, presented at meeting of Toronto Police Services Board, 30 May 2019; Calgary Police Service, "Facial Recognition Technology, Ref #IN-006-1" (obtained through freedom of information request 18-G-1921); and Calgary Police Service, "Facial Recognition 2018" (obtained through freedom of information request 18-G-1921).

650 *Vancouver (City) v Ward*, 2010 SCC 27. In civil claims seeking damages for *Charter* violations, courts are empowered to provide damages for the purpose of personal compensation, vindication, or deterrence. Personal damages are not exclusively the focus. Personal compensation focuses on the claimant's personal loss (physical, psychological and pecuniary), as well as the claimant's intangible harm such as distress, humiliation, embarrassment, and anxiety.

651 *Vancouver (City) v Ward*, 2010 SCC 27 at para 28.

652 See Section 5.3 ("Rights to Freedom of Expression, Peaceful Assembly, and Association"), which discusses the growing body of empirical evidence shining a light on the problematic link between government online surveillance— including the mere prospect of such surveillance— and such chilling effects on freedom of expression.

653 For example, the Toronto Police Service and RCMP's surveillance of Black and Indigenous protesters only became publicly known information following the release of documents in response to freedom of information requests: Marilyn Robak, "'We've always been seen as a threat,' says former N.W.T. premier of RCMP surveillance revelations", *CBC News* (20 November 2016) <https://www.cbc.ca/news/canada/north/indigenous-trust-reconciliation-mmiw-protesters-rcmp-surveillance-1.3857009>; Stephen Davis, "Police monitored Black Lives Matter Toronto protesters in 2016, documents show", *CBC News* (3 May 2018) <https://www.cbc.ca/news/canada/toronto/police-monitored-black-lives-matter-toronto-protesters-in-2016-documents-show-1.4645628>.

violated. This is no simple matter when it comes to algorithmic policing technology because individuals may not even be aware that they have been subject to algorithmic surveillance or predictions.[654] For example, in New Orleans, individuals who were accused of belonging to a gang, based on Palantir-driven data analytics, were not informed about the software's use in their criminal proceedings.[655] Notice may also be logistically difficult to provide in some circumstances where an algorithmic tool is used to collect large volumes of information about many individuals. However, individuals (and their legal counsel) cannot challenge algorithmic decisions or inferences about them if they are not aware of such decisions or inferences, let alone raise legal challenges to the algorithmic policing tools themselves.

Even where individuals are aware that they have been targeted by algorithmic policing, the black box problem presents an additional informational barrier to the ability to access effective remedies.[656] If individuals and their legal representatives cannot comprehend how the system that targeted them operates, they may not understand how their rights have been infringed. Further, the right to a remedy is adversely affected if individuals cannot examine the algorithmic policing technologies that affected them and, thus, challenge the accuracy, reliability, and fairness of those technologies, which potentially violated their human rights, whether by reason of intelligibility or commercial resistance and attempts to shield proprietary software from scrutiny.[657]

## 5.7.2. Remedies for Human Rights Violations Must Be Effective

Effective remedies must be known and accessible to individuals whose rights have been violated.[658] To be effective, remedies must be capable of ending ongoing rights violations. Moreover, states must take measures to prevent rights violations from recurring.[659] For example, remedies should involve the ability for a court to order a law enforcement agency to stop using a particular algorithmic policing tool or category of tools.

Under the *Charter*, the right to a remedy can potentially bring widespread or systematic practices regarding *Charter* violations to a court's attention in an individual case.[660] Given algorithmic policing

654 UN Human Rights Council, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at para 54; UN General Assembly, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, A/73/348 (29 Aug 2018) <https://undocs.org/A/73/348> at para 40.

655 Ali Winston, "New Orleans ends its Palantir predictive policing program", *The Verge* (15 March 2018) <https://www.theverge.com/2018/3/15/17126174/new-orleans-palantir-predictive-policing-program-end>.

656 See the above discussions on algorithmic transparency and the black box problem, and the example of *State v Loomis*, both in Section 5.6.1 ("Informational Barriers to Due Process: Algorithmic Transparency and Private Sector Influence").

657 UN Human Rights Council, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (3 August 2018) A/HRC/39/29 <https://undocs.org/A/HRC/39/29>, at para 55.

658 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>, para 40.

659 UNHRC, *General Comment No 31 [80] (The Nature of the General Legal Obligation Imposed on States Parties to the Covenant)*, 80th Sess, adopted 29 March 2004, CCPR/C/21/Rev1/Add13, at paras 15, 17, 19 <https://digitallibrary.un.org/record/533996?ln=en>.

660 See *R v Rogers Communications*, 2016 ONSC 70. However, the ability of individual litigants to raise *Charter* violations of the rights of third

technologies may have community-level impacts, the need for remedies to be sufficiently meaningful and responsive to the true scale and impact of the violation is important. In some section 8 cases (involving the right to be free from unreasonable search and seizure), for example, the courts have acknowledged the importance of protecting the privacy rights of third parties who are not the defendant before the court.[661] Originally, the Supreme Court of Canada held that the extent of privacy invasion involving third parties was only relevant in circumstances involving "a 'potentially massive invasion of . . . privacy' of members of the general public who were not involved in the suspected criminal activity."[662] However, this position was extended in 2017, where the unconstitutional search of another individual's cellphone was constitutionally relevant to a defendant's claim that their own section 8 right was violated. The third-party violation had bearing towards the defendant's *Charter* remedy that sought the exclusion of evidence obtained.[663] Such reasoning may apply to individuals where their privacy rights or those of third parties have been violated by, for instance, facial recognition or algorithmic analysis of social networks. Therefore, in Canada, an effective right to a remedy for constitutional or human rights violations by the use of algorithmic policing technologies may require the recognition that violating a third party's right to privacy through use of these technologies may render a search unconstitutional under section 8 of the *Charter* in the case of a given defendant.

Despite judicial decisions that have to date provided one form of remedy for unlawful surveillance in criminal justice cases, accountability for misuses of intrusive technologies may be elusive if the oversight principally emerges only through case litigation. Individual litigants may provide an insufficient check on the systemic practices of mass surveillance. Regulatory and judicial oversight on a prospective and ongoing basis (e.g., through warrants, reporting requirements, and laws setting out limits and safeguards on the use of algorithmic policing technologies) can provide necessary checks and balances, assuming that the algorithmic tool in question can be used in a manner that is compliant with the *Charter* and with law enforcement agencies' human rights obligations. However, safeguards must be carefully delineated on the basis that overly broad standards or rules run the risk of simply functioning as vehicles for meaningless assurances of 'compliance' without providing genuine or substantive protections of *Charter*-protected and internationally protected human rights.

### 5.7.3. Concluding Comments: Algorithmic Policing and the Right to a Remedy

In light of the many constitutional and human rights concerns highlighted throughout Part 5 ("International Human Rights and *Charter* Rights Implications of Algorithmic Policing"), it is essential for individuals to have access to effective remedies for potential rights violations caused by algorithmic

---

parties is still evolving and somewhat uncertain.

661 See *R v Marakah*, [2017] 2 SCR 608; R v Thompson, [1990] 2 SCR 111 (where the SCC held that intercepting from a public telephone led to breach of third-party privacy rights which made wiretap intercepts by law enforcement unreasonable and violative of section 8); *R v Mahmood*, [2008] OJ No 3922 (SCJ), additional reasons [2009] OJ No 319, and later on appeal, 2011 ONCA 693 (where the court considered and found section 8 violations occurring due to a tower dump production order's sheer breadth and scope); *R v Guindon*, 2015 ONSC 4317.

662 *R v Edwards*, [1996] 1 SCR 128 at para 38; *R v Thompson*, [1990] 2 SCR 1111 at 1143.

663 *R v Marakah*, [2017] 2 SCR 608.

policing. However, these technologies present challenges insofar as their operation and use are routinely obscured by secrecy and black box problems. Without access to information, individuals cannot exercise their right to a remedy. They would therefore lack a critical avenue of redress for the harmful effects of these technologies, which could potentially go either entirely or largely unchecked, thereby replicating historical injustices that can arise from biased policing practices or systems.

## 5.8. Towards a Human Rights-Based Approach to Algorithmic Policing

Part 5 of this report provided dedicated legal and policy analysis of the potential implications of algorithmic policing technologies for each of several fundamental human rights protected by international and domestic human rights law and by the Canadian *Charter*. Specifically, the use of algorithmic policing technologies by law enforcement introduces or exacerbates risks of violating the right to privacy (Section 5.2); the rights to freedom of expression, peaceful assembly, and association (Section 5.3); the right to equality and freedom from discrimination (Section 5.4); the right to liberty and to be free from arbitrary detention (Section 5.5); the right to due process (Section 5.6); and the right to a remedy (Section 5.7). The findings and conclusions for how each of these human rights are impacted by algorithmic policing technologies have been summarized in their respective sections above and are reiterated in corresponding sections in the next part of this report, Part 6 ("Recommendations & Conclusion").

Part 6 draws on the legal and policy analysis in Part 5 of the report, synthesized with the factual findings regarding the current state of algorithmic policing in Canada in Part 4 ("Algorithmic Policing in Canada: The Current Landscape"), to provide a suite of recommendations to the Canadian government, law enforcement agencies, and other actors in the criminal justice system. Each recommendation flows directly from the research and analysis conducted throughout this report; however, some recommendations may introduce new information that is required to more fulsomely substantiate how such a recommendation might be carried out. Taken together, the recommendations provide a comprehensive, albeit non-exhaustive, framework to support legal and policy reform to mitigate or prevent the negative impacts of law enforcement usage of algorithmic policing technologies on constitutional and human rights, particularly those of historically marginalized communities, who will be the most detrimentally affected.

# 6. Recommendations and Conclusion

This report has revealed a number of significant policy, practice, and legal deficits related to the use of algorithmic policing technologies in Canada. The research findings in Part 4 ("Algorithmic Policing in Canada: The Current Landscape") described how multiple law enforcement agencies across the country are using or developing various forms of algorithmic policing technologies. The accompanying legal analysis in Part 5 ("International Human Rights and *Charter* Rights Implications of Algorithmic Policing") discussed how such technologies have high potential to infringe fundamental human rights and freedoms that are protected under the constitution and international human rights law.

Part 6 synthesizes those deficits and, in the process, provides recommendations to ensure that law enforcement agencies and governments uphold constitutional and human rights whenever they consider developing or adopting algorithmic policing technologies. These recommendations should also be considered to apply retroactively to algorithmic policing technologies that have been developed, adopted, or otherwise already put into use by Canadian law enforcement.

A key animating principle behind the recommendations is the need for robust standards of transparency and accountability. In the process of producing this report, a common set of obstacles arose, which demonstrated significant information asymmetry between law enforcement authorities and the public. In addition to barriers in Canada's freedom of information (FOI) processes, as described in Section 4.4 ("Limitations of Research Findings"), some law enforcement agencies have been reticent with respect to publicly disclosing their use or adoption of algorithmic policing technologies. This reluctance has included failure to disclose which agencies are using particular types of algorithmic policing technologies, including specific commercial products, and failure to proactively explain how such technology is being used. The absence of complete information poses a significant challenge in determining the extent to which existing or potential uses of algorithmic policing technologies may violate police agencies' constitutional and human rights obligations or may raise other legal concerns. As a result, many of this report's recommendations focus on establishing transparency requirements as a necessary precondition to public accountability. Strong accountability mechanisms are necessary to enable policy-makers and the public to meaningfully think through and determine the risks and harms to constitutional and human rights that arise from the development or use of any given algorithmic policing technologies, before any such development or use occurs. In the event that a considered decision is made to implement an algorithmic policing technology, accountability mechanisms are needed to establish the limitations and measures required to safeguard constitutional and human rights whenever that particular tool is used.

In addition to transparency and accountability requirements, the recommendations in this report are animated by the need to impose nation-wide moratoriums on all algorithmic policing technologies until full inquiries into this class of technology have occurred and constitutional safeguards are put in place. Such moratoriums are necessary to mitigate harms from unscrutinized deployment of algorithmic policing technology and to ensure that technology does not outrun human rights and the law when it comes to criminal justice. With respect to implementing such moratoriums, Canada has a complex network of regulatory actors that share partially overlapping roles in governing and overseeing law

enforcement agencies. Regulation varies according to the province any given police service is located in and to the classification of the service as municipal, provincial/territorial/regional (all referred to throughout Part 6 as 'provincial'), or federal. For example, both municipal and provincial governments can regulate municipal police services through imposing moratoriums on certain technologies. As a result, all levels of government that possess legal authority related to law enforcement agencies can and must establish both immediate temporary stops (i.e., moratoriums) and, pending further study and impact assessments, long-term limits or complete bans on the use of certain algorithmic policing technologies.

Part 6 presents a total of twenty recommendations for protecting human rights in the context of algorithmic policing. Among these, the authors of this report have identified a set of seven priority recommendations that governments and law enforcement authorities must act upon with urgency. These recommendations, if they are 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.

## Priority Recommendations for Algorithmic Policing in Canada

1. **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.
2. **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.
3. **Governments must make reliability, necessity, and proportionality prerequisites 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.
4. **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.

5. **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.

6. **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.

7. **Governments and law enforcement authorities must engage external expertise, including expertise 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.

These priority recommendations are each developed and explained in greater detail below, where they appear within the full set of recommendations. The full set, presented in Sections 6.1 through 6.5, follows the structure of the legal analysis in Part 5 and is categorized under each human right discussed: the right to privacy (Section 6.1); the rights to freedom of expression, peaceful assembly, and association (Section 6.2); the right to equality and freedom from discrimination (Section 6.3); the right to liberty (Section 6.4); and the rights to due process and to a remedy, with emphasis on accountability and transparency (Section 6.5). Section 6.6 provides concluding comments for the report as a whole.

Each section contains recommendations that take ultimate priority and should be considered threshold questions when considering any given algorithmic policing technology. These threshold recommendations, which overlap with the priority recommendations, are of far greater importance than the others and must be addressed before all else because, if heeded, the threshold recommendations may result in bans or severe limitations on some forms or uses of algorithmic policing technology; 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.

For guidance, the recommendations are colour-coded according to whether they are a priority threshold recommendation or an ancillary recommendation that would apply only if an algorithmic policing technology had not already ben limited by moratoriums, bans, or other significant legal restrictions that prevent its usage. The colour code is set out in the following legend:

**PRIORITY RECOMMENDATIONS:** These are the priority threshold recommendations that governments and law enforcement authorities must act upon now to mitigate some of the worst human rights and *Charter* violations, which could occur as a result of the Canadian government and law enforcement agencies using algorithmic policing technologies.

**ANCILLARY RECOMMENDATIONS:** These are recommendations that would become applicable and important in circumstances where an algorithmic policing technology is not prohibited by human and constitutional rights or blocked or limited by the moratoriums and restrictions set out in the priority recommendations.

## 6.1. Recommendations to protect the right to privacy

Algorithmic policing technologies engage the right to privacy as a result of the data-collection, data-processing, and data-sharing methods that such technologies typically rely on as well as from the data accuracy issues that frequently arise with these technologies. These kinds of policing tools generally process large data sets to attempt to forecast or reveal information or make inferences that can then be acted upon by law enforcement. Legal safeguards or constitutional protections must be developed or upheld, so individuals retain the ability to be fully free from unreasonable interference with privacy and to ensure that protected zones of privacy are not eroded by expanding data-collection practices and algorithmic surveillance capabilities.

Determining the appropriate protective measures is not always an easy task. Algorithmic policing technologies can challenge existing constitutional and human rights safeguards where the legal system has not yet had a chance to create a bright-line set of rules for law enforcement to follow, but where the need for privacy protection looms large. This includes the aggregation of data that has been 'scraped' from the Internet or the use of biometric data that can be obtained without a person's consent. Further, algorithmic policing technologies create new privacy challenges by making *new* uses of *old* data (i.e., *repurposing* police data) that was collected by law enforcement agencies long before algorithmic policing methods were contemplated. Existing legal protections for those types of data, such as mug-shot databases, may no longer be sufficient in light of advanced algorithmic processing capabilities.

The authors propose seven recommendations to address the likely privacy challenges associated with algorithmic policing technologies. These recommendations generally focus on requiring all algorithmic policing technologies to meet prerequisite conditions of necessity, proportionality, and reliability before they can be used; on oversight mechanisms; and on the importance of data accuracy.

### Recommendation 1: Governments must make reliability, necessity, and proportionality prerequisites for the use of algorithmic policing technology.

Municipal, provincial, and federal governments, to the extent they oversee police services in Canada, should implement moratoriums on all algorithmic surveillance technologies that do not meet threshold requirements of reliability, necessity, and proportionality. A moratorium should immediately begin with facial recognition technology. All algorithmic policing technologies should undergo assessment to determine whether the technology is independently verified as reliable; whether the use of the technology by law enforcement authorities is necessary for the tasks performed and their stated objectives; and whether the technology is proportionate to the tasks and objectives, given associated costs, risks, and harms. In some circumstances, the use of an algorithmic policing technology may lack sufficient reliability to justify use; may not be necessary given reasonable alternatives (including the alternative of not adopting the proposed technology for the stated purpose); or may disproportionately inflict privacy harms. For example, facial recognition technology that relies on a large volume of images scraped from the Internet will likely be inconsistent with fundamental privacy norms. As a growing body of research has demonstrated, the danger of this algorithmic surveillance technique is only made worse by the fact that facial recognition algorithms regularly lead to misidentification, including the finding that such algorithms are far more likely to misidentify racialized individuals and women, compared to white men.

### Recommendation 2: Law enforcement authorities should enhance police database integrity and management practices, including strengthening the ability of individuals to verify and correct the accuracy of personal information stored in police databases.

Existing policing databases are often rife with biased and inaccurate data, and any algorithmic policing technology that relies on such databases risks replicating and reinforcing such biases and inaccuracies. Law enforcement and the justice system must develop processes to successfully maintain and update such databases (e.g., criminal record databases, databases containing police stop data), especially when the data contained in them would be processed by algorithmic policing technology.[664] Law enforcement agencies in most provinces are already subject to meaningful standards of data accuracy under privacy legislation in Canada. However, data accuracy standards should be reinforced with a web of meaningful checks and balances, including regular audits and guidance from technical experts, in conjunction with privacy rights and criminal justice experts, about applicable best practices concerning database management as it relates to algorithmic technology. Only data that is subject to

664 Brigitte Bureau, "RCMP database remains out of date, police and prosecutors say", *CBC News* (10 March 2015) <https://www.cbc.ca/news/politics/rcmp-database-remains-out-of-date-police-and-prosecutors-say-1.2989397>.

data accuracy standards that are reinforced by adequate checks and balances should be considered for algorithmic processing for criminal justice purposes, provided all other criteria are met (such as those set out in these recommendations or established by a judicial inquiry).

### Recommendation 3: Governments should expressly regulate the retention and destruction of biometric data by law enforcement authorities.

The collection and retention of personal information such as fingerprints and mug shots is protected by section 8 of the *Charter* and privacy legislation. However, individual police services have differing policies with respect to the destruction of biometric data (e.g., fingerprints, mug-shot photos) and, 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 according to internal policies). Current processes through which a person can request the destruction of records after their case is dealt with are likewise inconsistent, vague, or overly discretionary. Express government regulation is necessary to standardize police policy, reinforce privacy protections, and provide guidance to bring practices into compliance with the principles of necessity and proportionality. Requesting the destruction of data or records should be free for individuals. Data should be automatically and promptly destroyed in cases where no charges are laid or where charges are stayed, dismissed, or withdrawn.

### Recommendation 4: The federal government should reform the judicial warrant provisions of the *Criminal Code* to specifically address the use of algorithmic policing technology by law enforcement authorities.

One of the most fundamental ways to safeguard protected privacy interests is to ensure that law enforcement activity that intrudes into individuals' lives is the subject of meaningful oversight. The absence of oversight will usually render law enforcement techniques that engage privacy interests unconstitutional.[665] Traditionally, such oversight has meant obtaining prior authorization from judges (e.g., in the form of a warrant or production order) before law enforcement carries out an action that interferes with any individual's privacy. Following this model, judicial warrants should be obtained before law enforcement authorities can conduct algorithmic data processing on previously collected data. While general warrants provide a catch-all procedure for police techniques that are not otherwise regulated under other warrant or production order mechanisms, Parliament should reform the *Criminal Code* to specifically address law enforcement agencies' use of algorithmic policing technologies. Such reform should specifically address data-processing methods that involve law enforcement's search or seizure of data for the purpose of algorithmic analysis of the kind examined in this report, including 'predictive' analytics. For example, while the existing oversight regime in the *Criminal Code* regulates forensic DNA analysis, it does not provide any specific guidance or clear limits on the use of biometric data and facial recognition software on photographs that are already in the possession of the police (which were collected for other purposes). Legal reform should be implemented to rectify this deficit.

665 See e.g., *R v Tse*, 2012 SCC 16.

### Recommendation 5: Federal and provincial legislatures should review and modernize privacy legislation with particular attention to re-evaluating current safeguards to account for the advanced capabilities of algorithmic policing technologies.

All police services across Canada are subject to either federal or provincial privacy legislation. Privacy legislation plays an important role in regulating the minimum standards that must be met by law enforcement agencies when they collect, process, or disclose an individual's personal information. Parliament and legislative assemblies should review privacy legislation and, as appropriate, update it to best govern law enforcement's use of big data through algorithmic technology. For example, privacy legislation often establishes exemptions and permissive authorization for law enforcement related activities. While such exemptions were, for the most part, included and drafted at a time when more traditional policing activities were contemplated, the same exceptions could, troublingly, now be repurposed to exempt contemporary algorithmic policing technology from much needed privacy controls. As such, these exemptions must undergo reform to sufficiently protect the standards of proportionality and necessity. More specifically, potential areas for review and reform should include the manner in which privacy legislation governs the collection, processing, and disclosure of metadata, biometric data, personal data in public environments, information-sharing arrangements, redress mechanisms, and consequences for failing to safeguard personal information.[666]

### Recommendation 6: Law enforcement authorities must exercise extreme caution to avoid unconstitutional data-sharing practices with the private sector and non-police government agencies.

Regularized data-sharing practices between law enforcement authorities and either other governmental actors—such as social service agencies, schools, or public transit authorities—or the private sector must be handled with extreme caution. Such caution, including total avoidance wherever possible, is required because data-sharing arrangements where data flows from non-law-enforcement entities to law enforcement agencies may result in constitutional obligations for the former that are both unavoidable in law yet unworkable in practice, leading to an untenable situation with respect to upholding the section 8 right to privacy.

Specifically, if a public or private entity is engaged in a formal or ongoing data-sharing arrangement to assist police with law enforcement activities, that entity may inadvertently become bound by constitutional privacy obligations under section 8 or according to the law enforcement agency doctrine. Such obligations could include the requirement to obtain a judicial warrant when collecting private data prior to sharing it with a police service. However, not only are non-law enforcement entities unaccustomed to complying with the constitutional safeguards normally applied to police use of private information, but as a matter of law and practice, they would not be able to bring themselves

666 See for example, Report of the Standing Committee on Access to Information, Privacy and Ethics, "Protecting the Privacy of Canadians: *Reform of the Privacy Act*", (December 2016), <https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP8587799/ethirp04/ethdirp04-e.pdf>.

into constitutional compliance, even if they tried, because Canadian judicial warrant procedures are available only to law enforcement authorities. Thus, data-sharing arrangements between law enforcement agencies and other governmental agencies or private sector entities, for policing purposes, likely cannot constitutionally exist without causing significant and complex ramifications for the data-collection practices of such non-police entities.

To guard against unconstitutional data-sharing arrangements, any instances of data sharing with law enforcement agencies, by non-police government actors or private sector entities, should be formally documented in memorandums of understanding, and such memorandums should be submitted to the relevant privacy commissioners for review and for public record purposes. As a general rule, data from public sector agencies and private sector entities should not be passed on to or placed into the custody of law enforcement agencies. These non-police actors must adhere to their own privacy obligations that govern the lawful treatment and safeguarding of personal data and individuals' privacy rights.

## 6.2. Recommendation to protect the rights to freedom of expression, peaceful assembly, and association

Algorithmic policing technologies, and particularly algorithmic surveillance techniques, risk chilling the exercise of the rights to freedom of expression, peaceful assembly, and association. Algorithmic policing technologies highlight the particularly close connections between the right to privacy and these fundamental freedoms, all of which are protected under international human rights law and section 2 of the *Charter*. For example, algorithmic surveillance tools such as facial recognition technology and social media surveillance software threaten the anonymity of the crowd that has traditionally protected the identities of protesters in outdoor and online environments[667] and may also pose a chilling effect on protected freedoms[668]; these chilling effects were indicated by the formal research interviews conducted for this report and have been established in research studies. Such chilling occurs, in part, due to the historical and ongoing context of disproportionate law enforcement surveillance against racial justice and Indigenous rights advocates. The recommendation in this section focuses on ensuring that uses of algorithmic policing technology are necessary and proportionate to legitimate aims, relative to the potential significant harm to the rights to freedom of expression, peaceful assembly, and association resulting from the use of such technology.

**Recommendation 7: Law enforcement agencies must obtain prior judicial authorization in order to deploy algorithmic surveillance technology at public gatherings and in online environments.**

667 See Section 5.2.1 ("Data Collection: Mass Surveillance and Public Space").

668 See Section 5.3 ("Rights to Freedom of Expression, Peaceful Assembly, and Association").

Where algorithmic surveillance methods are used, the use of such techniques should be subject to prior judicial authorization in light of the heightened privacy interests at stake and constitutional protection under section 2 regarding proportionality and necessity. The warrant must be based on reasonable and probable grounds that there is a specific threat and that the use of the method will yield results that are necessary to address that threat.

Government agencies cannot legally justify monitoring either expressive or associational activities on the basis of monitoring political activism per se. For example, according to the *Security of Canada Information Disclosure Act*, "advocacy, protest, dissent or artistic expression is not an activity that undermines the security of Canada."[669] Restrictions on the right of peaceful assembly must be content-neutral and not based on race, ethnicity, political opinion, sexual orientation, or other protected or adjacent factors, while remaining alert to potential indirect discrimination through adverse impacts.[670] While further jurisprudence regarding section 2 of the *Charter* remains to be developed in the specific context of algorithmic policing technologies, indiscriminate surveillance is never necessary or proportionate under international human rights law.

## 6.3. Recommendations to protect the right to equality and freedom from discrimination

Algorithmic policing techniques can violate certain individuals' rights to equality and to be free from discrimination by way of adverse impact discrimination. The seemingly "neutral" application of algorithmic policing tools masks the reality that they can disproportionately impact marginalized communities in a protected category under equality law (i.e., communities based on characteristics such as race, ethnicity, sexual orientation, or disability). Historical and ongoing over-policing, harsher treatment, and systemic bias in the criminal justice system all cause police data to reflect historic disadvantages and discrimination imposed on particular groups, such as Black and Indigenous peoples, the LGBTQ community, people who are impacted by mental illness, people who are unhoused or otherwise socio-economically disadvantaged, and other vulnerable populations. Police data also reflects under-policing of those same communities when they are victims or preferential under-policing of offenders from dominant social classes. Numerous inaccuracies, biases, and other sources of unreliability are present in most of the common sources of police data in Canada. As a result, drawing reliable inferences based on historic police data is likely impossible, and thus any use of algorithmic policing technology that relies on such data is likely unconstitutional under section 15 of the *Charter*.

Some Canadian law enforcement authorities that use, or are considering using, algorithmic policing technologies have incorporated certain measures to prevent or mitigate potential discriminatory bias

669 *Security of Canada Information Disclosure Act*, SC 2015, c 20, s 2.

670 The Supreme Court of Canada has made clear that the *Charter* should be interpreted as a unified system that maintains its underlying values and is internally coherent throughout. *Health Services and Support – Facilities Subsector Bargaining Assn v British Columbia*, [2007] 2 SCR 391 at paras 80-86; *R v S* (RJ), [1995] 1 SCR 451 at 561.

linked with such technologies. For example, the Vancouver Police Department removes police-reported incidents from data used to train their location-focused algorithmic policing technology (the GeoDASH algorithmic prediction system). However, it is dubious that bias in the criminal justice system can be substantively mitigated if algorithms rely on data sets that reflect historic and ongoing systemic bias (which is also routinely reflected in incident reports initiated by members of the public).

Extreme caution must be exercised before law enforcement authorities are permitted, if at all, to use algorithmic policing technologies because these tools may exacerbate the already unconstitutional and devastating impact that systemic targeting of marginalized communities can cause (such as through heightened data visibility resulting from accessing social welfare services). Further, methods that could independently evaluate or verify the accuracy and reliability of algorithmic policing technologies are either lacking or are yet to be developed. The following three recommendations are made in light of deep uncertainty regarding whether it is possible to use algorithmic policing technologies in a manner that does not discriminate against or otherwise unjustly impact individuals protected by section 15.

**Recommendation 8: 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.**

A national judicial inquiry should be struck by the federal government to examine the potential use of algorithmic policing technology that processes mass police data sets. Examining (im)permissible uses of historic police data sets for the purpose of preventing adverse impact discrimination in Canada is critical in light of the government's obligations under the *Charter*, international human rights law, and ongoing processes of Reconciliation with Indigenous communities in Canada. The scope of an inquiry must include authority to investigate the scope of police data sets that are accessible to law enforcement authorities, to examine systemic biases that may be present in such data sets, and to scrutinize law enforcement practices relating to retention of data. The judicial inquiry should, in particular, focus on developing guidance that elucidates section 15 protections to assist law enforcement authorities, governmental actors, and justice system participants who may be involved with litigating and assessing algorithmic technologies under section 15. This recommendation is made in part due to the relatively under-developed nature of the jurisprudence under section 15 of the *Charter* in relation to governmental activity (i.e., actions taken by law enforcement actors based on inferences or forecasts from an algorithmic policing technology), as opposed to government legislation. Law enforcement agencies, legal counsel, and individuals involved in the criminal justice system would benefit from assistance in elucidating the state's responsibilities.

**Recommendation 9: Governments must place moratoriums on law enforcement agencies' use of technology that relies on algorithmic processing of historic, mass police data sets, pending comprehensive review.**

The *Charter* prohibits government activity that perpetuates or causes any prejudice or disadvantage to individuals on the basis of distinctions made on protected grounds under section 15. All levels

of government (i.e., municipalities, provincial governments, and the federal government), which are mandated with law-making authority in relation to law enforcement agencies, should establish moratoriums on technologies that rely on algorithmic processing of historic policing data sets. Establishing such moratoriums would prevent further harms from continuing or the identified human rights risks from materializing, while simultaneously providing time to complete a necessary, comprehensive, and holistic assessment (as recommended in Recommendation 8) of whether it is possible to use algorithmic policing technologies in a manner that does not unconstitutionally violate the rights of individuals protected by section 15, by perpetuating the discrimination that section 15 serves to prevent.

**Recommendation 10: Law enforcement authorities must implement ongoing tracking to monitor potential emergence of bias in the use of any algorithmic policing technology.**

Any use of algorithmic policing technologies must be accompanied by monitoring practices that are attentive to patterns that reflect bias, such as bias in relation to marginalized or historically oppressed communities. Monitoring should cross-reference the outcomes of algorithmic assessments against outside sources and disciplines to the extent possible (e.g., social sciences evidence, human rights reports, and community consultations or complaints) to ascertain whether undue bias is present in the algorithmic tools. In some cases, bias towards protected groups may be detected by looking at proxy data that tend to correlate with the historic discrimination experienced by protected groups. Proxies can include seemingly innocuous indicators (e.g., social media interests, purchase history) that are, in practice, linked with potentially sensitive data such as socio-economic status, race or ethnicity, geographic location, reliance on government services, or indicia associated with mental health treatment.

## 6.4. Recommendation to protect the right to liberty and to be free from arbitrary detention

The *Charter* and international human rights law guarantee the right to liberty, including the right not to be detained or arrested arbitrarily (under sections 7 and 9 of the *Charter*, respectively). Based on constitutional and international human rights obligations, law enforcement actors must have reasonable grounds (i.e., a sufficiently robust and objective reason) to interfere with an individual's liberty by detaining or arresting the individual. This constitutionally enshrined requirement of reasonable grounds prevents law enforcement authorities from relying on generalized predictions drawn by algorithmic policing technologies as a basis to detain or arrest an individual. By design, algorithmic policing technologies typically rely on generalized or stereotypical inferences about risk; these are prohibited grounds upon which to justify interfering with a person's liberty.[671]

671 This conclusion does not necessarily apply to all algorithmic policing technologies. Some forms of algorithmic surveillance technologies might be sufficiently reliable and specific to the individual's case, such that evidence obtained from the use of the technology could be considered by a police officer when forming grounds to conduct a detention or arrest. For example, an automated licence plate reader may

The generalized nature of algorithmic predictions is not the only problem that prevents algorithmic policing technologies from being appropriate tools to justify interference with liberty. Law enforcement authorities also cannot justify an arrest or detention on the basis of unreliable information. Algorithmic policing technologies remain widely untested and, in many cases, the algorithms are trained using biased police data.

**Recommendation 11: Law enforcement authorities should establish a blanket prohibition against relying on algorithmic predictions to justify interference with individual liberty.**

Law enforcement agencies and their associated oversight bodies must ensure that algorithmic policing technologies are not used to restrict individual liberty through detention and arrest. To implement the constitutional imperative that algorithmic predictions cannot be relied upon to justify interference with liberty, this report recommends that law enforcement agencies establish and enforce written policies that specifically prohibit the use of algorithmic policing technologies as grounds for a detention or arrest. A clear prohibition against the use of algorithmic predictions to justify police activities such as stops, detentions, and arrests is necessary due to the inadequacy of alternative protective measures that could be considered. The dangers associated with unjustified and biased policing actions are too great.

Such risks of unconstitutional infringements of the right to liberty arise from two forms of bias in particular: unconscious bias based on protected characteristics, which leads to issues such as racial profiling, and automation bias, which is the tendency of humans to defer to technology as superior to human judgment, even when they have reason to believe the technology is flawed or incorrect. While studies from other fields have shown that some forms of training or mitigation techniques can reduce automation bias in some cases, outcomes on the whole have been mixed.[672] It must be emphasized that such measures, even if perfectly implemented and adhered to in practice, cannot eradicate automation bias.[673] Thus such training and mitigation measures are insufficient to ensure that the use of algorithmic policing technologies in police decision making does not result in violations of human

---

capture a clear image of a licence plate that is connected to a suspended licence, which would constitute more reliable evidence than an algorithmic inference or generalization.

672 See e.g., "[A]gencies should make it clear to hearing officers that automated systems are fallible. To that end, hearing officers should receive explicit training about the phenomenon of automation bias. Studies demonstrate that individuals who receive such training are more likely to scrutinize an automated system's suggestions. The training of judges has been effective in a parallel enterprise. Special workshops on scientific theory and methodology have provided needed training to federal district court judges charged with assessing the reliability of expert testimony. [...] [A]gencies should require hearing officers to explain, in detail, their reliance on an automated system's decision. Officers should identify the computer-generated facts or legal findings on which they relied in making their decisions. This accords with administrative law's long-standing faith in the prophylactic power of requiring explicit statements of reasons. Asking hearing officers to evaluate the basis for their decisions would further mitigate the effects of automation bias" Danielle Keats Citron, "Technological Due Process" (2008) 85:6 Washington University Law Review 1249 at 1306-07 (footnotes omitted); Osonde Osoba & William Welser IV, "An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence", RAND Corporation (2017) at 23-24 <https://pdfs.semanticscholar.org/b7be/0be36706c30a76312b34d60ff02d97698191.pdf>; and Kate Goddard, Abdul Roudsari & Jeremy C Wyatt, "Automation bias: a systematic review of frequency, effect mediators, and mitigators" (2012) 19 Journal of the American Medical Informatics Association 121 at 125.

673 See e.g., John Zerilli, Alistair Knott, James Maclaurin & Colin Gavaghan, "Algorithmic Decision-Making and the Control Problem" (2019) 29 Minds and Machines 555 at 575.

rights through unreasonable restrictions on individual liberty. This particular use of algorithmic policing technology should be subjected to a complete ban.

## 6.5. Recommendations to protect the rights to due process and remedies (accountability and transparency)

Robust procedural safeguards protect fundamental human rights that are affected by law enforcement activities. A central way of protecting *Charter* rights and international human rights, including the right to due process and the right to a remedy for rights violations, is to develop strong accountability mechanisms through a comprehensive system of checks and balances. Accountability mechanisms enable parliamentarians, the press, courts, civil society organizations, criminal defense attorneys, and the public writ large to have access to information and fair processes through which to guard against rights infringements and to provide measurable standards with which to examine law enforcement conduct.

The legal landscape of police oversight bodies is a complex patchwork of entities. Such entities include civilian oversight agencies for police services, governmental privacy and human rights commissioners, courts, public inquiries and systemic reviews, and police service boards. Police oversight regimes incorporate and balance an underlying principle in Canada's legal system that respects the independence of the police from certain forms of political interference.[674] If algorithmic policing technologies continue to be used in Canada by law enforcement authorities, all of these elements of oversight will have roles to play. As a result, the following nine recommendations focus on mechanisms to coordinate oversight through the development of institutional expertise, guidance, and accountability within this complex landscape.

**Recommendation 12: Law enforcement agencies must be immediately and fully transparent with the public and privacy commissioners regarding all uses of algorithmic policing technologies.**

Law enforcement agencies across Canada should immediately and publicly disclose information about any algorithmic policing technologies that are being considered, developed, procured, tested, or put in use for policing purposes. Agencies should make publicly available, with alacrity, information about any current uses or testing of algorithmic policing technology, as an interim step until other long-term and permanent transparency and accountability measures can be established (as will be detailed in Recommendations 13 and 14). Law enforcement agencies across Canada should also urgently

674 See Kent Roach, "Models of Civilian Police Review: The Objectives and Mechanisms of Legal and Political Regulation of the Police" (2014) 61 *Criminal Law Quarterly* 29; Kent Roach, "Police Government Relations and Police Independence" (June 2017), <https://www.cepcsj.gouv.qc.ca/fileadmin/documents_client/recherche/Quebec_Police_Independence_pour_depot.pdf>.

begin, or expand, disclosures and dialogue with the federal and provincial information and privacy commissioners regarding all algorithmic policing technologies that are being considered, procured, tested, or deployed for policing purposes. Adopting a robust set of transparency practices is critical in light of how productive discussions are often predicated on all parties understanding the technologies being discussed. Pre-emptive disclosure should be widely adopted and implemented as a best practice among all law enforcement agencies going forward.

**Recommendation 13: Governments and law enforcement authorities must engage external expertise, including expertise from historically marginalized communities that are disproportionately impacted by the criminal justice system, in the development of regulation and oversight mechanisms for algorithmic policing technologies, as part of completing algorithmic impact assessments and in monitoring the effects of any such technologies that have been put into use.**

Historically marginalized communities that are subjected to systemic discrimination in the criminal justice system must be involved in any processes to develop, implement, or monitor algorithmic policing tecchnologies, including associated regulation and oversight mechanisms. These communities may provide reasons or illuminate why a given technology is inappropriate, illegal, unnecessary, harmful, or unreasonably intrusive, which law enforcement agencies or governments may not be aware of otherwise. Impacted communities may also be able to offer alternative or more effective measures to address a specific problem, in lieu of the proposed technology, or identify a more pressing issue requiring attention. Furthermore, independent experts—such as legal, racial justice, and technology and human rights scholars, public interest technologists, or security researchers—should be included in any consultations so that the legal, policy, and technical aspects of a proposed algorithmic policing technology are adequately assessed in the consultation process. Any consultation of community representatives or other experts should include fair compensation for their time and expertise; one potential approach is to follow models adopted by the Canadian Radio-television and Telecommunications Commission and other administrative tribunals, which provide funding to enable substantive public interest participation in proceedings.

**Recommendation 14: Provincial governments should enact directives regarding the use and procurement of algorithmic policing technologies.**

Provincial governments should enact Ministerial directives to require that all uses of algorithmic policing technologies—to the extent they are not otherwise banned by moratorium or constitutional prohibition—to fully comply with a government-wide directive governing the responsible development and use of these technologies.[675] The Report of the Ipperwash Inquiry in Ontario supports the use of Ministerial directives as a method of introducing regulatory oversight for law enforcement activities on

675 For an example of such a directive, see: <https://seattle.legistar.com/LegislationDetail.aspx?ID=2981172&GUID=0B2FEFC0-822F-4907-9409-E318537E5330&FullText=1>, where Seattle's City Council issued a law governing the acquisition and use of surveillance equipment, arising out of concerns about privacy and lack of process for the City's acquisition of surveillance technologies such as drones and the installation of video cameras along Seattle's waterfront and downtown.

areas of particular concern to human rights.[676] Provincial directives regarding the responsible development and use of algorithmic policing technologies should include the following key requirements:

- A requirement that law enforcement authorities complete an **algorithmic impact assessment** prior to using an algorithmic policing system, according to a standardized framework that explicitly evaluates compliance with international human rights law and the *Charter*. This impact assessment should incorporate a reliability, necessity, and proportionality assessment, with an accompanying prohibition on the use of algorithmic technologies that are determined to potentially result in a disproportionate impact on human rights.[677]
- For algorithmic policing technologies that have the potential to impair *Charter* and human rights, **prior Ministerial approval** should be required along with prior consultation with privacy commissioners.
- Robust requirements for **independent review and scientific validation (published to enable public accountability and review in court proceedings)** of the underlying algorithms in policing technologies prior to their use; in particular, they should evaluate accuracy, fairness, and statistical or discriminatory bias. Arms-length contracts with compensation will be required to facilitate independent review.
- A requirement that law enforcement authorities that are using algorithmic policing technology must proactively **publish information, such as through an open data portal**, about the types of training data and operational police data used in algorithms. Reports must include demographic information, including, in particular, racially disaggregated data. One model for such an approach is found in the Chicago Data Portal, which published data used to create the Chicago Police Department's now discontinued risk assessment algorithm known as the Strategic Subject List (SSL).[678] An open data portal should provide transparency into how algorithmic policing technologies use, process, and rely on the data; should provide data in a format available for independent use and cross-referencing with other data sets; and must be clear with respect to data

676 The Report recommended the issuance of a number of Ministerial directives for law enforcement authorities in Ontario to respond to the particular human rights and policing issues that were the subject of that inquiry: Sidney B. Linden, *Report of the Ipperwash Inquiry* (Toronto: Published by Ministry of the Attorney General, Queen's Printer for Ontario, 2007). As set out in IN FOCUS #2: Overview of the Canadian Criminal Justice System, police services in Canada fall under provincial jurisdiction, and provincial governments therefore have the authority to engage in oversight through formal directives. Municipalities can also regulate municipal law enforcement authorities where provincial responsibility has been delegated, and both the federal and provincial governments can regulate in relation to the RCMP.

677 For more details, see "IN FOCUS #8: Algorithmic Impact Assessments", in Section 5.6.3. Concluding Comments: Algorithmic Policing Technology and Due Process.

678 "Strategic Subject List" (7 December 2017) Chicago Data Portal <https://data.cityofchicago.org/Public-Safety/Strategic-Subject-List/4aki-r3np>.

- that is not provided because it does not exist, or because it was not collected.[679] Any open data and similar public disclosure initiatives must proceed with due caution with respect to the potential for privacy harms and violations depending on the type of data provided.[680] As Teresa Scassa has warned, public sector privacy laws, which apply to law enforcement, "require public bodies to protect individual privacy by balancing privacy rights against the public interest in disclosure of personal information. In cases where the personal information is highly sensitive in nature, privacy rights generally prevail over disclosure."[681]

- A requirement that all algorithmic policing technologies that are adopted be **compatible with a robust framework of procedural fairness** and due process in the implementation of algorithmic methods including, but not limited to, requirements that the law enforcement agency has the ability to provide complete disclosure in criminal proceedings.[682]

- No decision or action by a justice system actor (law enforcement official or in criminal court) that impacts the constitutional or human rights protected interests of an individual is taken as a result of an algorithmic system alone (i.e., there must always be a **human in the loop**).

- All uses of algorithmic policing technology should incorporate statistical **tracking and a formal documentation process for all known errors and incidents** (e.g., data breach, tampering).

- The use of algorithmic policing technologies should occur in a manner that **errs on the side of caution** to avoid rights infringements of disadvantaged or marginalized individuals or groups.

- **Public interest legal standards and public sector control** should apply to commercial vendors that enter into contracts with government or law enforcement for algorithmic policing tools, where criminal jeopardy is at stake. Such initiatives might follow the model of the Saskatchewan Police Predictive Analytics Lab, which is developing its predictive analytics technology in-house

679 See e.g., "[F]or example, if one clicks on 'sexual offenses' in a city that does not provide this data, the resulting map will show no sexual offences in the searched area—which might suggest to the user that no such crimes occurred during the specified time frame, rather than that the data are not available." Teresa Scassa, "Police Service Crime Mapping as Civic Technology: A Critical Assessment" (2016) 5:3 International Journal of E-Planning Research 13 at 20.

680 See e.g. (in the context of crime mapping, but applicable where similar details are made publicly available, even if not visualized on a map), "Privacy considerations may also influence the mapping of other crime data. For example, some police forces choose not to map crimes of domestic violence or child sexual abuse for privacy reasons. Such crimes often occur within the home, and mapping, even to the 100-block level may lead to the identification of either the victim or the perpetrator (or to harmful incorrect assumptions about their identities)." *Ibid*.

681 *Ibid*.

682 For more details regarding the scope of mandatory disclosure obligations in respect of algorithmic policing technology, see Section 5.6.2 ("Non-Disclosure and the Right to Make Full Answer and Defence").

and in partnership with academic experts, under a university research ethics protocol.

- Law enforcement authorities must provide **notice in clear language** on public websites, whenever a decision will be informed by an algorithmic decision system. Further, individuals who have been affected by a government decision that was undertaken in whole or in part by an automated decision system must receive a **meaningful explanation** of how and why the decision was made.

### Recommendation 15: The federal government should expand the parliamentary reporting provisions under the Criminal Code that currently apply to only certain electronic surveillance methods.

The federal government should consider expanding parliamentary reporting requirements that are set out in the *Criminal Code* and that currently apply to live electronic surveillance of private communications. Under the existing framework, the federal and provincial governments must present annual reports to Parliament with information regarding authorizations to intercept private communications. The annual reports are prepared in cooperation with the RCMP and provincial and municipal police services. Updating these could, in theory, help the public to understand the use of new technologies.

Parliament should also consider expanding public reporting mechanisms so the mechanisms provide better context concerning the use of algorithmic policing technology. In particular, Parliament could compel the governments to include in the tabled annual report a narrative depiction of the specific kinds of technologies that have been adopted or are under consideration for adoption. This narrative might also discuss why such technologies are needed. Equivalent requirements could be mandated, through parliamentary reform, for the similar reports that are tabled annually by the provincial solicitors general. The benefit of expanding the type of information that is subject to public reporting is that such expanded reporting will enable legislatures, and the public, to hold governments and law enforcement agencies to account for algorithmic policing technologies, in their impacts and in their use of public funding.

### Recommendation 16: Privacy and human rights commissioners must be empowered and provided with sufficient funding and resources to initiate and conduct investigations into law enforcement's use of algorithmic policing technology.

Algorithmic policing technologies warrant focused oversight by privacy commissioners, who are particularly well-suited to assess the ways new technologies can unduly infringe on individuals' privacy. However, not all privacy commissioners in Canada currently have the authority to initiate investigations or audits in the absence of a complaint, which can prevent them from exercising their oversight role.[683]

683 For example, only the mandates of the privacy commissioners and ombudspersons in British Columbia, Alberta, Northwest Territories,

As such, all privacy commissioners should be empowered to initiate and conduct investigations in relation to police adoption and use of algorithmic policing technologies.

Provincial and federal human rights commissioners also play an important role in shining a light on the human rights issues that can develop with the use of algorithmic policing technology. Governments must ensure that these bodies are equipped with adequate resources to perform this task.[684] This form of investigative review could occur as a complaint-driven process, as a form of randomized audit, or as an investigation initiated on the commissioner's own authority in response to received information (such as details revealed through news reports or information provided by a party that is not a complainant).

**Recommendation 17: Law enforcement agencies must adopt and formally document in writing internal oversight and accountability mechanisms, best practices, and policies regarding the consideration, development, procurement, use, monitoring, auditing, and disbanding of algorithmic policing technologies.**

Law enforcement agencies should create documentation and provide training concerning any use of algorithmic policing technology, at every stage, from initial consideration to ongoing auditing to potential disbanding, of incorporating an algorithmic policing technology into operations. Based on research and interviews with law enforcement representatives, the formality and documentation of policies differed between agencies involved in algorithmic policing. In some cases, practices were governed by a formal research ethics board protocol, while in others, there was no formal documentation and best practices appeared to result from a single individual championing them. When putting written policies in place, law enforcement authorities should prioritize distilling *Charter* requirements developed throughout case law into clear written guidance for front-line officers.

Moreover, municipal chiefs of police should be required to publicly present their written policies to their oversight boards and city councils; all such presentations should be made open to the public and not moved to *in camera* meetings. Provincial and federal policing bodies should be required to similarly publish policies; these policies should be tabled by either public safety ministers or attorneys general in either the legislature or relevant legislative committee. These policies should be submitted prior to any implementation of an algorithmic policing technology, and any new class of technologies (such as person-based predictive policing models) should be explicitly and specifically addressed in these plans.

---

Nunavut, and Newfoundland expressly include the authority to initiate investigations or audits of public bodies in respect of compliance with applicable privacy legislation. The mandates of other provinces and territories focus on complaint-driven investigations only.

684 See e.g., Ontario Human Rights Commission, *A Collective Impact: Interim report on the inquiry into racial profiling and racial discrimination of Black persons by the Toronto Police Service* (November 2018). <http://www.ohrc.on.ca/en/public-interest-inquiry-racial-profiling-and-discrimination-toronto-police-service/collective-impact-interim-report-inquiry-racial-profiling-and-racial-discrimination-black>; Office of the Privacy Commissioner of Canada, "Cell site simulators used by RCMP not capable of intercepting private communication", (September 2017), <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2016-17/pa_20170816_rcmp/>.

Law enforcement authorities should also adopt and document review and audit mechanisms involving routine monitoring and random audits of system access logs. Specifically, these mechanisms would focus on uncovering unusual behaviour and breaches of the policies and procedures that govern the use of algorithmic policing technology. Officers would be made aware that their activities are subject to audit or monitoring and that they may be called upon to justify their use of the system.[685] Most law enforcement services already house internal professional standards departments that handle public complaints and conduct internal investigations.

### Recommendation 18: Governments should make funding available for research to develop the availability of independent expertise on the human rights implications of algorithmic policing technologies.

Federal and provincial governments should make public funding available for individuals to develop expertise at the nexus between algorithmic technology, criminal justice, and human rights. This funding should include, for example, federal funding through the Office of the Privacy Commissioner of Canada, the Natural Sciences and Engineering Research Council (NSERC), or the Social Sciences and Humanities Research Council (SSHRC). If algorithmic policing technologies continue to be used in the criminal justice system, due process and remedial rights will likely be hindered in practice by the lack of available expertise to test and challenge the validity of algorithmic methods. Areas to be examined should include the overall reliability of the algorithm and any training and operational input data used, maintenance practices after the algorithm has been put into use, and the outputs of the algorithm (e.g., testing for arbitrary or inaccurate results and the efficacy of the tool in comparison with non-algorithmic methods).

### Recommendation 19: Governments must ensure adequate assistance is available for low-income and unrepresented defendants in order to retain expert witnesses in criminal proceedings.

To bring human rights claims about the use of algorithmic policing technology before judges, defendants will require access to experts to potentially serve as witnesses to assess the accuracy of algorithmic policing technologies. In many cases, defendants do not qualify for legal aid representation but still cannot retain either counsel or experts. In cases where the defendant is unrepresented, heightened obligations fall on the court and the Crown prosecutor to ensure the defendant has access to a fair trial. Governments should provide funding to legal aid organizations to ensure that public interest technologists are available to serve as expert witnesses. This funding could be paid through the legal aid funds that are distributed either through legal aid processes or, alternatively, through court-ordered funds made available to retain an expert in cases where defendants cannot afford to retain counsel

685 As an example of an internal audit process, the Information and Privacy Commissioner of Ontario recommends that police services in Ontario adopt regular audit processes in relation to the use of automated licence plate recognition technology: Information and Privacy Commissioner of Ontario, "Guidance on the Use of Automated License Plate Recognition Systems by Police Services", (July 2017), <https://www.ipc.on.ca/wp-content/uploads/2016/09/alpr_systems.pdf>.

and are not directly eligible for legal aid. Assistance may also entail training Crown prosecutors and courts about *Charter* issues and evidentiary issues that can arise in cases where law enforcement authorities have relied on algorithmic policing technology.

**Recommendation 20: Governments and law enforcement agencies must by default make the source code of algorithmic policing technologies publicly available or, where that is impossible for public interest reasons, confidentially available to public bodies and independent experts for the purposes of algorithmic impact assessments, preprocurement review, security testing, auditing, investigations, and judicial proceedings.**

Government and law enforcement agencies that develop their own algorithmic policing technologies—whether in-house or with private vendors—must make the source code and related details of such technologies publicly available in machine-readable and human-readable forms. Applying open software licensing in this context may be appropriate on the basis that such technologies are publicly funded and should be available to members of the public for purposes of review or research.[686]

If extenuating circumstances engage the public interest to an extent that outweighs the importance of disclosing the source code and related details of algorithmic policing technologies to the public, the information must still be accessible to oversight bodies and independent experts on a confidential basis (where the source code itself remains confidential, but findings and rulings are public) in order to complete impact assessments, procurement reviews, security testing, auditing, investigations, or court proceedings.

Governments and law enforcement agencies that acquire off-the-shelf algorithmic policing technologies from commercial vendors must include open-source code review as a condition of all procurement contracts, including the waiving of trade secret and related proprietary rights where the review, testing, oversight, and auditing mechanisms listed above are concerned. Possible agencies that could play an oversight role with respect to ensuring source code transparency, review, testing, and auditing include the Office of the Privacy Commissioner and the Canadian Centre for Cyber Security.

## 6.6. Conclusion

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. Multiple law enforcement agencies in Canada have used, developed, procured, or tested a range of algorithmic policing technologies. These include both location-focused and person-focused algorithmic policing technologies ('predictive policing' technologies) as well as algorithmic surveillance technologies.

686 For more details, see "IN FOCUS #7: Open Source Algorithms and Source Code Review" in Section 5.6.1 ("Informational Barriers to Due Process: Algorithmic Transparency and Private Sector Influence").

The public interest demands concerted democratic engagement and legal reform that targets the use of algorithmic policing technologies in the criminal justice system. Canadian lawmakers and law enforcement authorities should draw lessons from jurisdictions where such technologies have already long been in use. In the United States, the Chicago Police Department, the New Orleans Police Department, and the Los Angeles Police Department have all stepped back from their use of much-criticized algorithmic policing technologies and have shut down multiple programs.[687] The City of Santa Cruz, California, is presently considering a full ban on all predictive policing technologies.[688] Other cities, such as San Francisco and Oakland, California, and Boston and Somerville, Massachusetts, have implemented moratoriums on the use of facial recognition technology. Independent studies and audits of algorithmic policing technologies used in the United States have demonstrated that numerous risks and harms have already transpired due to relatively unchecked uses of algorithmic surveillance tools or the deployment of police resources on the basis of algorithmic predictions derived from statistical analysis.[689]

Replicating, amplifying, or automating policing methods of the past through police algorithms further risks entrenching a hostile, distrusting, and antagonistic relationship between the Canadian law enforcement system and the public. Civil liberties and fundamental freedoms are detrimentally infringed upon when police indiscriminately use these technologies or when such technologies are used in the absence of adequate constitutional safeguards. The balance between criminal law enforcement objectives and protection for fundamental freedoms is already often off-kilter when it comes to marginalized communities, particularly Black and Indigenous communities. Adopting algorithmic policing technologies threatens to further undermine the civil liberties and fundamental freedoms of such communities and their individual members, curtailing their human dignity and autonomy as well as their ability to fully participate in public life or benefit from equal protection of the law.

The wielding of algorithmic technologies within the powerful apparatus of policing surveillance and law enforcement systems has the potential to cause real and significant harm to individuals and communities, to perpetuate unfairness and injustices already meted out by the criminal justice system, and to cause a fundamental reorienting of policing methods in ways that will challenge conventional understanding of *Charter* rights and remedies. For instance, the use of predictive policing

687 See e.g. Ali Winston, "New Orleans ends its Palantir predictive policing program", *The Verge* (15 March 2018) <https://www.theverge.com/2018/3/15/17126174/new-orleans-palantir-predictive-policing-program-end>; Jeremy Gorner & Annie Sweeney, "For years Chicago police rated the risk of tens of thousands being caught up in violence. That controversial effort has quietly been ended", *Chicago Tribune* (24 January 2020), <https://www.chicagotribune.com/news/criminal-justice/ct-chicago-police-strategic-subject-list-ended-20200125-spn4kjmrxrh4tmktdjckhtox4i-story.html>; and Mark Puente, "LAPD to scrap some crime data programs after criticism", *Los Angeles Times* (5 April 2019) <https://www.latimes.com/local/lanow/la-me-lapd-predictive-policing-big-data-20190405-story.html>.

688 Avi Asher-Schapiro, "In a U.S. first, California city set to ban predictive policing", *Reuters* (17 June 2020) <https://uk.reuters.com/article/usa-police-tech/corrected-refile-feature-in-a-us-first-california-city-set-to-ban-predictive-policing-idUKL8N2DO3LD>.

689 For example, when announcing the decommissioning of CPD's "Strategic Subject List" (a person-focused algorithmic policing technology), the Inspector General explained that this decision was made due to "the unreliability of risk scores and tiers; improperly trained sworn personnel; a lack of controls for internal and external access; interventions...which may have attached negative consequences to arrests that did not result in convictions; and a lack of a long-term plan to sustain the [models]": Sam Charles, "CPD decommissions 'Strategic Subject List'", *Chicago Sun Times* (27 January 2020), <https://chicago.suntimes.com/city-hall/2020/1/27/21084030/chicago-police-strategic-subject-list-party-to-violence-inspector-general-joe-ferguson>.

technologies alters traditional policing methods by using bulk, historic policing data sets in a way that was never contemplated or intended by justice system actors, including those who formulated current constitutional safeguards. The use of predictive policing technologies can subject individuals to heightened police suspicion, scrutiny, detention, or more, based not on the individual's own actions, but on generalizations drawn from broad, community- or national-level historic patterns.

As examples of predictive policing technologies in Canada, the Vancouver Police Department (VPD) uses a location-focused algorithmic policing technology associated with their GeoDASH system, while the Saskatchewan Police Predictive Analytics Lab (SPPAL) is developing person-focused algorithmic policing tools that are intended to conduct risk assessments to determine potential victims and potential repeat or violent offenders. While each of these programs include built-in measures that attempt to mitigate the harms and risks identified above, they have incorporated these measures voluntarily. Not all law enforcement agencies who adopt algorithmic or predictive policing technologies may opt to or proactively implement adequate safeguards; thus, the constitutional and human rights dangers associated with such technologies continue to loom large across Canada. Fundamental human rights and civil liberties cannot be left to the individual discretion of local law enforcement agencies to uphold.

Other police services throughout Canada may also be using or developing predictive policing technologies outside of public awareness. Many of the FOI requests submitted for this report were met with responses from law enforcement authorities that claimed privilege as justification for non-disclosure. In other cases, law enforcement agencies did not provide any response to the submitted FOI request. The authors of this report also previously submitted an FOI request to the TPS, which included a broad request for records relating to facial recognition during a time period that included March 2018. The TPS did not provide any information or responsive documents regarding the use of facial recognition, despite the fact that it is now known that the police service spent $451,718 on a facial recognition system during the time period that was the subject of the FOI request.[690]

Some law enforcement agencies are not currently engaging in predictive policing, but they are already equipped with the technological capability to do so or may consider engaging in the future. For instance, the Calgary Police Service (CPS) has the ability to conduct person-focused predictive policing through its Palantir Gotham software, though a member of law enforcement in Calgary stated that the system is currently only used for non-algorithmic data management and analysis. In 2018, an article by a representative of Environics Analytics, which collaborates with the TPS on data-driven policing initiatives, stated that one of the goals of the organizations' collaboration was to develop algorithmic models that would identify areas considered to be 'high crime.' According to research interview findings for this report, the TPS does not currently engage in algorithmically driven predictive policing nor does it intend to adopt predictive policing technologies immediately. However, this position does not rule out the possibility that the TPS may consider doing so in the future, and the agency is interested in using data to inform policing decisions about property crime and gun violence.

690 Phillip Lee-Shanok, "Privacy advocates sound warning on Toronto police use of facial recognition technology", *CBC News* (30 May 2019), <https://www.cbc.ca/news/canada/toronto/privacy-civil-rights-concern-about-toronto-police-use-of-facial-recognition-1.5156581>.

The algorithmic surveillance technologies described throughout this report also risk producing seismic changes to the way in which law enforcement authorities monitor and surveil the public in Canada. Canadian law enforcement relies on several different kinds of such technologies. Facial recognition technology, automated licence plate readers, and social media surveillance software have been implemented by numerous law enforcement authorities across the country. Algorithmic processing allows law enforcement to make fundamentally new uses of data that was previously collected on a relatively uncontested or unregulated basis or permitted to be collected without contemplation of today's technological realities (e.g., when mug-shot databases or CCTV video footage that contain data collected under previous regimes are fed to facial recognition technology for law enforcement purposes). Algorithmic surveillance technology tends to aggregate and analyze personal information from public spaces, such as the outdoors, at public events like mass protests, or in online environments. The prospect of a further ballooning sphere within which police can indiscriminately surveil members of the public should provoke significant concern, particularly if these technologies are not subjected to necessary constraints and oversight mechanisms.

Facial recognition technology appears to be undergoing rapid adoption by Canadian law enforcement. The NEC Corporation's NeoFace Reveal tool is currently in use by the CPS and was pilot-tested in early 2019 by the Ottawa Police Service. The TPS is also using a facial recognition technology that is either NeoFace Reveal or another product by the NEC Corporation. Moreover, media reports in early 2020 revealed that the controversial facial recognition tool, Clearview AI, was used or tested by all of the RCMP, the CPS, the Edmonton Police Service, and multiple Ontario police services including the TPS and those in Peel, Halton, Ottawa, Durham, Niagara, and Hamilton. Given the demonstrable human rights risks of facial recognition tools, in addition to their unreliability, police services should halt any further use or adoption of facial recognition technologies 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.

Canadian law enforcement agencies are also widely engaged in social media surveillance. The RCMP currently uses social media monitoring software known as Social Studio, provided by Carahsoft and developed by Salesforce. The RCMP also issued a public tender in April 2020, seeking even more sophisticated social media surveillance services than those already in use—despite an ongoing internal review of the legality of its current social media surveillance operations. The CPS and the TPS have both conducted algorithmic social media surveillance in the past, using the Media Sonar tool created by a company in London, ON. Both police agencies stopped using this software after Twitter and Facebook banned it from their respective platforms (including Instagram) because Media Sonar promoted use of its technology to target social movements such as Black Lives Matter. Additionally, the CPS engages in algorithmic social network analysis, using a system that imports networked relational data from Palantir's software into IBM's i2 Analyst Notebook, to identify key players in given social networks. Accountability and oversight mechanisms are critical to bring the use of these technologies within constitutional limits and to protect the rights to freedom of expression, equality, and privacy, which are undermined by algorithmic police surveillance and monitoring in online, outdoor, or otherwise public environments. Moreover, law enforcement agencies appear to be using additional technologies in ways that violate more traditional constitutional boundaries. Specifically, this report uncovered information suggesting that the Ontario Provincial Police and Waterloo Regional Police Service may be unlawfully

intercepting private communications in online private chat rooms through reliance on another form of social media surveillance technology known as the ICAC Child On-line Protection System (ICACCOPS).[691]

Although algorithmic policing technologies remain an emerging issue area for the Canadian legal system, analogous lessons have already been learned in the criminal justice system in the wake of systemic failures flowing from flawed novel scientific, technological, or investigative methods. The use of "faulty forensic procedures, unreliable science and flawed expert opinion testimony have been factors in a number of wrongful conviction cases in Canada,"[692] which have resulted in numerous public inquiries that have endeavoured to identify and establish methods to prevent recurring failures.[693] These inquiries have repeatedly underscored the necessity of extreme caution when it comes to reliance on novel or otherwise untested methods in the criminal justice system.

Assessing algorithmic policing technologies through a human rights lens has shown how their use by law enforcement can cause a myriad of civil liberties violations under the Canadian constitution and international human rights law. Specifically, the use of algorithmic policing technologies acutely endangers the following human rights:

- **the right to privacy** (through issues such as indiscriminate surveillance, eroding reasonable expectation of privacy in public and online spaces, the accuracy of data inferences, and data-sharing between law enforcement and other governmental agencies);
- **the rights to freedom of expression, peaceful assembly, and association** (through issues such as undermining anonymity of the crowd and targeting social movements and marginalized communities);
- **the right to equality** (through issues such as algorithmic bias perpetuating discriminatory feedback loops, heightened data visibility of socio-economically disadvantaged individuals, and math-washing systemic discrimination curtailing possibilities of structural reform to address root issues);
- **the right to liberty and to be free from arbitrary detention** (through issues such as generalized statistical inferences supplanting individualized suspicion, and risks of automation bias); and

691 See discussion of the ICACCOPS tool and related legal analysis in Section 4.3.2 ("Social Media Surveillance").

692 Public Prosecution Service of Canada, "Prevention of Wrongful Convictions", Public Prosecution Service of Canada Deskbook (September 2014), <https://www.ppsc-sppc.gc.ca/eng/pub/fpsd-sfpg/fps-sfp/tpd/p2/ch04.html#fnb37-ref>.

693 The Hon. Commissioner Stephen T. Goudge, Inquiry into Pediatric Forensic Pathology in Ontario (Toronto, 2008); The Hon. Justice Cory, The Report of the Commission of Inquiry regarding Thomas Sophonow (September 2001), <https://digitalcollection.gov.mb.ca/awweb/pdfopener?smd=1&did=12713&md=1>; The Hon. Fred Kaufman, C.M., Q.C., Report of the Kaufman Commission on Proceedings Involving Guy Paul Morin (1998).

- **the right to due process and to a remedy** (through issues such as lack of transparency, accountability, and oversight mechanisms, such as notice and disclosure requirements).

Among the numerous constitutional and human rights concerns that were identified throughout this report, several particularly prominent dangers emerged that demonstrate a fundamental incompatibility between the use of algorithmic policing technologies and constitutional and human rights protections. These incompatibilities are a glaring red light that law enforcement agencies, justice system participants, and policy-makers must heed: if they do not steer the course of justice to avoid these treacherous crags, historical inequities will continue to occur or worsen, and the Canadian justice system will be cast into doubt at best or sink into outright disrepute at worst. To mitigate the most harmful legal and policy implications associated with algorithmic policing technologies, the criminal justice system must take into account the following three issues in particular.

First, systemic bias and tainted data in historic police data sets pose a particularly critical problem for person-focused and location-focused algorithmic technologies. These kinds of algorithmic policing tools produce outputs that purport to forecast who will commit a criminal offense, how likely someone is to commit a criminal offence within a given time, or where and when certain types of criminal offenses may take place. If all of the most common sources of historic police data are laden with systemic bias and inaccuracies, the integrity of algorithmic outputs obtained through the use of that data will be similarly compromised. As a result, this report emphasizes the need for a moratorium on the use of historical police data in the training or operating of police algorithms and the need to establish, simultaneously, a judicial inquiry into such usage. Where communities have been subjected to discriminatory treatment based on *Charter*-protected grounds, data collected about them must be considered unfit for use in training algorithms that inform police decision making.

Second, relying on predictive forms of algorithmic policing technologies or unreliable algorithmic surveillance technologies to justify interfering with an individual's liberty (e.g., through arrest or detention) is incompatible with constitutional and human rights law. Algorithmic predictions are, by nature, generalized to the extent that they fail to meet the requirements of specific and individualized suspicion to justify impeding a person's liberty. This fundamental incompatibility between algorithmic policing technologies and the right to liberty must foreclose the use of such technology in most, if not all, front-line policing work in order to prevent the occurrence of detentions, arrests, or charges on the basis of unconstitutional grounds obtained from algorithmic predictions or otherwise unreliable algorithmic technologies.

Third, the increasing use of algorithmic surveillance technologies by law enforcement authorities in Canada threatens the right to privacy and the *Charter*-protected fundamental freedoms of expression and association. The Canadian legal system presently lacks sufficient safeguards to ensure that algorithmic surveillance techniques conform with constitutional requirements and are subject to robust and necessary regulatory, judicial, and parliamentary oversight mechanisms. Unrestricted use of algorithmic surveillance technologies has great potential to damage the ability to exercise fundamental freedoms and civil liberties, thereby undermining a free and democratic society. Combined with the lack of oversight and accountability mechanisms, including compliance with

limits established by the principles of necessity and proportionality, the use of such technologies currently lacks legal justification.

In conclusion, the legal analysis and review of Canada's inadequate oversight systems in this report demonstrate that the vast majority of the examined algorithmic policing technologies should not be in use by any Canadian law enforcement authority. Theoretically, there might be some very narrow and specific uses of algorithmic policing technologies that do not explicitly offend constitutional and human rights law, assuming they are even sufficiently reliable for use. However, it is extremely difficult to identify what those rare technologies or use cases might be without public transparency and fulsome information from law enforcement agencies that includes detailed disclosures about what technologies they are considering, developing, or adopting; whether any such technologies have been subject to independent scientific validation; and how any such technologies would be used and internally regulated. Nevertheless, as it stands, there are many red flags that warn of significant danger ahead for governments, police services, and—most of all—the public and members of historically marginalized communities who will bear the brunt of negative impacts that result from the use of algorithmic policing technologies. It is for this reason that Part 6 has set out a short list of priority recommendations that emphasizes the need for targeted moratoriums and clear limits with respect to the most problematic uses, from a constitutional and human rights perspective, of algorithmic policing technologies. It is also for this reason that this report emphasizes the need to meaningfully consult with and listen to historically marginalized communities disproportionately impacted by the Canadian criminal justice system, in determining how—or whether at all—to move forward with adopting algorithmic policing technologies in Canada.

With respect to marginalized communities that have historically been subjected to systemic discrimination in the criminal justice system, algorithmic policing technologies raise compelling questions regarding their *collective* interests and rights. This report has predominantly focused on situations in which an *individual*'s civil liberties or human rights may be violated by the use of such technologies. However, where an individual is detrimentally affected by an algorithmic policing technology by virtue of their membership in a group characterized by a section 15 protected ground and specifically against a socio-political and historical context of that group being over-policed in Canada, such technology also raises issues about its material and systemic impacts on the *collective* privacy, liberty, and equality rights of that *community as a whole*. Thus, individual remedies may not suffice where the violative impacts of algorithmic policing technologies are both distributive and communal, yet concentrated within specific communities with a history of being subjected to systemic discrimination. The nexus between individual and collective human rights with respect to historically marginalized communities, and particularly the role of the right to equality as it intersects with other *Charter* protections, warrants further study in research investigations and should be examined as part of the recommended judicial inquiry.[694]

694 See e.g., Linnet Taylor, Luciano Floridi & Bart van der Sloot, eds, Group Privacy: New Challenges of Data Technologies (Cham, Switzerland: Springer International Publishing, 2017); Christopher Parson, "Beyond Privacy: Articulating the Broader Harms of Pervasive Mass Surveillance" (2015) 3:3 Media and Communication 1 (discusses how surveillance can have both personal and collective rights implications and demonstrates that focusing exclusively on either one prevents an adequate assessment of the aggregate harms); Jane Bailey, "Towards an Equality-Enhancing Conception of Privacy" (2008) 31:2 Dalhousie LJ 267.

Given the myriad perils that algorithmic policing technologies pose to human rights, it is deeply questionable whether such technologies are worth their substantial cost (in procurement, development, testing, implementation, monitoring, auditing, and defending challenges to their use or results). Algorithmic policing technologies would also come at the cost of diverting further funding and public resources away from more urgent priorities to impacted communities and more effective approaches to community safety. Numerous questions are being raised across the country regarding the appropriate role of police services, and there is increasing recognition that the scope and budget of policing has ballooned far beyond proportion and ill-fittingly into areas such as mental health treatment, counselling, student well-being, and related social services—with the result of wrongful criminalization of individuals who require such services. This report has also discussed the connection between underlying factors of marginalization and the tendency to be disproportionately criminalized and unjustly and unnecessarily drawn into the criminal justice system. Algorithmic policing technologies would do nothing to address the root causes of societal problems that are systemically and detrimentally intertwined with the criminal justice system, including homelessness, inadequate mental health and addiction services, underfunded education systems, inadequate community resources to support struggling youth and violence prevention, lack of health care, unemployment, or Canada's legacy of colonialism and associated intergenerational trauma.

Any analysis of algorithmic policing technologies must begin with evaluating their impact on constitutional and human rights. This report has demonstrated that some uses and some types of such technologies are fundamentally incompatible with the *Canadian Charter of Rights and Freedoms*, which make it largely irrelevant whether the technology is reliable or has a discernible benefit for law enforcement objectives. The Canadian government and law enforcement authorities have a constitutional imperative to consider and prevent harms that would arise from further entrenching existing discriminatory patterns of policing and incarceration, particularly with respect to historically marginalized communities protected by section 15 of the *Charter*. Whatever law enforcement agencies' interest may be in having access to algorithmic policing technologies' capabilities, that interest does not and must not override the fundamental rights and freedoms that the constitution guarantees to every individual, including the rights to privacy, equality, and liberty, nor should that interest take precedence over the values such rights and freedoms inherently uphold, such as human dignity and autonomy.

Successive inquiries and reviews have emphasized that law enforcement agencies and the Canadian government writ large must act to obviate inequities in the criminal justice system and throughout society generally, particularly with respect to historically marginalized and disenfranchised individuals and groups who have been the most profoundly and unjustly impacted. Calls to undertake this work are not new or a novel response to advances in policing techniques, technological or otherwise. Moving towards algorithmic policing technologies—whether for mass surveillance, forecasting crime, or risk assessment of individuals—or otherwise further entrenching a 'big data' model of policing in Canada risks further perpetuating layers of systemic discrimination in the criminal justice system to an even greater and potentially irreversible degree. Such perpetuation would occur despite the broad consensus that has emerged among justice system oversight bodies and the public's recognition of the need to end and redress the disproportionate policing and incarceration of communities that have been the subject of historic and ongoing systemic discrimination, including Black and Indigenous

individuals. Rather than redress excessive policing and incarceration, algorithmic policing technologies may, instead, irrevocably encode additional layers of inequality and discrimination into the criminal justice system. Such technologies may, at the same time, mask this very injustice through maintaining a thin veneer of mathematical 'neutrality'. Whatever modest benefit algorithmic policing technologies might theoretically obtain for law enforcement authorities, public resources should instead be devoted to addressing the root causes of injustices examined through the lens of intersectional evidence-based policy-making and to ending the legacy of preventable tragedy, oppression, and systemic harm that is reflected in the history of Canada's criminal justice system.

# Appendix A: Sample FOI Request

Date

Name
Title
Address

Dear [FOI or ATIP Officer],

I am writing to file a request for records pursuant to sections 4(1) and 6 of the Canadian *Access to Information Act*, R.S., 1985, c. a-1. Specifically, I am requesting the following:

1. **All records**—including but not limited to draft and final versions of policies, guidelines, meeting agendas, meeting minutes or notes, briefing notes, technical specifications, training documents, bulletins, memoranda, executive summaries, slide decks, handouts, handwritten notes, preparatory notes, notes from phone calls, faxes, reports, diagrams, studies, surveys, contracts, budgets, financial documents, and all internal and external correspondence, including e-mail—produced **between January 1, 2013 and November 1, 2018**, that contain **discussion of or reference to the use of:**
    a. **Algorithms, algorithmic decision-making, algorithmic analytics, algorithmic analysis, or automated analysis;**
    b. **Algorithmic risk assessment or algorithmic risk analysis;**
    c. **Predictive analytics, predictive analysis, predictive modelling, predictive intelligence;**
    d. **Machine learning, deep learning, neural networks, artificial intelligence, "big data"- or data-driven intelligence;**
    e. **Social media monitoring, social media analytics; and/or**
    f. **Facial recognition**

**For the purposes of collecting, managing, analyzing, or assessing data and information related to monitoring, investigating, or responding to criminal activity, suspected criminal activity, and/or predicted criminal activity.**

2. **All records**—including but not limited to draft and final versions of policies, guidelines, meeting agendas, meeting minutes or notes, briefing notes, technical specifications, training documents, bulletins, memoranda, executive summaries, slide decks, handouts, handwritten notes, preparatory notes, notes from phone calls, faxes, reports, diagrams, studies, surveys, contracts, budgets, financial documents, and all internal and external correspondence, including e-mail—produced **between January 1, 2013 and November 1, 2018**, that contain **discussion of or reference to the use of:**
    a. **Algorithms, algorithmic decision-making, algorithmic analytics, algorithmic analysis, or automated analysis;**
    b. **Algorithmic risk assessment or algorithmic risk analysis;**
    c. **Predictive analytics, predictive analysis, predictive modelling, predictive intelligence;**
    d. **Machine learning, deep learning, neural networks, artificial intelligence, "big data"- or data-driven intelligence;**
    e. **Social media monitoring, social media analytics; and/or**
    f. **Facial recognition**

**For the purposes of making determinations about an offender or suspected offender, accused, defendant, prisoner, or convicted individual, including but not limited to for purposes of correctional services, remand, bail, sentencing, inmate security classification, risk assessment, or parole.**

3. **All records**—including but not limited to draft and final versions of policies, guidelines, meeting agendas, meeting minutes or notes, briefing notes, technical specifications, training documents, bulletins, memoranda, executive summaries, slide decks, handouts, handwritten notes, preparatory notes, notes from phone calls, faxes, reports, diagrams, studies, surveys, contracts, budgets, financial documents, and all internal and external correspondence, including e-mail—produced **between January 1, 2013 and November 1, 2018**, that contain discussion of or reference to **any of the following:**
    a. **Predictive policing**
    b. **Proactive policing**
    c. **Intelligence-led policing**
    d. **Algorithmic policing**

e. **Big data policing**
f. **Predicting criminal "hot spots"**
g. **Policing algorithms**
h. **Evidence-based policing**
i. **Proactive patrol management**

If possible, please send any meaningful portion of responses to any of the above items as soon as they are complete, rather than waiting until all of the information for the entirety of this request has been compiled.

**If a full response will take more than thirty days to complete, please send, as an initial interim disclosure, a list of the documents that will be disclosed in response to the request**.

I would prefer to receive all records electronically, in a readable computer format. Please send them by e-mail to the following two addresses:

cynthia@citizenlab.ca
yolanda.song@utoronto.ca

Please find enclosed the $5.00 fee. I look forward to a response in the next thirty days, as provided for in section 7(a) of the *Act*. I would also greatly appreciate acknowledgement of your having received this request, if the response will take more time.

Please feel free to contact me if any clarification is needed or if it would help to fulfill or expedite the response to this request. I would be pleased to discuss further and assist.

Yours truly,