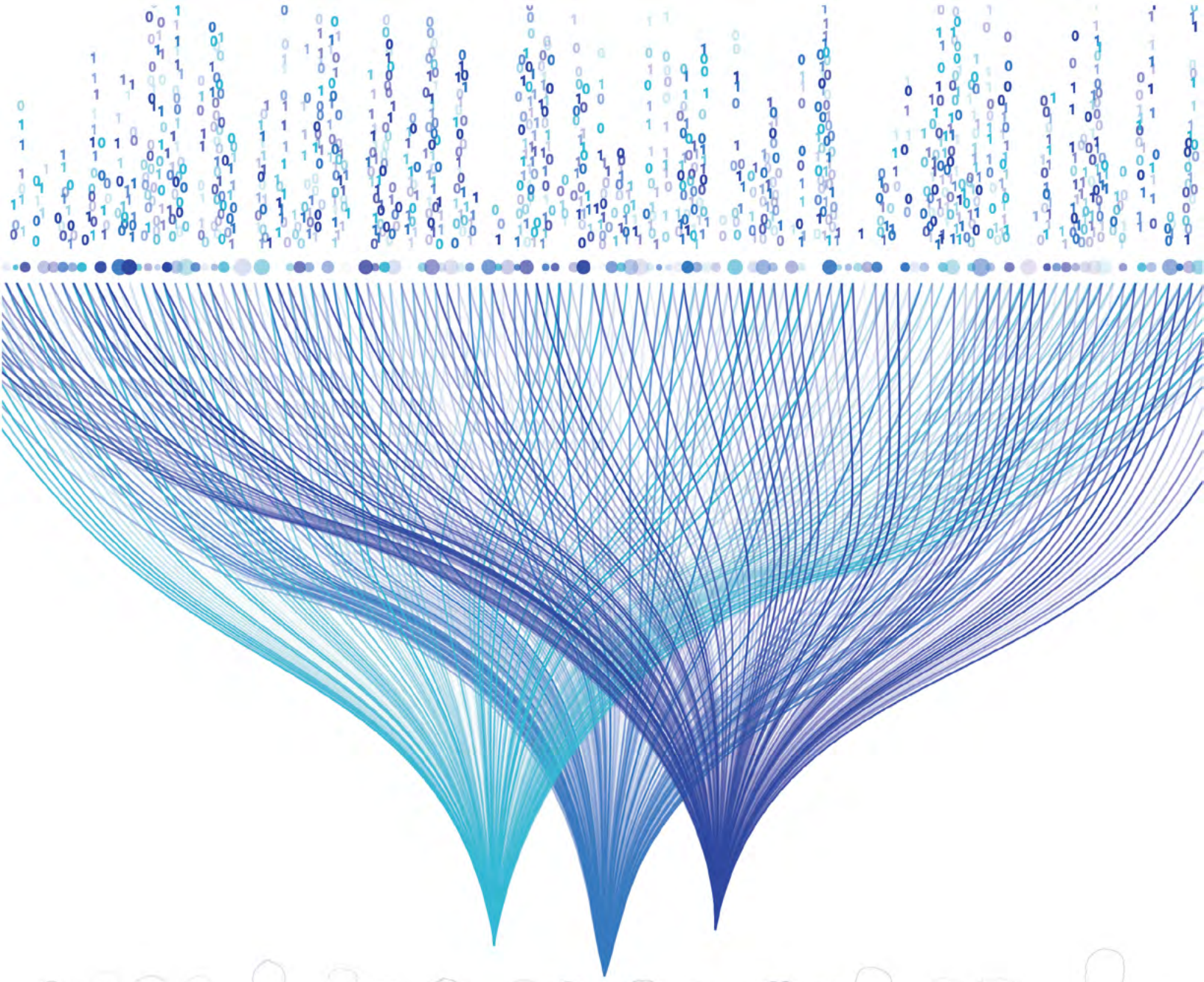


Law Commission of Ontario

AI IN CRIMINAL JUSTICE PROJECT | PAPER 2

Law Enforcement Use of AI

April 2025

LAW COMMISSION OF ONTARIO
COMMISSION DU DROIT DE L'ONTARIO

About the Law Commission of Ontario

The Law Commission of Ontario (LCO) is Ontario's leading law reform agency.

The LCO provides independent, balanced, and authoritative advice on complex and important legal policy issues. Through this work, the LCO promotes access to justice, evidence-based legislation and policies, and public engagement on important law reform issues. The LCO is independent of stakeholder interests and is committed to a public interest perspective for every project.

The LCO has considerable experience analyzing AI regulation in the Canadian justice system. Recent LCO reports and submissions addressing these issues include:

- Human Rights AI Impact Assessment (with the Ontario Human Rights Commission, 2024)
- Submission to Government of Ontario Re Bill 194 (2024)
- *Accountable AI* (2022)
- *Regulating AI: Critical Issues and Choices* (2021)
- *Legal Issues and Government AI Development* (2021)
- The Rise and Fall of Algorithms in the American Justice System: Lessons for Canada (2020)

More information about the LCO and this project is available at: https://www.lco-cdo.org.

Author

Ryan Fritsch, Counsel, Law Commission of Ontario

Series Editors

Nye Thomas, Executive Director, LCO
Ryan Fritsch, Counsel, LCO

The LCO AI In Criminal Justice Project Paper Series

Paper 1 Introduction and Summary: LCO AI in Criminal Justice Project
Nye Thomas, Executive Director, LCO
Ryan Fritsch, Counsel, LCO

Paper 2 Use of AI by Law Enforcement
Ryan Fritsch, Counsel, LCO

Paper 3 AI and the Assessment of Risk in Bail, Sentencing, and Recidivism
Armando D'Andrea, Staff Lawyer, Provincial Office, Legal Aid Ontario
Gideon Christian, Professor of Law, Faculty of Law, University of Calgary

Paper 4 AI at Trial and on Appeal
Paula Thompson, Strategic Initiatives, Ministry of the Attorney General
Eric Neubauer, Defense Counsel, Neubauer Law, and Co-Chair, Criminal Lawyers Association Technology Committee

Paper 5 AI and Systemic Oversight Mechanisms in Criminal Justice.
Brenda McPhail, Senior Technology & Policy Advisor, Information and Privacy Commissioner of Ontario
Marcus Pratt, Senior Advisor, Policy Department, Legal Aid Ontario, and Chair of the LAO Test Case Committee
Jagtaran Singh, Legal Counsel Ontario Human Rights Commission

Annex A Executive Summary and Consultation Questions

Annex B Project Case Studies

Project materials are available online: https://www.lco-cdo.org/CrimAI.

Student Researchers

Thurka Brabaharan
Dixon Emanuel
Nouran Hamzeh
Shahmurad Lodhi
Masha Michouris
John Nyman
Ani Semanjaku

External Advisory Committee

Alpha Chan, Chief Information Security Officer, Toronto Police Services

Marco Galluzzo, Office of the Chief Justice, Ontario Superior Court of Justice

Rosanna Giancristiano, Director, Court Operations, Ministry of the Attorney General

Rosemarie Juginovic, Office of the Chief Justice, Ontario Superior Court of Justice

Associate Professor Daniel Konikoff, Department of Sociology, University of Alberta

Michelina Longo, Director, External Relations, Ministry of the Solicitor General

Jessica Mahon, Policing Standards Section, Ministry of the Solicitor General

Jane Mallen, Ministry of the Attorney General and LCO Board of Governors

Elena Middelkamp, Crown Law Office Criminal, Ministry of the Attorney General

Savio Pereira, Policing Standards Section, Ministry of the Solicitor General

Professor Ben Perrin, Faculty of Law, University of British Columbia

Michael Swinburne, Senior Policy Advisor, Canadian Human Rights Commission

Professor David Murakami Wood, Department of Criminology, University of Ottawa

Disclaimer

The analysis, findings, and recommendations in this paper do not necessarily represent the views of the LCO's funders, supporters, Advisory Committee members, or Issue Paper authors.

The analysis, findings, and recommendations in the project Issue Papers do not necessarily represent the views of the LCO, its funders, supporters, or Advisory Committee members.

Citation

Law Commission of Ontario, ***Use of AI by Law Enforcement: Paper 2 in the LCO AI in Criminal Justice Project*** (Toronto: April 2025).

Contact

Law Commission of Ontario
2032 Ignat Kaneff Building
Osgoode Hall Law School, York University
4700 Keele Street, Toronto, ON, M3J 1P3

Tel: (416) 650-8406
E-mail: LawCommission@lco-cdo.org
Web: https://www.lco-cdo.org
LinkedIn: https://linkedin.com/company/lco-cdo
Bluesky: @lco-cdo.bsky.social
X: @LCO_CDO
YouTube: @lawcommissionofontario8724

Funders

Financial support is provided by the Law Foundation of Ontario, the Law Society of Ontario, and Osgoode Hall Law School. The LCO is located at Osgoode Hall Law School in Toronto.

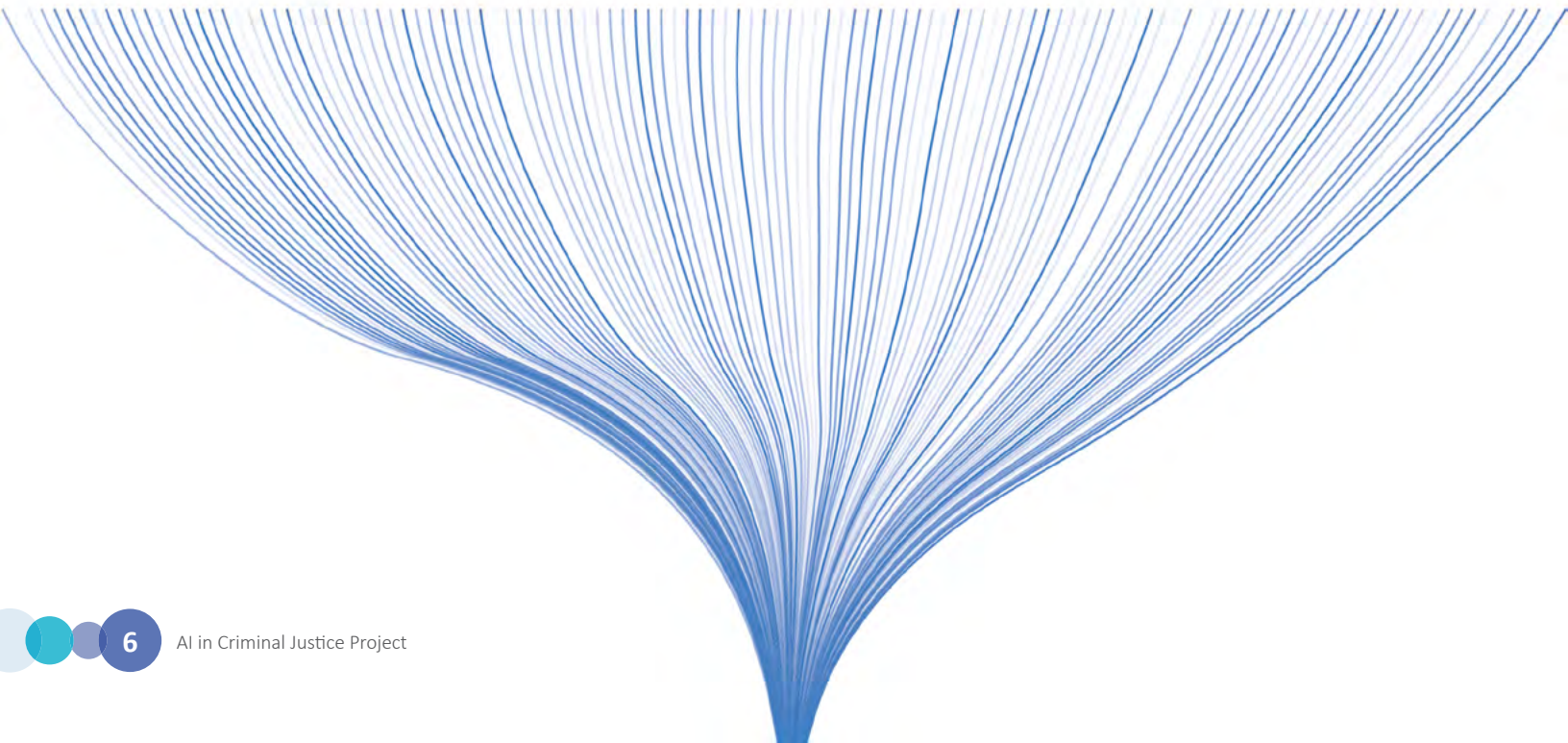
The Law Foundation of Ontario
Advancing access to justice

Law Society of Ontario | Barreau de l'Ontario

OSGOODE HALL LAW SCHOOL | YORK UNIVERSITÉ UNIVERSITY

Layout and Design by 12thirteen.

Contents



1. Introduction

1.1 The LCO AI in Criminal Justice Project

The Law Commission of Ontario (LCO) AI in Criminal Justice Project is a pioneering survey and analysis of the opportunities, risks, and law reform issues regarding artificial intelligence (AI) in the Canadian criminal justice system.

Many AI technologies have potential to improve public safety, improve police investigations, and improve the efficiency and fairness of criminal proceedings. Many AI technologies also appear to have potential to address, at least in part, long-standing concerns about racialized criminal justice and access to justice.

At the same time, the use of AI in criminal justice is controversial. Technologies such as predictive policing, facial recognition and biometric surveillance, and bail/sentencing algorithms have been criticized in many jurisdictions for their impact on racialized and low-income communities, constitutional rights, human rights, criminal procedure, criminal common law principles, privacy, and access to justice.

The LCO AI in Criminal Justice Project is a unique collaboration of leading practitioners and experts from across the Canadian criminal justice system. Project authors and advisors include representatives from governments, police services, Crowns, the criminal defence bar, courts administration, legal aid, human rights commissions, civil society organizations, and academics.

Working together, the LCO and our collaborators believe this project is an important contribution towards developing "Trustworthy Criminal AI" in the Canadian justice system. Our collective goal is help inform policymakers and stakeholders about the law reform issues, choices, opportunities, and challenges in this complex and fast-moving area.

This paper is the second of a series of five Issue Papers that comprise the project.[1] Each Issue Paper is an expert collaboration considering the use of AI in a distinct phase of the criminal justice process, including:

Paper 1	Introduction and Summary: LCO AI in Criminal Justice Project
Paper 2	Use of AI by Law Enforcement
Paper 3	AI and the Assessment of Risk in Bail, Sentencing, and Recidivism
Paper 4	AI at Trial and on Appeal
Paper 5	AI and Systemic Oversight Mechanisms in Criminal Justice.

Many of the topics addressed in this Introduction and the Issue Papers have been addressed individually in international and Canadian analyses. Unlike earlier reports, however, the LCO project addresses systemic issues that transcend discussions about specific technologies or proceedings. In other words, the LCO project assesses the collective or cumulative impact of AI on criminal justice in Canada. The LCO project is the first independent and collaborative initiative in Canada to address these important and timely issues.

The LCO believes this project is urgent. AI in the criminal justice system affects some of most important issues and rights in Canadian society, including public safety, personal liberty, rights to equality and procedural fairness, and public trust in key public institutions, including courts and the police. At the same time, fast-paced technological, legislative, and policy developments in Canada and internationally have put pressure on Canadian police services, governments, courts, and stakeholders to respond to criminal AI issues quickly.

To their credit, some Canadian police services and other agencies have taken important initiatives to address AI risks. As will be seen, however, there are still wide and consequential gaps in the legislative or legal framework governing these systems. Indeed, Canadian lawmakers are far behind their international counterparts, where the first "wave" of criminal justice AI governance has already been supplanted by more sophisticated laws and policies.

The LCO AI in Criminal Justice Project is organized around four key themes or topics.

First, the project considers several important practical and legal questions that will soon confront Canadian police, courts, policymakers, Crowns, defence counsel, and criminal accused, including:

- What AI tools could be used at each important stage of Canadian criminal justice?
- What legal issues are likely to arise at each stage?
- What is the state of Canadian law and procedures to address these issues, particularly in relation to the Canadian *Charter of Rights and Freedoms*, procedural fairness, and criminal common law?
- What issues cut across specific proceedings or stages and suggest the need for a systemic response or framework?

Second, the LCO project asks who is likely to be affected by AI in the criminal justice system. What institutions, agencies, organizations, or individuals will be affected in some way? And what does the breadth or complexity of those actors suggest about criminal justice AI regulation and governance?

Third, the LCO project surveys potential solutions at the specific and systemic level. In so doing, the project highlights the speed, variety, sophistication, and breadth of AI regulation in recent years. This Introduction and the Issue Papers discuss potential policy, procedural, or law reform responses to the issues arising at each respective stage, including:

- What can we learn from the experience of other jurisdictions that have confronted these issues?
- How have Canadian policymakers, courts, and others responded to the emerging challenges?
- Are there gaps in Canada's current criminal AI regulatory landscape?

Finally, the project tries to foreshadow or predict what is likely to happen in Canadian criminal justice if action is not taken. In other words, what is likely to happen if we fail to address these issues? What can we learn from the experience in other jurisdictions?

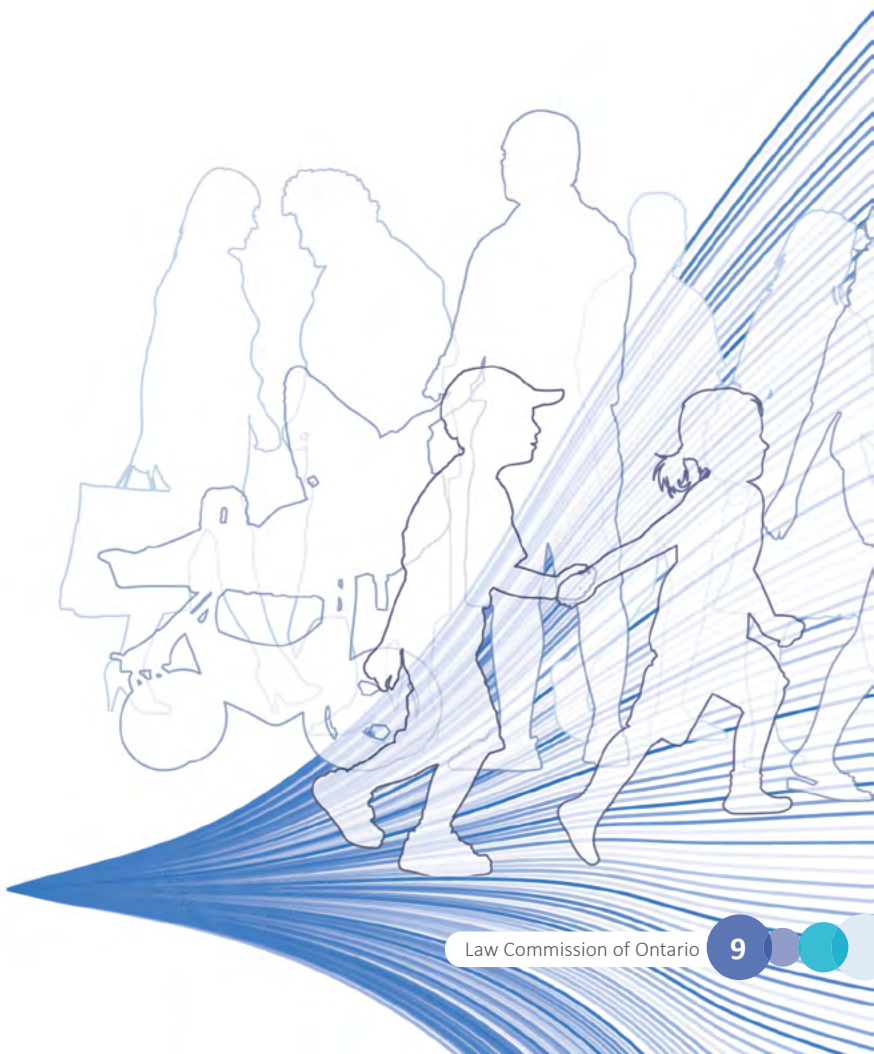
The LCO's series of Issue Papers are designed to facilitate discussion and consultation. We have learned that "trustworthy criminal AI" depends on complex legal, technical and operational considerations. We have also learned that broad collaborations and consultations are crucial. Accordingly, each Issue Paper includes questions for Canadian criminal AI policymakers and stakeholders. In this manner, the LCO hopes the papers will become a catalyst for a wider Canadian discussion about these issues.

Publication of the Issue Papers commences a period of stakeholder consultations to be conducted by the LCO. The LCO will analyze and summarize the feedback we receive. A Final Report will recommend a series of law, policy and programmatic reforms.

More information about this project is available on the LCO project website: https://www.lco-cdo.org/CrimAI.

Background and Definitions.

Readers are encouraged to first review LCO's *Introduction and Summary: LCO AI in Criminal Justice Project*. This paper establishes a definition for "artificial intelligence" used throughout this project. In addition, the paper provides an overview of various AI technologies in criminal justice and gives a primer on the basic legal and policy frameworks governing AI in Canada and elsewhere.



1.2 Executive Summary: The Use of AI By Law Enforcement

This is the second of five Issue Papers in the LCO's AI in Criminal Justice Project. This paper discusses how law enforcement agencies are using AI-enabled systems and the kinds of systems that are under consideration. Examples are drawn from within Canada and internationally. A more in-depth examination is made of three specific AI-enabled technologies which have already known to be used by Canadian law enforcement: facial recognition, predictive policing, and object recognition. The paper concludes with a discussion about the foreseeable risks, benefits and systemic impacts of AI technology, and identifies options that might help the criminal justice system prepare for these challenges.

The discussion that follows is practical and timely, as well as forward-looking.

Criminal justice systems in Canada have been relatively more cautious in adopting AI technologies than have other jurisdictions. However, the experience of other jurisdictions can tell us much about the potential risks and benefits of AI. This helps assess the state of Canadian law and procedures to address such issues, particularly in relation to the Canadian *Charter of Rights and Freedoms*, procedural fairness, and criminal common law.

At the same time, there are already several – and in some cases controversial – uses of AI by Canadian law enforcement agencies. This includes facial recognition, facial matching and arrest photo ("mugshot") identification, automated fingerprint identification, predictive policing, de-encryption of digital devices, object recognition in images and video, and classification of purportedly high-risk inmates.[2]

Law enforcement agencies outside of Canada further employ AI to profile public activities on social media, engage in mass tracking of movements, facilitate autonomous surveillance, automate police reports including event, video and audio summaries, conduct open-source intelligence scans, and use reverse photo geolocation to identify places of interest.[3]

In many cases, law enforcement does not need to adopt or deploy its own AI systems to leverage such technology. Law enforcement may may obtain AI-generated and AI-mediated evidence from third parties such as mobile app developers, social media platforms, cloud services providers, private commercial and personal surveillance systems, or community and social service providers. Largely unregulated data brokers may also be willing to disclose or sell detailed profiles that track online activities, geolocation data, and personal relationships. Over the coming years it is certain that these and many other AI-enabled technologies and sources will be considered for use in Canadian criminal justice.

It is also certain that choices made by law enforcement will trigger direct and indirect ripple-effects on the criminal justice process. Information gathered in an investigation and prepared by law enforcement may influence assessments for bail and sentencing, the review of charges by Crown prosecutors, the decision by an accused to plead guilty or go to trial, and the admissibility and interpretation of evidence.[4] Law enforcement use of AI may also be subject to systemic reviews, such as police misconduct investigations, Coroner's Inquests, wrongful conviction reviews, and human rights investigations, among others.

Less well understood is what the regulatory framework will be for AI technology. There are open questions about the legal standards against which such technology will be assessed; how any deployed technology will be governed; and the extent to which existing law, procedure and convention is sufficiently adaptable and resourced to respond to the challenges of AI.

More to the point: many of the challenges AI presents are readily foreseeable. The LCO AI in Criminal Justice Project details the many ways in which AI will be challenged by existing legal protections under the *Charter of Rights and Freedoms*, guarantees to a fair hearing through criminal procedural fairness, and established criminal case law precent and principle. The concern is that courts alone are not suited to developing a comprehensive set of rules to govern AI

within law enforcement or consistently across all the institutions involved in a criminal justice proceeding. A more proactive, systemic, forward-looking approach is needed.

At present, there are no specific laws which govern the use of AI-enabled technology by law enforcement in Ontario. But the context and background for AI governance is changing rapidly. AI legislation and regulations are much more sophisticated today than they were even three or four years ago.

At the federal level, the Government of Canada has proposed the *Artificial Intelligence and Data Act* (AIDA)[5] and adopted an administrative Directive on Automated Decision-Making.[6] AIDA only applies to private sector AI developers and the Directive only applies to the federal government (and excludes National Security Systems including the RCMP).[7] However, both initiatives set benchmarks against which law enforcement use of AI can be compared, including how various sectors are presumptively considered "high-risk" fields for deploying AI.[8] To date, however, the legislation is stalled at second reading in a prorogued Parliament.

The Government of Ontario also recognizes the need to act. In May 2024, Ontario introduced Bill 194, *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*.[9] Schedule 1 under Bill 194 enacts the *Enhancing Digital Security and Trust Act, 2024*[10] to establish legislation and regulations recognizing "that artificial intelligence systems in the public sector should be used in a responsible, transparent, accountable and secure manner that benefits the people of Ontario."[11] After relatively short debate and limited hearings before committee, Bill 194 was granted Royal Assent in November 2024.

Bill 194 has the potential to regulate public sector AI systems effectively. However, as enacted, the Bill 194 falls short of this ideal. Most critically, the Bill is brief and lacks key provisions needed to ensure public sector AI use is beneficial, lawful, and accountable.[12] More specifically, the Bill does not address several widely acknowledged regulatory priorities for AI, including AI systems used in the criminal justice system.[13] Any and all details of how risk assessments might be conducted or the issue which will require risk assessments are left to future regulations.

Almost immediately following Bill 194, in December 2024, the Ontario government implemented its "Responsible Use of Artificial Intelligence Directive."[14] The goal in adopting the Directive is to "ensure responsible, accountable and transparent use of AI in the Government of Ontario, ministries and provincial agencies."[15] The Ministry of Public and Business Service Delivery and Procurement is responsible for the Directive and any operational policies.

Generally, the Directive "requires the application of AI risk management by ministries and provincial agencies that are seeking to use AI systems, or use services that include AI functionality (including procured, ministry/provincial agency developed and publicly available tools), as part of the development or delivery of, or decision-making for, a Government of Ontario policy, program, or service."[16] Overall, the Directive adopts a broad and principled approach with few operational details. It adopts six core principles requiring that the use of AI must be:

- Used to benefit the people of Ontario;
- Justified, proportionate, reliable and valid;
- Safe, secure and protective of privacy;
- Human-rights affirming and non-discriminatory;
- Used in a transparent way with meaningful explanations of decisions made; and
- Accountable and responsible.[17]

The LCO's early analysis also identified several potential significant gaps or uncertainties. For example, the Ontario AI Directive:

- Does not apply explicitly to provincial law enforcement agencies or any other provincial police service. Ministries may also be exempt from the Directive.[18]
- Does not include several trustworthy AI elements identified by the LCO in our reports. [19]
- Does not establish a consistent, transparent AI risk management framework, including systems or criteria of prohibited AI systems.[20]
- Does not establish consistent and comprehensive disclosure obligations.[21]
- Does not establish a remedial regime and lacks access to justice provisions.[22]

Consequently, the extent to which law enforcement agencies are bound to this Directive, or will adopt its principles, is uncertain. Furthermore, it is not yet clear how the Ontario AI Directive relates to the regulatory powers established in Bill 194. Both frameworks also rely on broad, principle-based approaches. The lack of a detailed legal regulatory framework may undermine public confidence and trust in the use of AI by law enforcement while undermining implementation and consistency.

This is a significant deficit generally, and in law enforcement context specifically. Despite the relative novelty of AI technology, there are already several known risks associated with the use of AI in criminal justice. Individually and collectively, these risks can lead to "accusation by algorithm" without effective pre- and post-facto checks and balances.[23] Known risks with AI include the following:

- AI systems are often trained on historical population and criminal justice system data that reflects generations of biased and discriminatory decision making – and may reproduce these patterns in its recommendations about where or who to police.
- AI systems may encourage "automation bias" or "automation deference" where human decision makers – often under the pressures of lengthy investigations, enormous case loads and limited resources – uncritically defer to the expediency of AI evidence or recommendations. Users of AI systems may also misinterpret AI recommendations or apply them selectively to confirm their own decisions.
- Biometric systems are known to disproportionately misidentify persons because of their race, age or gender.
- Risk assessment tools may be unable to explain recommendations and may not be calibrated, validated or audited to achieve objective performance standards, including controlling for bias.
- Expanded surveillance powers, profiling, social scoring or the potential for law enforcement "micro-directives" may have a chilling effect on public participation and freedom of assembly.[24]
- Open-source intelligence and privately purchasable data sets may be mined by AI systems to create powerful tools for tracking and correlating individuals, activities and objects across desperate events and multiple data sources.
- Generative AI assistant tools – such as transcription services, incident report generators and research tools – may misinterpret input, hallucinate citations and authorities, cloud the recollection of personal accounts, or disclose sensitive information that may jeopardize public safety or an investigation or prosecution.

More broadly, public trust figures as a key consideration in whether and how such technologies are used. Each technology raises concerns for fundamental rights, including the protection of civil liberties and privacy under the Canadian *Charter of Rights*; human rights to be free of biased or discriminatory state action; and procedural fairness guarantees of transparency, disclosure, and the production of valid and reliable evidence.

Without an effective and comprehensive framework to establish and enforce "trustworthy AI" in criminal justice, there is also the significant risk of undermining and underfunding the many potential benefits of AI. For instance:

- AI could potentially help mitigate well-established biases in human decision making and contribute to better informed and more neutral outcomes.[25]
- AI-powered legal tools may make law enforcement and legal procedures more effective and efficient, mitigating resource constraints, processing routine issues faster, and alleviating investigative delays.[26] For instance, police forces specifically highlight how AI can expedite the "classifying and editing [of] large amounts of photo and video evidence" that now feature in many investigations.[27]
- AI tools could better track performance characteristics in criminal justice, such as patterns in decision making and identifying racial over-representation.
- AI may mitigate barriers in accessing justice, including examples where AI ChatBots help victims of abuse safely submit evidence and create safety plans, or help expunge criminal records by drafting required personal statements.[28]

In the absence of legislation in Canada and Ontario, and given these concerns for AI, several active initiatives merit our consideration.

First: AI is increasingly governed through self-regulatory and soft-law policy instruments. Already there are several examples operating in or adjacent to criminal justice, and other areas where this opportunity is in the early stages of conception and exploration. This includes:

- **Law Enforcement:** Two of the largest law enforcement agencies in Canada have established internal assessment and review procedures for AI: the RCMP's National Technology Onboarding Program (NTOP)[29] (which assesses all proposed operational technologies including AI) and the Toronto Police Services Board "Use of AI Technology Policy."[30] The Durham Regional Police Service Board also recently adopted a "Use of AI" policy (October 2024).[31]
- **Law Enforcement Umbrella Organizations:** There appears to be an opportunity for umbrella organizations to develop model AI policies, such as the Ontario Association of Chiefs of Police, the Canadian Association of Chiefs of Police, or the Ontario Association of Police Service Boards. Such policies could help set baseline expectations, assist smaller police forces with policy development, and encourage consistent standards and practices across the province. Development of such policies may also consider alignment with federal agencies and institutions.
- **Courts in Canada:** The Federal Court has adopted a pair of policies to guide both the use of AI by the court itself, and to direct the use of AI by parties and professionals appearing before the court.[32] Courts in other provinces have adopted AI policies to varying degrees including in Alberta, Manitoba, and Quebec, among others.[33] The Canadian Judicial Council also released guidelines for the use of AI by judges.[34]
- **Courts in Ontario:** A Tri-Court Committee was formed in May 2024 and is developing AI policies to prevent judges from making mistakes in the use of AI and to consider ways in which this technology can be used by judges to make their work easier and better.[35] More recently, the Civil Rules Committee's Artificial Intelligence Subcommittee "passed rule amendments requiring lawyers to authenticate judicial precedents in their filings and requiring experts to authenticate source materials they were relying on in their reports."[36] The Committee are also "mulling requiring parties to disclose the AI program they're using to generate evidence, for example, in motor vehicle accident reconstruction files."[37]
- **Legal Professionals:** The Law Society of Ontario issued guidance to the profession on how rules of professional conduct apply to the delivery of legal services empowered by generative AI.[38] Guidance has also been published by law societies in British Columbia, Alberta and Saskatchewan.[39] Outside of Canada guidance has been issued by the European Bars Federation and the Law Societies of England and Wales,[40] as well the United Kingdom Courts and Tribunals Judiciary.[41]

Self-regulatory efforts are laudatory but also limited. This is particularly evident in the context of law enforcement.

For instance, the Toronto Police Services recently attracted criticism of the Ontario Human Rights Commission and the Information and Privacy Commissioner of Ontario for categorizing their use of AI technologies – including automated license plate readers and fingerprint identification – as "low risk technologies" with fewer assessment and oversight requirements. This is despite candid acknowledgement by police that such technologies "could be used to assist in the identification of individuals for the purpose of their arrest, detention or questioning."[42]

Self-regulatory approaches are also problematized by various public interest legal research groups as failing to address systemic ripple-effects, particularly as they construct an outsized role for courts as the bottom-line check-and-balance on AI. In addition to the LCO's AI in Criminal Justice Project, the Citizen Lab published *To Surveil and Protect*, outlining the human rights and constitutional law implications of the use of algorithmic policing technologies by law enforcement authorities.[43]

Read together, these papers suggest that leaving AI to "regulation by courts" has several drawbacks, namely that:

- Existing criminal case law necessarily has significant gaps in relation to a new technology like AI while cases often turn on narrow facts, specific technology, and contextual use cases that limit the reach of precedent.
- Criminal justice litigation is an intensive and expensive process and comes with significant access to justice limitations including equitable access to experts, funding for defence counsel, and availability of court time.
- Criminal justice litigation is certain to lag the use of AI technology by several years, and only ameliorates the lack of proactive governance and regulation.
- The 50+ distinct and overlapping jurisdictions for both law enforcement agencies and criminal courts across Ontario suggest a patchwork approach will contribute to a variegated system with competing precedents and technologies.

In the meantime, other jurisdictions have enacted or proposed strong regulatory schemes governing AI in criminal justice and its use by law enforcement. Leading jurisdictions include the European Union's *Artificial Intelligence Act* (EU AIA),[44] and several instruments in the United States, including the *AI in Government Act of 2020*, the *Advancing American AI Act 2022*, and White House Executive Orders directing the "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" (2023) and "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence" (2024).[45]

These instruments provide lessons for Ontario on how AI in criminal justice could be effectively governed through a coordinated and multi-layered approach.

For example, the EU AIA presumptively prohibits uses of the highest-risk AI technologies including mass biometric identification, social scoring, and predictive policing (with some exceptions for emergencies including investigations into missing persons, child apprehension, and sex trafficking). At the same time, high-risk uses of AI – including in the law enforcement context – are subject to clear procedural requirements for judicial authorization in combination with reporting requirements and public registries that foster transparency and public trust. The EU AIA also establishes an AI Office with a mandate to issue interpretive and policy guidelines, as well as a role to assess AI technologies and certify their performance and reliability – and streamlining their availability.

It is also worth pointing out that Canadian law enforcement agencies have a long history of adopting new technologies. Many of these technologies have been controversial or used in controversial ways. Many have become commonplace and rights-balancing through procedural frameworks and certification measures that make their use predictable, reliable, and efficient. For instance, breathalyzer evidence can be rapidly relied on and admitted into evidence

because the Criminal Code sets out a detailed and complete scheme for their use, including certification of approved instruments and qualified technicians that support presumptions about reliability and validity.[46] At the same time, many other technologies are adopted and deployed without formal procedural and certification measures. Relatively recent technologies such as electronic surveillance practices, cell site simulators, tracking devices, or on-device investigation tools instead rely on established checks and balances in the criminal justice, such a judicial authorization.

All these initiatives have much to teach Ontario and Canada about the range of available options and responses to governing AI systems. Crucially, all these initiatives suggest that many of the concerns for the use of AI by law enforcement are foreseeable. They further suggest that Trustworthy AI provides the guardrails needed for the benefits of AI to be realized.

This paper explores these themes as follows:

- Section 2 discusses how AI-enabled technologies like facial recognition, predictive policing, and object recognition are different from other technologies used and analyzed by law enforcement;
- Section 3 discusses key concerns and questions raised by these technologies, including:
  - limited regulatory and governance frameworks;
  - the efficacy of voluntary self-regulatory policies;
  - the impact on Charter of Rights requirements including privacy rights, arbitrary detention, and evidentiary production;
  - the relationship between legal expectations for full disclosure and known limitations of AI including explainability, bias, and expert testimony;
  - warrantless requests by law enforcement for private information; and
  - potential uses of "AI for good;"
- Section 4 summarizes the key questions for public consultation raised in this paper.

AI in Criminal Justice Case Studies.

See the LCO AI in Criminal Justice Project *Annex B: Project Case Studies* for a discussion contrasting the legislative, regulatory and implementation framework for intoxilyzers in comparison to some of the challenges AI presents. These issues are also reviewed in Project Paper 4, *AI At Trial and On Appeal*.

Overall, this discussion suggests the need for public consultations on the following issues:

Consultation Questions

1. The discussion suggests the need for provincial rules establishing key trustworthy criminal AI rules and criteria. The Issue Papers suggest many potential models, including:
   - Federal legislation or regulations (Criminal Code, federal ADM Directive?).
   - Provincial legislation or regulation (EDSTA, policing legislation, Ontario AI Directive?).
   - Criminal justice institutional policies (Police, courts, Crown Policy Manual?).

   a. Do you agree some kind of provincial framework is necessary? If so, which approach (or approaches) is best and why?

2. The EU AI Act, AIDA, and the Toronto Police Services AI policy all adopt some form of risk-based AI governance, including presumptive prohibited uses and/or presumptive "high risk" AI systems subject to stricter requirements and more oversight.

   a. In principle, do you agree with the prohibited/high risk framework? What criteria should be adopted to identify prohibited or high-risk systems? Does Canadian law suggest which, or how, different AI systems or uses ought to be categorized?

   b. If you agree some systems or uses should be prohibited or identified as "high-risk":
      - What AI systems or uses should be in these categories?
      - Should real time FRT or predictive policing be prohibited? If so, are there reasonable exceptions, such as FRT to assist missing persons investigations? What rules should apply?
      - What oversight rules or procedural requirements are appropriate for high-risk systems?

3. Disclosure is a consistent theme in trustworthy criminal AI legislation and frameworks. There are choices about the timing, form and substance of disclosure obligations.

   a. How and to what extent should criminal AI systems be disclosed?

   b. Should there be a mandatory AI register or public report? If so, what should be included:
      - A detailed or summary impact assessment?
      - Comprehensive or a summary description of training data?
      - Output data to facilitate independent auditing, oversight and performance monitoring?
      - How to promote disclosure while protecting other legitimate objectives, such as sensitive investigating techniques?

4. The need for impact assessments is a consistent theme in criminal AI legislation and frameworks. There are choices about the timing, form and substance of impact assessments.

   a. Should the province require a mandatory impact assessment for criminal AI systems in Ontario? Do you agree an impact assessment should address privacy, human rights and procedural fairness and provide assurances about how an AI system will comply with other legal obligations?

   b. What other information or risks should be included?

   c. How best to ensure impact assessments are being used and reported consistently?

5. Many criminal AI systems have been criticized by communities who believe they were not consulted or informed about systems that affect them. Many trustworthy criminal AI initiatives, including the Toronto Police Service AI Policy, include public engagement requirements.

   a. How should the public be involved in criminal AI policymaking, evaluation or oversight?

6. Criminal AI systems raise new and complex procedural, evidential and litigation challenges, including:
   - Admissibility and reliability of AI evidence and whether AI is "expert evidence"
   - Use of AI to generate incident reports, summarize or analyze body cam data, etc.
   - AI-assisted submissions to court or disclosure summaries.
   - Deep fake evidence.
   - AI-generated witness statements, victim impact statements, Gladue reports, etc.
   - Litigating assertions of "trade secrets," "investigative privilege" or routine vs. investigative uses
   - Warrants or O'Connor Applications for third-party evidence.

   a. How can we regulate, formalize or streamline frequently litigated AI-related issues like the above?

   b. Would a routine requirement for full disclosure of an AI system and its components be mitigated by objective AI performance measures, such as independent technical audits that validate the reliability and performance of AI systems?

   c. Do we need standards or practices governing AI-generated statements/reports to ensure reliability and admissibility?

7. Criminal AI systems raise new challenges for Ontario's criminal justice institutions.

   a. Does the provincial justice system have sufficient institutional capacity to respond to these challenges? If not, what tools or supports are needed to help institutions to proactively respond to these challenges?

8. In addition to the measures discussed above, many believe there is a need for independent oversight of public sector AI system, including in criminal justice.

   a. Given that many criminal justice institutions have or are subject to forms of oversight, how would AI oversight work?

   b. Does Ontario need a new, independent oversight office or can this function be built into existing organizations?

1.3 Consultations, Contacts and Project Support

Consultations

The LCO believes that successful law reform depends on broad and accessible consultations with individuals, communities, and organizations across Ontario. As a result, the LCO is seeking comments and advice on this issues paper. There are many ways to get involved. Ontarians can:

- Learn about the project and sign up for project updates on our project website.
- Contact us to ask about the project.
- Provide written submissions or comments on this issues paper.

Project Lead and Contact

The LCO Project Lead is Ryan Fritsch. Ryan can be contacted at rfritsch@lco-cdo.org.

The LCO can be contacted at:

Law Commission of Ontario
2032 Ignat Kaneff Building
Osgoode Hall Law School, York University
4700 Keele Street, Toronto, ON, M3J 1P3

Tel: (416) 650-8406
E-mail: LawCommission@lco-cdo.org
Web: https://www.lco-cdo.org
LinkedIn: https://linkedin.com/company/lco-cdo
Bluesky: @lco-cdo.bsky.social
X: @LCO_CDO
YouTube: @lawcommissionofontario8724

Author and Project Editors

This paper was written by Ryan Fritsch, Counsel, LCO. Ryan Fritsch supported and edited the project Issue Papers.

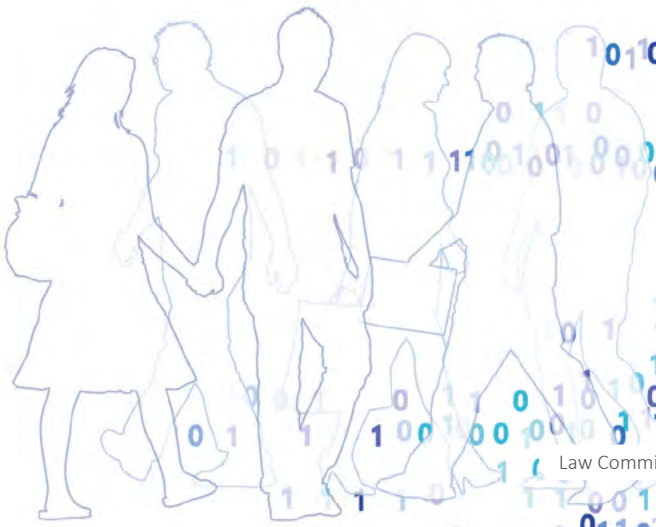
Project authors include:

- **Gideon Christian**, Professor of Law, Faculty of Law, University of Calgary
- **Armando D'Andrea**, Staff Lawyer, Provincial Office, Legal Aid Ontario
- **Ryan Fritsch**, Counsel, Law Commission of Ontario
- **Brenda McPhail**, Senior Technology & Policy Advisor, Information and Privacy Commissioner of Ontario
- **Eric Neubauer**, Defense Counsel, Neubauer Law, and Co-Chair, Criminal Lawyers Association Technology Committee
- **Marcus Pratt**, Senior Advisor, Policy Department, Legal Aid Ontario, and Chair of the LAO Test Case Committee
- **Jagtaran Singh**, Legal Counsel Ontario Human Rights Commission
- **Nye Thomas**, Executive Director, Law Commission of Ontario
- **Paula Thompson**, Strategic Initiatives, Ministry of the Attorney General

Advisory Committee

An external Advisory Committee oversees the project and provides ongoing feedback through the research, drafting, and consultation process. Advisory Committee members include:

- Alpha Chan, Chief Information Security Officer, Toronto Police Services
- Marco Galluzzo, Office of the Chief Justice, Ontario Superior Court of Justice
- Rosanna Giancristiano, Director, Court Operations, Ministry of the Attorney General
- Rosemarie Juginovic, Office of the Chief Justice, Ontario Superior Court of Justice
- Associate Professor Daniel Konikoff, Department of Sociology, University of Alberta
- Michelina Longo, Director, External Relations, Ministry of the Solicitor General
- Jessica Mahon, Policing Standards Section, Ministry of the Solicitor General
- Jane Mallen, Ministry of the Attorney General and LCO Board of Governors
- Elena Middelkamp, Crown Law Office Criminal, Ministry of the Attorney General
- Savio Pereira, Policing Standards Section, Ministry of the Solicitor General
- Professor Ben Perrin, Faculty of Law, University of British Columbia
- Michael Swinburne, Senior Policy Advisor, Canadian Human Rights Commission
- Professor David Murakami Wood, Department of Criminology, University of Ottawa



2. Use of AI by Law Enforcement

This section of the paper explores the use of AI-enabled systems by law enforcement in Canada and elsewhere. It begins with an overview of the mix of AI-enabled systems in use or contemplated for use. It then takes a more in-depth look at the challenges associated with three specific AI-enabled systems in the law enforcement context:

- facial recognition technology (FRT);
- predictive policing; and
- automated object recognition.

These systems have been used by Canadian law enforcement. However, relatively little information in publicly available assessing the effectiveness, scope, and oversight of these systems. Accordingly, this paper looks at challenges associated with the use of these systems in other jurisdictions to identify the kinds of challenges Canadian law enforcement are likely to face and the lessons that can be learned from these other jurisdictions.

2.1 What is New or Different about AI Compared to Other Policing Technologies?

Law enforcement agencies have a long history of adopting and contending with new technology in their work. Many of these technologies have been controversial or used in controversial ways. Recent and well-known examples in Canada include the use of technologies like body cams, tasers, mobile phone tracking and triangulation, decryption, DNA identification and probabilistic genotyping, and aerial surveillance.

Public trust figures as a key consideration in whether and how such technologies are used. Each technology raises concerns for fundamental rights, including the protection of civil liberties and privacy under the Canadian Charter of Rights; human rights to be free of biased or discriminatory state action; procedural fairness guarantees of transparency, disclosure, and the production of valid and reliable evidence; and compliance with criminal common law principles and precedent.

In response to these challenges, governments and law enforcement agencies may seek to develop safeguards relating to the approval, use and oversight of new technology. Many different governance instruments may be used, and when used in conjunction, may create a coordinated and multi-layered governance model. Governance instruments can include:

- Presumptive prohibitions on the use of particular technologies or in particular use cases;
- Restricted use of particular technologies subject to external oversight such as judicial authorization or warrants, specially trained officers, or to comply with privacy and data governance requirements;
- Procurement rules that first require risk assessments, cost-benefit analyses, mitigation of foreseeable harms, public transparency, and public consultation;
- Post-deployment governance, including the regular use of technical and performance assessments, validation and certification;
- The development of training programs, performance measures, and reporting requirements, and restricted use of technology to specialized roles and certifications;
- Law, policies or procedures to standardize responsible use of new technologies, such as certified labs or breathalyzer certification; and
- Public participation in assessing and overseeing law enforcement practices and tools.

AI technology is certain to require a set of procedural and other safeguards like those applied to existing and deployed technologies.

At the same time, the novelty and sophistication of AI technology suggests a new set of concerns and invites the need to consider additional safeguards that may be required.

For instance:

- AI-enabled systems may create new forms of "cybercrime," challenging police to track developments with issues as diverse as online and intimate partner harassment, AI generated child pornography, impersonation used to defraud and scam, or the investigation of misleading video, image and audio "deep fakes" (see below sidebar "**The Challenge of Investigating Deep Fakes**");
- AI-enabled systems may supplement or supplant human decision making, which can contribute to systemic "automation bias" or "algorithmic deference" and an uncritical acceptance of AI recommendations.
- AI-enabled systems may be used to make investigative predictions or risk recommendations that can make law enforcement more efficient and effective, but which may reproduce historical patterns of discrimination, over-police different populations, or lead to wrongful arrests.
- AI-enabled systems may automate tasks such as surveillance and identification previously done by people. Such activities can skirt human and procedural checks and balances, import implicit and express biases, and foster a culture of technological over-reliance.
- AI-enabled systems may make it easier to correlate disparate pieces of information, leading to new forms of mass surveillance, object tracking, and behavior monitoring.
- AI-enabled systems may automate investigative tasks such as transcription and translation services, incident report generators and research tools. These are prone to misinterpret input, hallucinate citations and authorities, cloud the recollection of personal accounts, or disclose sensitive information and jeopardize an investigation or public safety.
- AI-enabled systems may give rise to enforcement through "AI micro-directives," which "provide individualized instructions for legal compliance in a particular scenario… Made possible by advances in surveillance, communications technologies, and big-data analytics… [to] prescribe action or inaction required by law."[47]

More broadly, the need for trustworthy AI is increasingly apparent as new AI products are aggressively marketed to law enforcement agencies.

For instance, reports from the recent International Association of Chiefs of Police Conference – billed as "the largest gathering of police chiefs in the United States, where [attendees are the] leaders from many of the country's 18,000 police departments" – found that one needed only "to look to where the largest crowds gathered to understand that AI was the major draw" among the more than 600 exhibitors.[48]

Observers indicate the focus was on three classes of AI in policing:

- The use of virtual reality systems for officer training;
- Deployment of an expanding suite of sensors and cameras that, in conjunction with the power of AI recognition and analysis, create "domain awareness systems" that greatly expand surveillance powers; and
- The use of AI to replace administrative tasks and reporting, including generating officer reports by summarizing footage of body cams and audio sources.[49]

These technologies raise questions about the need for procedural safeguards for the use of AI technology, including:

- which safeguards are well suited to govern the responsible use of AI systems;
- which safeguards are best suited to specific uses of AI; and
- how AI is likely to be interpreted through legal lenses.

Law enforcement agencies are also interested in AI for its potential to greatly enhance investigative efficiency in general, and to keep pace with digital evidence in particular.

For instance, investigations related to child exploitation, human trafficking or missing persons may require sifting through tens of thousands of images or hundreds of hours of video found on hard drives. One algorithmic impact assessment filed by the RCMP in 2024 described the need for Griffeye "facial matching technology" to aid in investigations given that "the average single case" of "child pornography and sexual abuse videos and images" contains "in excess of 3 million media items to review […] to quickly identify, locate and safeguard children being victimized."[50] Similarly, complex financial fraud cases often involve massive and complex spreadsheets totalling millions of fields. AI systems are uniquely capable of rapidly sifting through such data and, unlike human resources, easily scale up as the volume of data does. Examples of AI assisting in these circumstances are given in the sidebar "The Challenge of Investigating Deep Fakes" and in section 2.2 below.

The Challenge of Investigating Deep Fakes

The use of AI technology, and in particular "deep fake" images, audio and video content, complicates criminal investigations and is a significant and evolving concern. Online generative AI tools can produce high-quality video, audio and images, making the creation of false evidence relatively simple and accessible to the average person.[51]

Deep fake technology generally involves creating visual or audio content by "insert[ing] faces and voices into video and audio recordings of actual people"[52] so that the content created "would falsely appear to a person to be authentic or truthful."[53] The result is that people can create media content showing "real people saying and doing things they never said or did."[54] It has become easier to make deep fakes, and requires decreasing amounts of technical expertise.

Deep fakes present challenges for investigators and creates new crimes for investigation. For instance, deep fake child porn is being generated to such volumes that "cops [are] bogged down by flood of fake AI child sex images… [as] Investigations tied to harmful AI sex images will grow "exponentially"."[55]

Deep fakes can also feature prominently in commissioning crimes. In April 2024, a public-school athletic director in Baltimore was arrested after it was determined he framed the school principal using AI voice synthesis.[56] Police say the accused used AI voice synthesis software to simulate the principal's voice, leading the public to believe the principal made racist and antisemitic comments and resulting in the principal's suspension amidst the investigation.

Courts increasingly face AI-mediated evidence too. In the 2024 murder trial *State of Washington vs. Pulsoka*, the presiding judge reviewed "AI enhanced video" produced by the defense. The evidence was deemed inadmissible on the strength of expert testimony that the video was in fact "enhanced" but used AI to add detail where none existed, undermining the integrity of the images.[57]

Early cases are appearing in Canadian courts too.

In *R. v. Larouche* (2023 QCCQ 1853), the accused used deep fake software that sequenced video extracts frame by frame, creating a database of thousands of images that were then used to create several deep fake pornographic images and videos of children.[58] By using this software to produce 7 video files of child pornography, the accused created 86,000 new photos of child pornography.[59] Each of the files produced also contained an independent digital footprint, effectively replacing the source material known to police with tens of thousands of new files.[60]

This development of changing known hash values for known child pornography will complicate police investigations of child pornography offences moving forward.[61] The existing technology available to law enforcement is described as becoming "obsolete" and "ineffective" at controlling the spread of child pornographic files on the internet.[62]

Canadian courts acknowledge a "consensus among the experts is that deepfake AI will be easy to produce but very hard to detect. Whether it will become a major problem for the courts is unclear. But we need to be ready… [otherwise] the justice system will take an enormous hit."[63]

What to do about deep fake evidence is under active deliberation. In the United States a judicial panel is discussing the possible need for new rules of evidence.[64] Tech companies have also formed various alliance groups who are working towards developing reliable and indelible watermarking technology that would be embedded in AI systems.[65] This follows direction from the White House in Executive Order 14110 (2023) directing the development of digital watermarking technology.[66]

2.2 How is AI Being Used by Law Enforcement in Canada?

Canadian law enforcement agencies are not immune from trends observed elsewhere. Several law enforcement agencies in Canada have already adopted different forms of AI to aid in investigations. These are as follows.

Toronto Police Service (TPS): In January 2024 a report to the Toronto Police Services Board disclosed the use of five AI-enabled systems by TPS. TPS also self-assessed the level of risk each technology poses. One system was classified as "high-risk:" an AI-enabled facial recognition system that automates arrest photo identification. Four other AI-enabled technologies were classified as "low-risk:"

- an automated fingerprint identification system;
- two automated license plate recognition systems; and
- a video-based object recognition system capable of identifying and differentiating between uniformed people, vehicle make and model, and other "unique object classes" as defined by the system user.[67]

Royal Canadian Mounted Police (RCMP): The RCMP's recently released *Transparency Blueprint* (July 2024) emphasizes that "AI is increasingly being used in law enforcement to improve the efficiency of many different functions or tasks" including "classifying and editing large amounts of photo and video evidence," capabilities increasingly essential to "the investigation and identification of criminal suspects, missing persons, children at risk of online sexual exploitation, or [as] may assist in mitigating imminent threats to public safety."[68] The report emphasis how RCMP are, at present, only using facial matching technology which is built into "certain software applications that are used for processing, sorting and analyzing large volumes of images and videos [...] lawfully obtained in the course of an investigation."[69] Future uses of facial matching and facial recognition technology are contemplated, evidently subject to the development of a forthcoming RCMP policy governing such technology.[70]

In the recent past, the RCMP has expressed interest in other AI technology too, for instance, issuing a "request for proposals" for an "AI solution to assist in legally accessing encrypted data."[71] That request for proposals sought "AI technology that would process a person's known passwords, web history and documents to determine potential passwords for encrypted data."[72]

The development of the policies introduced above was driven by investigations in 2021 which revealed RCMP had earlier used facial recognition technology provided by Clearview AI. Clearview "amassed a database of over three billion images of faces and corresponding biometric identifiers, including those of a vast number of individuals in Canada, including children."[73] As discussed in later sections of this paper, the investigation concluded the use of this technology introduced serious public interest privacy concerns.

Going forward, the RCMP's 2024 *Transparency Blueprint* communicates how the RCMP will rely on the National Technology Onboard Program (NTOP) to assess and "onboard" new operational and investigative technologies (including those incorporating AI) prior to adoption and deployment. More broadly, this signals a shift to more proactively developing "key principles" to guide "the responsible use of operational technologies" including AI.[74] In addition to describing the assessment and review process, the *Transparency Blueprint* is clear that future AI technologies are contemplated, including "open-source intelligence" tools like Babel X and AI tools including facial recognition technology.[75]

York Regional and Peel Regional Police (Ontario): In 2024 these police forces began "implementing facial recognition technology provided by multinational French company Idemia," claiming the tools "help speed up investigations and to identify suspects sooner" adding that in terms of privacy, "nothing has changed because security cameras are all around."[76]

Vancouver Police Department, Calgary Police Department, and Ontario Provincial Police: In 2017 the VPD was the first in Canada to adopt "a new crime prediction model that allows the VPD to forecast the location of property crime and take proactive measures to prevent it."[77] Their "new model provides data in two-hour intervals for… 100-metre and 500-metre zones… [to which] police resources can be dispatched to that area on foot or in patrol cars."[78] Predictive policing aim to predict who might predict a crime or where a crime is likely to occur, leading to proactive deployment of patrols, apprehensions and other activities. The has been strongly criticized for reproducing historical patterns of bias and discrimination.[79] Both the Calgary Police Service and the Ontario Provincial Police ("OPP") have also made use of Palantir's Gotham system. The product website describes the product as "a commercially-available AI-ready operating system that improves and accelerates decisions for operators across roles and all domains."[80] As recently as 2022, the OPP refused to disclose publicly how it uses the program, purportedly "…to protect investigative and intelligence techniques."[81] The Calgary Police Service also uses the product, but says it does not use it for "predictive or algorithmic policing", only for "social network analysis."[82]

Toronto East Detention Centre: Introduced the use of "an algorithm that classifies inmates according to risk of violent behaviour."[83] The tool "is designed to assess the risk an inmate will engage in severe and frequent violent misconduct while in custody" based on "a computer algorithm known as SAFER (security assessment for evaluating risk), which analyses several factors including an inmate's prior conduct while in custody, particularly whether there is any history of violent conduct." Critics suggest the system operates to unfairly target overrepresented inmate populations and amounts to "rebranded segregation."[84]

As described above in section 1.2, there are no specific laws which govern the use of AI-enabled technology by law enforcement in Ontario. Legislation has been introduced at the federal and provincial level, though both have notable limitations. The strengths and limitations of these proposals is examined in more detail below in section 2.4.5 "Restrictions and Prohibitions on the Use of FRT in Canada and Elsewhere."

Accordingly, some law enforcement jurisdictions have adopted self-regulatory policies to guide adoption and deployment of these technologies. The leading examples are the Toronto Police Services Board "Use of AI Policy" (which works in conjunction with a procedural manual)[85] and the RCMP National Technology Onboarding Program (NTOP).[86] The programs incorporate a variety of risk assessment criteria, including:

- Declaring key principles for the responsible use of operational technologies including AI, including a proactive approach to establishing policies and criteria.
- Legal compliance, including consideration of human rights, Charter rights, and privacy law.
- Confirmation of an operational need for the technology.
- Clear roles and lines of responsibility for decision makers.
- Risk assessment, risk categorization, and mitigation measures, with AI systems given the highest priority.
- Consideration of "human in the loop" decision making models.
- Transparency initiatives including ongoing disclosure, public reporting, and consultation with arms-length advisory groups.

The strengths and limitations of the self-regulatory approach to trustworthy AI will be discussed in greater detail in section 3 below.

2.3 What Other Forms of AI are in Use by Law Enforcement Outside of Canada?

Canadian jurisdictions can also learn from a broader array of AI-enabled technologies adopted in other jurisdictions. The experience of these jurisdictions has attracted considerable criticism. Leading and well-known categories of these technologies are as follows.

- **Social Media Surveillance & Platform Profiling.** This can include platform profiling to identify people, places, and suspects;[87] automated scanning of threatening language or other criminal intent; activity profiling received from online apps and platforms, for example, of certain medical procedures.[88] Significant concerns have been raised about proactive or warrantless disclosure of such information,[89] and for detailed mass surveillance.[90]
- **Biometric and mass surveillance.** In the US, critics have raised questions about the legitimacy of surveillance data sharing between law enforcement and the private sector. At least four "multi-billion dollar private companies"—FedEx, the mall owner Simon Property, the home improvement company Lowe's, and the health insurer Kaiser Permanente—are reported to be using a car surveillance provider's AI tools and sharing their surveillance feeds with law enforcement as part of their agreement with the provider.[91] In New York City, the police service uses microphones and audio software to detect possible gunshots across the city and dispatch police to the site of a suspected shooting.[92] An audit by the city's comptroller, however, found that the surveillance technology is not very accurate, with 87 percent of dispatches yielding no evidence or confirmation of a shooting.[93] In addition, tools of biometric surveillance include mandatory DNA collection for people convicted or sometimes arrested for crimes and law enforcement access to genetic data held by private genealogy sites.[94]
- **Predictive Policing:** The US legal scholar Andrew Ferguson has highlighted examples of person-based and place-based predictive policing in major cities like Los Angeles and Chicago, using tools provided by private vendors, without being subjected to legislative or judicial limits.[95] The US Department of Homeland Security aims to predict child abuse by using AI to monitor online chats.[96] Two cited benefits of these tools are the fact that investigations are expedited and officers' exposure to traumatizing content is minimized.[97] In 2021, the US Department of Justice (DOJ)'s research arm launched a challenge for researchers to use parole data to "forecast recidivism using person- and place-based variables".[98] The ACLU critiqued the initiative for not engaging affected communities and advocates and stressed the need to embed the strongest protections in any risk assessment and predictive tool because of the great impact that decisions based on them have on people's lives. In January 2024, seven members of the US Congress asked the DOJ to not award federal grants to state and local police agencies if the funds are used for predictive policing systems, due to their potential for discriminatory impact, after the DOJ admitted that it had not kept track of how the funds were used.[99]
- **License Plate and Drone Dragnets:** A majority of large police departments in the US are reported to use automated license plate readers (ALPRs) that scan and track information on the license plates of passing vehicles.[100] With the assistance of AI these systems collect enough data to create comprehensive databases of individual movements. One lawsuit claims that the Illinois State Police's use of such technologies without warrant, or suspicion violates provisions of the US constitution on unreasonable search and seizure (the fourth amendment) and equal protection under the law (the fourteenth amendment). [101] ALPRs are also said to pose privacy and security concerns. In June 2024, the US' Cybersecurity and Infrastructure Security Agency released an advisory identifying vulnerabilities like "missing encryption and insufficiently protected credentials" in Motorola's ALPRs.[102] Notable

ALPR security breaches include unauthorized access to 105,000 license plate images and over 184,000 images of travellers in 2019 when hackers breached the vendor that Customs and Border Protection uses for border patrol checkpoints.[103] Police departments in several US cities also use drones as "first responders" to assess incidents of reported or potential crime before deciding whether or not to dispatch police.[104] Drones may capture live video analyzed by AI to identify objects, vehicles, and people. While residents are not necessarily opposed to such use of drones, these programs have been criticized for not always deploying the devices for a clear purpose, privacy concerns as they gather footage along flight paths on the way to the incident scene and creating a sense of constant surveillance in local communities.[105]

- **Evidence Processing and Enhancement:** A court in Washington State dismissed "AI-enhanced evidence" tendered by the defense in a murder trial on the basis the evidence was unreliable and potentially leading to prejudice.[106] In the *Frye* hearing on the admissibility of the "novel scientific" evidence, the court held that the "AI-enhanced version of a video recorded by a civilian witness on an iPhone" merely inserted detail where none existed, making "forensic analysis of the video impossible."[107] The expert witness for the defense was also unable to explain basic issues including whether the AI tool was certified for forensic use; what data it was trained on; was unfamiliar with any "testing, publications, or discussion groups… evaluating the reliability of AI tools for video enhancement purposes;" and could not explain the "opaque and proprietary" algorithms used to train the tool.[108] Similar concerns have been raised regarding the use of AI to transcribe crime scene video; to prepare event summary statements by analyzing video; or to draft incident reports. . In 2024 for instance, prosecutors in Washington State issued a memo to law enforcement clarifying that "AI-based tools to write narrative police reports based on body camera audio" should not be used, in part because of questionable "reliability" and the risk of making factual errors with potentially "devastating" consequences for the case and disciplinary consequences for police.[109]

AI systems have also been proposed in furtherance of public interest goals. For instance:

- **Emergency Response**: Dispatch call centres in the US have begun using AI-powered systems for several purposes, including creating scenario-based training exercises to sharpen skills[110] and triage low-priority or duplicate non-emergency calls.[111]
- **Monitoring Police Conduct**: Police departments around the US have equipped their officers with body cameras so that the footage can serve as evidence where the nature of their interactions with citizens is disputed. Researchers are reported to be using AI to scrutinize large amounts of such footage, analyzing the tone and word choice of officers in order to determine the frequency of unnecessary escalations and use the findings to improve training and promote accountability.[112]

A closer look at three of these technologies – facial recognition technology, predictive policing, and object recognition – outline the risks Canadian law enforcement and the criminal justice system will face in deploying AI technology in the absence of robust and comprehensive frameworks and regulation.

2.4 Facial Recognition Technology

As discussed above, Facial Recognition Technology ("FRT") technology is known to have been deployed by Canadian law enforcement. This includes RCMP use of Clearview, and the scanning of arrest photo databases by law enforcement agencies including Toronto, York Region, Peel Region, Calgary and Edmonton. These examples are reviewed in more detail below. This section also takes a broader look at FRT technology with reference to the experiences of other jurisdictions highlights lessons that can be learned to assess the use of such technology in Canada.

2.4.1 FRT and Concerns for Efficacy, Reliability and Misuse

FRT is defined by the Information and Privacy Commissioner of Ontario as:

> "… an artificial intelligence (AI) technology that collects and processes sensitive personal information to identify or verify an individual's identity. FRT uses image processing software to analyze an individual's facial features, such as the width of the nose, the length of the jawline, and the distance between the eyes (e.g., as they appear in a photograph). FRT algorithms turn facial features into a faceprint of an individual. A facial recognition system can then compare two faceprints and return a similarity score or match faceprints by searching a reference database of a large number of images for a list of potential candidates whose similarity score is at, or above, a given threshold."[113]

FRT technologies may be applied to different forms of evidence and investigative procedures. A recent report of the International Network of Civil Liberties Organizations surveys how FRT may be used to:

- Analyze large collections of lawfully obtained evidence, such as digital images and videos in child pornography cases;
- Analyze images or video collected by third parties;
- Analyze evidence collected through video surveillance;
- Scan a large database of arrest photos (aka "mugshots"); and
- Engage in real-time identification through body cam or drone video feeds.[114]

The ambit of actual or potential FRT use may continue to expand. For instance, the Ontario Human Rights Commission has described a facial recognition "function creep," noting FRT watchlists can be used to identify:

(1) subjects of outstanding warrants;
(2) individuals who are unlawfully at large;
(3) individuals suspected of having committed crimes,
(4) individuals who may be in need of protection (e.g. missing persons)
(5) individuals whose presence at a particular event causes particular concern to law enforcement,
(6) persons simply of possible interest for intelligence purposes, and
(7) vulnerable persons.[115]

The creeping growth of FRT has been observed in other jurisdictions as well. For instance, in the United Kingdom, London Metropolitan Police use of FRT jumped from 32 instances in the three years beginning in 2020, to 117 instances reported between just January-August 2024. Over the course of these uses, some 770,966 different people had their faces scanned.[116]

Just as concerning is that FRT creep may not always include FRT transparency. A recent investigation into US police use of FRT determined that "police seldom

disclose use of facial recognition despite [the potential for] false arrests."[117] The study found that "police in 15 US states used facial recognition in 1,000+ cases since 2020" and "routinely failed to tell defendants about their use of the software."[118]

The appeal, of course, is that FRT can scan images and video faster than humans. Because scanning is automatic, FRT may improve the efficiency of law enforcement investigations and make resources – including labour intensive surveillance resources – available for other work.

Some also suggest that FRT can mitigate and reduce human biases and errors in facial recognition. However, early studies on the use of FRT raise several concerns about the efficacy and reliability of the technology, the potential for misuse, and the limitations of existing oversight policies and procedures. Most recently, for instance, the US Federal Trade Commission launched investigations to crack-down on firms with unproven claims that their AI-powered facial recognition technology achieves "zero gender or racial bias" and has "an accuracy as high as +99%."[119] Ongoing studies overseen by the US National Institute of Standards and Technology (NIST) rather found that the company's software "weren't even among the top 100 tested" FRT systems measuring for error rates in identifying age, sex and race.[120]

More broadly, the NIST tested 189 facial-recognition algorithms from 99 developers, including Microsoft, Cognitec, and Megvii (a Chinese AI company).[121] Overall, its findings confirmed that "[t]he majority of commercial facial-recognition systems exhibit bias" and "falsely identified African-American and Asian faces 10 to 100 times more than Caucasian faces."[122] The systems "also had more difficulty identifying women than men… [and] falsely identified older adults up to 10 times more than middle-aged adults."[123]

NIST Researchers pinpointed several issues with commercial facial recognition systems, including:

- **False positives:** These occur when the algorithm erroneously says two photos are the same person. Investigators who rely on the recommendation may then misidentify a suspect or potential investigatory lead. False positives occurred at a higher rate amongst Asian and American Indian individuals included in a set of domestic arrest photos. False positives also occurred at a higher rate in people born in Africa and the Caribbean when analyzing lower-quality images gathered at border crossings.[124]
- **False negatives**: These occur when the algorithm says two photos are two different people who look similar. False negatives are highest among West and East African, and East Asian individuals when using high-quality photos.
- **Gender**: False positives occurred at a higher rate in women than men. The facial matching algorithms used by law enforcement had the highest error rates for Black women.
- **Age**: False positive also occurred at a higher rate among both children and older adults.[125]

Several cases in the United States further illustrate the consequences of the known frailties of FRT, even where police do not solely rely on an FRT match as proof of identification.

In 2023, Porcha Woodruff, a Black mother of two in Detroit, Michigan, was eight months pregnant when six police officers knocked on her door and handed her an arrest warrant for charges related to carjacking and robbery.[126] She was detained for eleven hours. Ms. Woodruff later learned that her arrest and detention was the result of faulty human identification and a faulty facial recognition software match. According to The Guardian, as of August 15, 2023, Ms. Woodruff's case was the sixth known case in the United States of an arrest made due to false AI facial recognition.[127] In each of those six cases, the individual wrongly arrested was black. On the heels of Ms. Woodruff's civil lawsuit, the Detroit Police Department "banned the use of facial recognition photos in photo lineups" and recommended additional policy changes, including modifications to how photo line-ups were conducted.[128]

Other examples demonstrate that policies designed to minimize the risks of FRT use may not achieve that goal. The American Civil Liberties Union has noted that false identifications continue despite numerous law enforcement organizations agreeing that FRT matches are insufficient to positively identify a suspect.[129]

For instance, in 2022, police arrested Georgia resident Randall Reid based on a warrant issued in Louisiana. The warrant relied on an identification recommended by Clearview AI, a leading FRT software product. The FRT recommendation was accepted despite the user contract requiring police to "conduct further research in order to verify identities or other data generated by the [Clearview] system."[130] Reid spent nearly a week in jail, falsely accused of stealing purses in a state he said he had neveR. v.isited.[131] Lawyers eventually discovered that Mr. Reid was arrested because he resembled the suspect, who had been recorded by a surveillance camera.[132]

Procedural checks and balances may also be prone to selection biases and coercion. For instance, in 2023, investigators in Texas relied on the FRT system used in a Macy's department store to identify a suspected robber. It is further alleged that Macy's security then coerced the sales associate who had been held at gunpoint to confirm the identified photo as the suspect in a photo lineup. Based on this combination of FRT identification and allegedly coerced confirmation, police obtained an arrest warrant for the identified suspect. The suspect, however, lived 2,000 miles away from the robbery. When later visiting Texas, he was arrested and alleges that "he was beaten and raped by three men in a Texas jail bathroom." Hours after the assault, the charges were dismissed.[133]

2.4.2 FRT Use by Public Law Enforcement Institutions in the United States and Internationally

Despite the issues identified above, FRT continues to be widely deployed in the United States and internationally. Six US agencies reported using FRT on images of civil unrest to assist with criminal investigations following George Floyd's killing in May 2020: the Bureau of Alcohol, Tobacco, Firearms and Explosives; the US Capitol Police; the FBI; the US Marshals Service; the US Park Police; and the US Postal Inspection Service.[134] These agencies used governmental and non-governmental FRT to identify suspects in various criminal investigations, including those relating to assaults on law enforcement, threats against a member of Congress, destruction of government property, theft, burglary and arson.[135]

Three agencies also reported using FRT on images from the January 6, 2021, insurrection at the United States Capitol, including the US Capitol Police, US Customs and Border Protection ("CBP") and the Bureau of Diplomatic Security.[136] The US Capitol Police used Clearview AI to generate investigative leads, CBP used its "Automated Target System" to conduct searches on behalf of another federal agency and the Bureau of Diplomatic Security used the Department of State's Integrated Biometric System to search on behalf of another federal agency.[137]

The New York City Police Department ("NYPD") used FRT in at least 22,000 cases between 2016 and 2019.[138] This use was scrutinized because of the disproportionate impact on the city's marginalized communities. Amnesty International's "Ban the Scan" campaign found that "the higher the proportion of non-white residents" in a particular area, "the higher the concentration of facial recognition compatible CCTV cameras".[139] The NYPD continues to use FRT.[140]

In 2021, the United States Government Accountability Office found that nearly half of 42 federal agencies employing law enforcement officers used FRT.[141] Fourteen of those agencies used FRT to support criminal investigations. As of April 2022, over seven states and 20 municipalities had placed legislative limits on the use of FRT.[142] LCO research indicates this trend is accelerating. As of July 2024, 11 US states have enacted legislation that placed limits on the use of FRT, and four additional states have introduced legislation to do so.[143]

Australian law enforcement agencies also use FRT systems. In 2021, New South Wales and Victoria adopted FRT to monitor compliance with strict COVID-19 quarantine rules. The program sent "random check-in requests requiring residents to take a 'selfie' at their designated quarantine address".[144] The AI software would then verify the image against a 'facial signature'. If the image was not verified, the local police force would follow up in person to confirm the person's location.[145] Civil liberties organizations, including the New South Wales Council for Civil Liberties, raised concerns over the lack of governance relating to the application, making "it difficult to assess how privacy concerns are managed, how long data is being kept, who it's shared with, and how it is stored."[146] More generally, the use of FRT by law enforcement in criminal investigations has been criticized by the Australian Human Rights Commission, which, in 2021, described law enforcement's use of FRT without any legal framework as "deeply concerning".[147]

The European Union recently introduced significant presumptive restrictions on the use of FRT, biometric surveillance, and other law enforcement uses of AI. These are further discussed in section 2.4.5 below.

2.4.3 FRT Use by Public Law Enforcement Institutions in Canada

Multiple law enforcement agencies in Canada use investigative FRT. Three comprehensive public accounts of this use are summarized by:

- the federal *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada and Commissioners of Quebec, British Columbia and Alberta* (February 2021);[148]
- the federal Office of the Privacy Commissioner of Canada report on the use of FRT by the Royal Canadian Mounted Police (RCMP) in *Police use of Facial Recognition Technology in Canada and the Way Forward* (June 2021);[149] and
- the Information and Privacy Commissioner of Ontario, *Facial Recognition and Mugshot Databases: Guidance for Police in Ontario* (January 2024).[150]

A brief summary of these investigations and key findings is set out below.

FRT and Clearview AI

Clearview AI, an American-based company specializing in facial recognition software, garnered a significant amount of negative attention in early 2020. Clearview AI maintained a database of over three billion images of faces collected from publicly accessible online sources.[151] Reports suggest that Clearview populated its FRT database "by collecting digital images from a variety of public websites, including but not limited to, Facebook, YouTube, Instagram, Twitter and Venmo, in apparent violation of those organizations' terms of service and without the consent of individuals."[152] The images were aggregated and assigned biometric identifiers, with correlations made to metadata associated with the images such as the webpage title, source link and text descriptions.[153] A Clearview user could upload a new image, obtain a list of matching images within the database, and view the original online source.

Canadian law enforcement's use of Clearview AI attracted negative attention in early 2020 when reports emerged that several agencies were using the technology.[154]

These events triggered a joint investigation into law enforcement's use of Clearview AI by privacy commissioners in Canada, Quebec, BC and Alberta, and also lead to a separate follow-up report on the RCMP's use of FRT technology. The Privacy Commissioner of Canada concluded that "[t]he result [of the use of FRT] was that billions of people essentially found themselves in a "24/7" police line-up."[155] These reports found, amongst other things, that:

- Clearview AI's collection, use and disclosure of personal information through its facial recognition tool "represents the mass identification and surveillance of individuals by a private entity" and does not comply with federal and provincial privacy laws;
- Clearview collected, used and disclosed the personal information of individuals in Canada for inappropriate purposes;
- The practice of "scraping" information from sources such as social media, professional profiles, and other public websites – and using that information for an unrelated purpose – does not satisfy the "publicly available" exception under federal and provincial privacy legislation (a legal definition distinct from a common understanding of "publicly accessible" information);[156]
- Scraping information and using it for purposes unrelated to the purpose for which the images were originally posted creates the risk of significant harm to individuals captured by those images;
- FRT technologies can result in misidentification. The technologies have significantly higher incidences of false positives or misidentifications when assessing the faces of people of colour, and especially women, which can result in discriminatory treatment;
- FRT can render racially biased results and has the potential to erode privacy and undermine freedoms and human rights;
- A government institution cannot collect personal information from a third-party agent where that information was collected unlawfully; and
- Clearview's large collection of sensitive biometric information made it a high value target for malicious actors. There had been two significant breaches of Clearview's database in the year preceding the report.[157]

Some Canadian investigative agencies, including law enforcement in Regina, London, Cornwall and Toronto, asserted that Clearview AI was used primarily by individual officers who obtained access on a trial basis, at times without the knowledge or approval of senior leadership.[158] The RCMP admitted to a limited use of Clearview AI on a "trial basis by a few units in the RCMP to determine its utility to enhance criminal investigations."[159] The RCMP said that Clearview AI had been used primarily to identify and rescue children suspected of being victims of online sexual abuse. However, the Privacy Commissioner's "investigation found the RCMP did not satisfactorily account for the vast majority of the searches it made."[160]

FRT and Arrest Photo ("Mugshot") Databases

Local and regional provincial police forces also use FRT software to scan arrest photo databases. This includes police services in Toronto, York Region, Peel Region, Calgary and Edmonton who use AI systems to compare still images with a database of "mugshots" collected by police.[161] The Information and Privacy Commissioner of Ontario (IPCO) investigation flags privacy-related concerns over the collection, use, disclosure and retention of biometric facial data for FRT purposes under the federal *Identification of Criminals Act*,[162] noting that Canadian courts have held repeatedly that non-conviction information collected by police forces, such as fingerprints and mugshots, attract s. 8 protection.[163] At the same time, a search and seizure that affects rights under section 8 is lawful where it complies with the *Collins* test, with the *Identification of Criminals Act* arguably providing sufficient authority to meet that test.[164] In addition to the concern raised by this legal tension, the IPCO additionally raise concerns about the technical performance of FRT in terms of reliability and accuracy, lack of standards governing image quality, lack of error correction, and whether FRT perpetuates bias.[165]

A key concern with AI-enabled systems is that they draw on these data sets to detect patterns and make recommendations that can – or are likely to – reproduce systemic biases.[166] Arrest photo databases are known to reflect patterns of racial profiling and discrimination of Black persons in Toronto. In their 2020 report *A Disparate Impact: Second interim report on the inquiry into racial profiling and racial discrimination of Black persons by the Toronto Police Service*, the Ontario Human Rights Commission found that:

- The charge rate for Black people was 3.9 times greater than for White people and 7.1 times greater than the rate for people from other racialized groups.
- Although they represented only 8.8% of Toronto's population in 2016 Census data, Black people represented 42.5% of people involved in obstruct justice charges and were 4.8 times more likely to be charged with obstruct justice offences than their representation in the general population would predict. By contrast, White people and people from other racialized groups were underrepresented.
- Black people represented 35.2% of people involved in "out-of-sight" driving charges (such as driving without valid insurance) – charges that arise only after a stop had already taken place. This suggests other motives for the stop, including both legitimate and illegitimate reasons.
- Black people represented 37.6% of people involved in cannabis charges and were 4.3 times more likely to be charged with a cannabis possession offence despite conviction rates and many studies showing that Black people use cannabis at similar rates to White people.
- Despite being charged at a disproportionately higher rate, Black people were overrepresented in cases that resulted in withdrawn charges. Their cases were also less likely to result in a conviction compared to cases involving White people. [167]

Arrest photo database FRT can also lead to errors outside of the criminal law sphere. For instance, in *Ali v. Canada (Public Safety and Emergency Preparedness)*, the Federal Court found that the refugee and permanent resident status of a Somali applicant was rescinded based on a photographic mismatch.[168] The Court held that the "Applicant was entitled to more than an assurance that facial recognition technology was not employed, given the high level of procedural protections required in vacation proceedings… and potential for severe consequences resulting from the proceedings."[169] Proceedings meant to take away the protection of someone who fled persecution require "a high level of procedural fairness… [which] includes a full opportunity for refugees to challenge the evidence supporting the request to vacate status, which in turn entails the provision of information to refugees regarding the source and methodology used to obtain the evidence being used against them."[170]

2.4.4 FRT Use by Private Entities

The private sector also uses FRT for surveillance, which may be accessed or relied upon by law enforcement. For instance, three major Australian retailers implemented FRT to capture the biometric data of their shoppers.[171] In 2018, Amazon filed two patent applications that consider using its Ring doorbell device to recognize "suspicious" people and automatically alert law enforcement.[172] Ring described that the facial recognition alert would work as follows:

> A video may be analyzed by an A/V recording and communication device that recorded the video (and/or by one or more backend servers) to determine whether the video contains a known criminal (e.g., convicted felon, sex offender, person on a "most wanted" list, etc.) or a suspicious person. Some of the present embodiments may automatically submit such a video stream to the law enforcement agencies.[173]

Private entities also use FRT. For instance, a joint investigation by privacy commissioners of Canada, Alberta and BC found that major Canadian mall operator Cadillac Fairview Corporation installed and used "Anonymous Video Analytics (AVA) technology installed in "wayfinding" directories" to track mall customers.[174] The AVA technology:

- took temporary digital images of individual's faces within the camera's field of view;
- used facial recognition software to convert those images into biometric numerical representations of the individual faces; and
- used that information to assess age range and gender.

Cadillac Fairview established a database that "collected and stored approximately 5 million numerical representations of faces" and "used personal information, including sensitive biometric information, via the AVA technology without valid consent."[175]

There is considerable concern over the legality of disclosure of third party FRT information to entities like law enforcement, an issue which is discussed in more detail below in section 3.3 "Warrantless Requests by Law Enforcement for Private Information."

2.4.5 Restrictions and Prohibitions on the Use of FRT in Canada and Elsewhere

Overall, the privacy commissioner reports conclude that:

> Despite the intended benefits of facial recognition systems, FRT technology raises significant legal, privacy, and ethical challenges given its potential to provide biased or inaccurate results and undermine rights and freedoms. Jurisdictions around the world continue to struggle with how to regulate its use.[176]

To date, the lawfulness of FRT use by law enforcement has yet to be comprehensively subject to a set of clear legal rules in Canada or Ontario. Other jurisdictions have introduced legislation and other forms of regulation that suggest options available in Ontario.

For instance, several American jurisdictions have limited law enforcement's use of FRT.

The Policing Project at the New York University Faculty of Law reports that three cities – San Francisco, Oakland, and Somerville (Mass.) – adopted ordinances banning the use of FRT by city officials, including law enforcement.[177] Eleven states have also enacted legislation that regulates FRT, including Alabama, Colorado, Maine, New York, and Washington.[178] Most recently in May 2024, Maryland state lawmakers unanimously enacted the "strongest facial recognition rules for law enforcement yet" and will limit "law enforcement's use of facial recognition systems to specific uses and outlines measures agencies must take to document and publish how they use the technology during investigations."[179] These include limits "to the investigation of certain crimes, including violent crime, human trafficking, child abuse, child pornography, hate crimes, and certain weapons crimes" while prohibiting law enforcement from using FRT "on images or recordings of individuals engaging in protected activity, such as protest."[180]

The European Union presumptively prohibits the use of FRT and other AI-enabled biometric systems through the recently enacted 2024 *Artificial Intelligence Act* (AIA).[181] Presumptively prohibited uses of AI systems include:

- biometric categorisation systems (including but not limited to FRT) which are used to infer sensitive attributes (race, political opinions, trade union membership, religious or philosophical beliefs, sex life, or sexual orientation);
- assessing the risk of an individual committing criminal offenses solely based on profiling or personality traits;
- compiling facial recognition databases by untargeted scraping of facial images from the internet or CCTV footage;
- "real-time" remote biometric identification (RBI) in publicly accessible spaces for law enforcement.[182]

Law enforcement may use biometric systems in exceptional and prescribed circumstances. These only arise "when not using the tool would cause considerable harm" and is subject to "authorisation from a judicial authority or independent administrative authority" in all circumstances other than the most urgent.[183] For instance, "real-time remote biometric identification" may be used when:

- searching for missing persons, abduction victims, and people who have been human trafficked or sexually exploited;
- preventing substantial and imminent threat to life, or foreseeable terrorist attack; or
- identifying suspects in serious crimes (e.g., murder, rape, armed robbery, narcotic and illegal weapons trafficking, organised crime, and environmental crime, etc.).[184]

Other obligations apply to such uses, including that such AI systems:

- shall be deployed for the purposes set out in that point only to confirm the identity of the specifically targeted individual;
- include an assessment of the seriousness, probability and scale of the harm that would be caused if the system were not used;
- include an assessment of the consequences of the use of the system for the rights and freedoms of all persons concerned;
- are previously subject to a completed fundamental rights impact assessment and the system is registered in the EU database; and
- provide notice of each use of a 'real-time' remote biometric identification system in publicly accessible spaces for law enforcement purposes to the relevant market surveillance authority and the national data protection authority; and
- that notices be published in publicly available annual reports.[185]

To date, Canadian jurisdictions have not legislated prohibitions on the use of FRT. However, several legislative and policy proposals may touch on FRT.

In June 2022, the Government of Canada tabled the *Artificial Intelligence and Data Act* (AIDA) as part of Bill C-27, the *Digital Charter Implementation Act, 2022*.[186] AIDA proposes to develop a regulatory definition to govern private sector development of "high-impact AI systems."[187] While regulations have not yet been introduced, the sponsoring Minister of Innovation, Science, and Industry wrote to parliament and clarified circumstances where AI systems are likely to be "high-impact." This includes:

- "The use of an artificial intelligence system to process biometric information in matters relating to (a) the identification of an individual;"
- "The use of an artificial intelligence system to assist a peace officer, as defined in section 2 of the Criminal Code, in the exercise and performance of their law enforcement powers, duties and functions;" and
- "The use of an artificial intelligence system by a court or administrative body."[188]

AIDA would require that systems identified as "high-impact" takes steps to "identify, assess, and mitigate risks of harm or biased output prior to a high-impact system being made available for use."[189] The measures identified in AIDA include:

- human oversight and monitoring of the AI system;
- transparency, including published public information about the existence and use of a system, as well as descriptions of the capabilities, limitations, and potential impacts;
- mitigation of discriminatory outcomes for individuals and groups;
- proactive assessment to identify harms that could result from use of the system, including through reasonably foreseeable misuse;
- accountability and governance mechanisms; and
- validation and robustness testing.[190]

To date the AIDA is stalled at second reading in a prorogued Parliament. It is unclear if amendment motions to establish "courts" and "law enforcement" as high-impact sectors will be adopted, or if the AIDA (or some variation on it) is likely to be reintroduced in a future parliament.

The federal government also introduced a Directive on Automated Decision-making and an Algorithmic Impact Assessment tool (AIA).[191] The tool is commendably detailed and sophisticated, and the LCO has written about it extensively. However, law enforcement is broadly exempt from the ambit of the Directive and AIA (although they can voluntarily follow it at their discretion).

Meanwhile, in May 2024, Ontario introduced the *Enhancing Digital Security and Trust Act, 2024* as part of Bill 194, the *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*.[192] The legislation would govern the use of artificial intelligence systems in public sector entities.

The LCO has provided extensive analysis of the strengths and limitation of Bill 194.[193]

In the main, the legislation is quite short and provides few specifics. It is framework legislation that enables regulatory powers to "prohibit" high risk AI technologies and "exempt" others in specific circumstances. But as introduced, the Bill provides few specifics. It only targets a limited number of public sector institutions – namely schools, universities, Children's Aid Societies, and hospitals – but is understood to likely to expand to cover other public sector institutions in the near future.

Consequently, there are significant gaps. For example, Bill 194 does not address AI systems used by police or by courts and tribunals, meaning that these institutions could adopt predictive policing, facial recognition and other forms of biometric surveillance, and automated risk assessments without having to comply with provincial AI accountability requirements.[194]

Finally, the privacy commissioner investigation into Clearview AI concluded in December 2021 with orders from privacy commissioners in BC, Alberta and Quebec binding Clearview to:

- Stop offering its facial recognition services that have been the subject of the investigation in the three provinces;
- Stop collecting, using and disclosing images of people in the three provinces without consent; and
- Delete images and biometric facial arrays collected without consent from individuals in the three provinces.[195]

The Commissioner's further noted "significant shortcomings" with the federal private sector privacy law and provincial privacy laws that undermine effective oversight of AI technologies, including:

- "order-making powers;"
- "quick and effective enforcement mechanisms;"
- the ability "to issue orders and impose significant monetary penalties," and
- "meaningful penalties [to] create strong incentives for businesses to comply with the law."[196]

As discussed below in section 3.1.2, police forces including the Toronto Police Services and RCMP have recently made efforts to more proactively manage the risks and benefits of AI by developing technology assessment, review and authorization schemes applied prior to the procurement and deployment of high-risk AI technology.

Overall, the risks associated with FRT merit some consideration of more detailed legislative or regulatory guidance. For instance, the recent report of the 15-member International Network of Civil Liberties Organizations (INCLO) highlights the fundamental rights at risk with police use of FRT, including:

- Rights to dignity, meaning people are not treated as objects.
- Rights to privacy, including associated rights that depend on privacy such as freedom of movement and association.
- Rights to freedom of expression, peaceful assembly and association.
- Rights to the protection of personal data, particularly the processing and correlating of data without consent.
- Rights to equality and non-discrimination, particularly in targeting specific populations and increased error rates among certain demographics, and persons with disabilities who may be deemed less trustworthy by FRT systems.
- Rights to the presumption of innocence, recognizing that as FRT systems scan databases of images the entire population is treated as a suspect.
- Rights to effective remedies and fair trials, meaning procedural fairness and Charter rights must be preserved.[197]

INCLO concludes that:

> "As legislators are passing laws for FRT use with inadequate guardrails for fundamental rights, courts are increasingly tasked with understanding and adjudicating on the risks. […] [Accordingly] We advocate for adopting even higher standards tailored to the specific circumstances of each jurisdiction to ensure the protection of human rights and the integrity of law enforcement practices."[198]

2.5 Predictive Policing

Predictive policing technology is known to have been deployed by Canadian law enforcement, including the Vancouver Police Department, Calgary Police Service and the Ontario Provincial Police ("OPP"). This and other examples are reviewed in more detail below. This section also takes a broader look at predictive policing technology with reference to the experiences of other jurisdictions highlights lessons that can be learned to assess the use of such technology in Canada.

2.5.1 Predictive Policing and AI

Predictive analytics refers to algorithmic systems that analyze large datasets, including historical crime data, to try to predict or 'forecast' future crime.

In their 2020 report *To Surveil and Protect*, The Citizen Lab at the University of Toronto clarifies that there are two main categories of algorithmic predictive policing:

- **Location-based** algorithmic policing systems "purport to identify where and when potential criminal activity might occur [by using] algorithms that drive these systems [to] examine patterns and correlations in historical police data to attempt to make predictions about the future."[199]
- **Person-based** algorithmic policing systems are "designed to identify individuals who are likely to be involved in future criminal activity [… or] to assess what level of risk a particular individual has for either engaging in or being the victim of future criminal activity [… by processing] personal details, such as information about family, friends, or associates; their social media activity; criminal records; or appearance in other police databases…"[200]

The use of predictive policing technology is typically characterized as a "technological promise" aimed at "revolutionizing law enforcement."[201] Professor Andrew Ferguson, a leading US scholar on predictive policing, writes of the promise where "data-driven insights [are] operationalized into concrete decisions about police priorities and resource allocation… offering police administrators the ability to identify higher crime locations, to restructure patrol routes, and to develop crime suppression strategies based on the new data."[202]

Ferguson further notes how predictive technologies intentionally or unintentionally forefront "decisions about the type of policing response that makes sense in their community" and "how police can choose between prioritizing additional police presence, targeting environmental vulnerabilities, and/or establishing a community problem-solving approach as a different means of achieving crime reduction."[203]

The experiment is in full swing. Major US cities have redesigned their police patrols based on predictive policing models through which "officers are provided daily computer-generated maps of areas to patrol, and… patrol car mobile devices provide almost real-time updates of crime patterns as they patrol."[204]

Concurrently, Fergusson also writes how predictions about people and places based on historical data and patterns of policing raise several significant concerns and question the efficacy and reliability of the technology as an investigative tool. "At its worst," Ferguson writes, predictive policing "can create a proxy for racially biased police presence in already over-policed neighborhoods and generate increased police-citizen tension."[205]

Additionally, Ferguson outlines several other concerns that predictive policing systems:

- Are all relatively new with most continuing to evolve and change;
- Are all relatively untested with only a handful of studies or empirical validation studies;
- May be based on proprietary technology owned by private entities;
- May be procured by law enforcement with little public oversight or input, and based on local rules.[206]

Real-world studies seem to evidence the notion that predictive policing technologies have their limitations. Chief among these is the propensity to reproduce historical patterns of biased and discriminatory investigative practices. Several independent investigations in the press have found that:

> popular "predictive" policing tools trained on historical crime data often replicate long-held biases, offering law enforcement, at best, a veneer of scientific legitimacy while perpetuating the over-policing of predominantly Black and Latino neighborhoods. An October headline from The Markup states bluntly: "Predictive Policing Software Terrible At Predicting Crimes." The story recounts how researchers at the publication recently examined 23,631 police crime predictions—and found them accurate roughly 1 percent of the time.[207]

Findings from a two-day workshop convened in June 2024 by the US National Academies of Sciences, Engineering, and Medicine found that implementation and deployment are key factors in limited instances among a review of 161 studies where predictive policing had some measure of success. Among instances where "limited" or "moderate" effectiveness of predictive policing approaches were found, the studies found that "matching a prediction to an appropriate intervention is a key element of effective predictive policing."[208]

If it is the case that AI-based "prediction models need to be paired with tailored interventions in the field" it suggests that AI assessment and responsible use laws or policies will only strike a balance and achieve responsible use where they emphasize not just safety, reliability, testing, and basic validation, but be very thorough in assessing, prescribing, and training police on appropriate and effective (and ineffective) deployments in the real world.[209]

Despite these empirical concerns, predictive policing technologies are known to have been deployed in both the United States and in Canada. These examples highlight the practical and systemic limitations of AI oversight through the criminal justice system.

2.5.2 Use of Predictive Policing by US Law Enforcement

The use of predictive policing is gradually spreading across the US. A study conducted in 2016 determined that twenty of the largest fifty police departments in the US use predictive policing (40%) while 36% of the remaining thirty departments are exploring options to use the technology.[210]

This follows from a decision in in 2009 by the U.S. National Institute of Justice to start issuing grants for predictive policing pilot projects.[211]

The Chicago Police Department used one of these grants to launch a program that generated a list of people believed to be at a high risk of gun violence.[212] The algorithm examined arrest data and whether an individual was socially connected with a known shooter or shooting victim. Police and social workers then attempted to conduct 'pre-crime' interventions with identified individuals. However, the only statistical correlation between individuals on the list and gun-violence was that the identified individuals were more likely to be arrested for a shooting. The list became a "data-driven 'most-wanted' list" for Chicago police, and not a tool to assist those deemed to be at "high-risk."[213]

Using Palantir Technology's purported crime-forecasting software, law enforcement in New Orleans generated a list of individuals who were believed to be more likely to commit or become a victim of gun violence.[214] The software analyzed people's social media, criminal databases, and associations to known gang members. The program ran in secret for six years and was terminated shortly after its use was made public.[215]

The Los Angeles Police Department (LAPD) has also experimented with predictive AI. In 2011, for example, the LAPD launched Operation Laser, a location-based algorithm that mapped "problem areas" based on historical crime data. Officers were directed to focus their efforts on the "problem areas." The program was criticized for validating biased policing patterns and criminalizing Black and Brown communities that were over-represented in the historical data.[216]

Nevertheless, the LAPD continued to pilot the use of new predictive policing technology. For instance, in 2021, the LAPD partnered with Voyager Analytics on a trial basis to use an AI system that purports to detect emerging threats to public safety based on a person's social media activity.[217] It was later disclosed that the software was used on over 15,000 Facebook users located in California.[218]

In 2023, the Guardian reported that the NYPD had entered into a nearly $9 million contract with Voyager Labs in 2018, purchasing "products the company claims can use artificial intelligence to analyze online behaviour and detect and predict fraud and crimes".[219] The NYPD renewed the contract in 2021, and confirmed to the Guardian in September 2023 that it was still working with Voyager.[220]

Predictive policing techniques are also ensnaring private entities in control of vast amounts of personal data. For instance, social media companies are raising concerns over mass "profile scraping" for the purposes of predictive policing, along with the creation of fake accounts to further other investigative purposes. In mid-November 2021, Facebook wrote to the Chief of the LAPD demanding that the LAPD cease creating fake profiles to conduct surveillance on users.[221] They indicated that the creation of false accounts for "online investigative activity" violated Facebook's terms of service, and noted that:

> "...officers must abide by Facebook's policies when creating accounts on our services… People on our platforms speak their minds, connect with others…and organize First Amendment protected activities. It is our intention that they do so in a space that is free from unlawful surveillance by the government or agents acting in inauthentic ways."[222]

Facebook also noted that developers were prohibited from using data obtained from their platform for surveillance for law enforcement or national security purposes.[223] In early January 2023, Meta (parent company for Facebook) filed a lawsuit against Voyager Labs, alleging that Voyager Labs had unjustly enriched itself at Meta's expense. [224] As of May 2024 the case continues to move forward.[225]

The use of predictive policing in the United States is increasingly attracting political attention.

In January 2024, seven members of US Congress and Senate wrote to the Department of Justice (DoJ) concerned that state and local police agencies are being awarded federal grants to buy "AI-based policing tools known to be inaccurate, if not prone to exacerbating biases long observed in US police forces."[226] The DoJ was encouraged to stop all "grants for predictive policing systems until the DOJ can ensure that grant recipients will not use such systems in ways that have a discriminatory impact."[227] The letter reminded the DoJ that they are "patently forbidden from funding programs shown to discriminate on the basis of race, ethnicity, or national origin, whether that outcome is intentional or not."[228]

Despite this obligation, the letter further emphasizes the lack of oversight and evidence-based assessment of these tools, noting how the DoJ "had not kept track of whether police departments were using the funding… to purchase so-called predictive policing tools" nor assessing "the accuracy and precision of predictive policing models across protected classes, their interpretability, and their validity… to determine which predictive models are discriminatory—and then reject funding for all those that fail to live up to them."[229]

2.5.3 Use of Predictive Policing by Canadian Law Enforcement

Canadian law enforcement also uses predictive software.[230] For instance, the Vancouver Police Department has used the GeoDASH system in combination with an algorithmic system to try to predict where break-and-enter crimes are more likely to occur within a 2-hour window.[231] Uniformed officers then patrol areas identified as high-risk to try to deter potential crime. The system purports to include some checks-and-balances against over-policing, including the manual creation of "exclusionary zones," designated areas to which officers will not be sent, and instructing officers that the forecasting of an area as high-risk cannot be used as grounds for a street check.[232]

Both the Calgary Police Service and the Ontario Provincial Police ("OPP") have also made use of Palantir's Gotham system. The product website describes the product as "a commercially-available AI-ready operating system that improves and accelerates decisions for operators across roles and all domains."[233] As recently as 2022, the OPP has refused to disclose publicly how it uses the program, purportedly "…to protect investigative and intelligence techniques."[234] The Calgary Police Service also uses the product, but says it does not use it for "predictive or algorithmic policing", only for "social network analysis."[235]

2.5.4 Criticism of Predictive Policing Software

As noted by the Ontario Human Rights Commission, predictive policing systems based on "good data, good decisions and appropriate deployment – in full compliance with the Code and the Charter – can produce positive public safety outcomes."[236] However, "the opposite can happen when predictive policing is used improperly."[237]

Generally speaking, the primary technological concern with predictive algorithms rests in the reliance on training data that imports and learns from patterns of systemic discrimination. The use of technologies reliant on historical data may undermine trust in policing practices where they unfairly target or focus on particular communities.[238] Through the "ratchet effect," any initial bias in the AI's training data is amplified as the information generated by the biased algorithm is fed back into the system through law enforcement decisions. The system then generates even more biased information.[239] Indeed, where "historical data from police practices is used to train the algorithm" it may lead to "forward-looking decisions that both reflect and reinforce past beliefs about which neighbourhoods (or which people) are 'safe' or 'dangerous'."[240] This may lead to further over-policing and continued systemic discrimination against marginalized communities.

In a 2024 statement the National Association for the Advancement of Colored People (NAACP) write that there is:

> "growing evidence that AI-driven predictive policing perpetuates racial bias, violates privacy rights, and undermines public trust in law enforcement. The data used to make decisions around predictive policing comes from compiling and analyzing historical criminal data and police activity. Relying on historical criminal data to make policing decisions is inherently biased, as data shows that the Black community is disproportionately negatively impacted in the criminal justice system due to targeted over-policing and discriminatory criminal laws."[241]

However, testing underlying biases of these systems in a courtroom may be difficult given the opacity of many AI algorithms, the technical difficulty of explaining algorithms, and corporate interests resistant to sharing information about a particular program or algorithm,[242] among other concerns cited by Professor Ferguson above in s. 2.2.1.

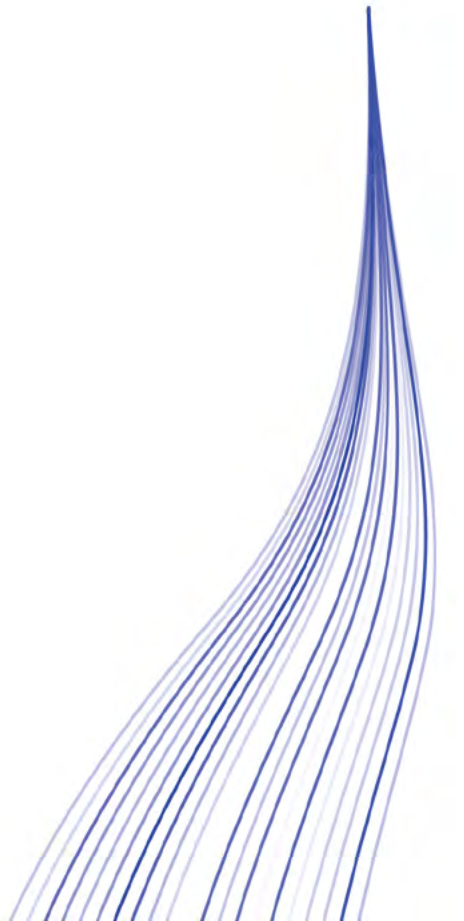
The extent of AI's potentially negative impact on equality and fairness has not yet been fully grasped or litigated in Ontario. But forward-looking studies suggest predictive policing is likely to raise significant legal concerns for human rights and Charter rights. In their 2019 report *Policy on Eliminating Racial Profiling in Law Enforcement*, the Ontario Human Rights Commission identifies several concerns about the objectivity of predictive policing software, including concerns for:

- Biased data;
- Self-justifying feedback loops;
- Data inputs that correlate with race by proxy;
- Biased police deployment;
- Perpetuating existing biases; and
- Conducting risk assessments based on social networks.[243]

Given these concerns, the OHRC emphasizes how "law enforcement use of predictive policing must be attuned to the dangers of *Human Rights Code* violations and adverse impacts and take measures to make sure such dangers do not emerge… [such as by] conducting impact assessments of predictive technologies before they are procured and used, and amending or abandoning these technologies if they are found to generate discriminatory outcomes."[244]

For their part, the 2024 statement from the NAACP makes five recommendations respecting predictive policing software and practices as follows:

- "Implement Rigorous Oversight: Establish independent oversight bodies to review and monitor the use of AI in policing, ensuring algorithms are fair, accurate, and non-discriminatory.
- Mandate Transparency and Accountability: Require law enforcement agencies to disclose the use of predictive policing tools, including the data sources, methodologies, and impact assessments.
- Promote Community Engagement: Involve community members in the decision-making process regarding the use of AI in law enforcement to build trust and accountability
- Ban the Use of Biased Data: Prohibit the use of historical crime data and other sources known to contain racial biases in predictive policing algorithms.
- Establish Legal Frameworks: Enact legislation to regulate the development, deployment, and evaluation of AI in policing, with strict penalties for violations of civil liberties."[245]



2.6 Object Recognition

Several law enforcement agencies use AI-based object recognition, which includes systems that automatically recognize and report certain features in video or audio data.

Some experimental uses of AI object recognition include:

- automatic detection of guns and other indicators of criminal activity in CCTV surveillance footage[246]
- a system to automatically determine who was at fault in a car accident,[247] and
- uses in forensic science, such as for impression and pattern analytics and crime scene evidence detection.[248]

Several potentially problematic AI object recognition tools are widely used. These are discussed below.

2.6.1 Automated License Plate Readers (ALPR)

Automated license plate readers (ALPR) read and record the license plates of vehicles scanned by infrared cameras on highways and check them against a database using pattern recognition software. In Ontario, police have access to a Ministry of Transportation and CPIC "hot list" – a database which lists vehicles in poor standing for issues like suspended licence plates or plates associated to people with outstanding warrants or who have been reported as missing.[249] The ALPR scans plates and notifies the officer of a "hit." In February 2023, the OPP announced an expansion to the ALPR system, making the system available to every OPP vehicle across Ontario.[250] The change allows police to scan "hundreds of license plates within minutes" while on the road.[251]

Despite broad police enthusiasm for ALPR,[252] the increasingly widespread use of ALPR cameras has led to fears that they may result in "dragnet-style" mass surveillance, especially in the US. ALPR cameras typically collect data on every car they scan, including the date, time, and location of the scan.[253] A 2021 Electronic Frontier Foundation analysis of ALPR systems in California found that 99.9% of the data is not related to any investigation when it is collected.[254]

Commentators further point out that:

- ALPR data is often collected without informing the public;
- ALPR scanning can be applied retroactively to years- or decades-old surveillance footage; and
- ALPR databases are typically governed by public-private partnerships – such as surveillance systems at malls or smart doorbells[255] – that may prevent police from disclosing the extent of data at their disposal.[256]

Police ALPR and other video surveillance databases across the US may also be integrated with private databases that expand the systems' overall scope.[257] The expansion and normalization of private sector ALPR has been criticized for invading personal privacy, facilitating discriminatory risk profiling in car financing and insurance, and may be disproportionately applied to lower income drivers.[258]

ALPR can also be combined with other sensors to create comprehensive object recognition systems. Professor Ferguson writes that such systems amount to "warrantless persistent surveillance:"

> These are the new realities of digital surveillance: technologies that are massive in scope, enduring in memory, retrospective, pervasive, and persistent.
> [...]
> Persistent surveillance raises different questions than traditional surveillance because the technologies operate at a different scale, duration, and reach than traditional investigative techniques. A plane that can record an entire city is simply not the same thing as a plane that flies over a single backyard. A network that captures all cell phone locations is not the same thing as a device that finds one phone's location... [yet] law has not fully recognized this shift in systemic surveillance capacity, and courts have struggled to adapt old law to new technologies.[259]

Indeed, these tensions are beginning to attract litigation.

In *Commonwealth v McCarthy*, the Massachusetts Supreme Judicial Court held that law enforcement's limited use of ALPR technology did not breach Fourth Amendment privacy rights but suggested that hypothetical "widespread use" could.[260] Police had tracked the defendant, who was accused of drug trafficking, using four cameras mounted at two locations.[261] The judge noted that "with enough cameras in enough locations," ALPR surveillance could reveal enough details about innocent people's lives to constitute a breach of the Fourth Amendment "because the whole reveals far more than the sum of its parts."[262] A similar line of reasoning is reflected in an Illinois lawsuit commenced in June 2024. It alleges that police use of ALPR already "amounts to dragnet surveillance" and seeks to end the use of ALPR in the state.[263] The suit asserts that with ALPR police:

> "are tracking anyone who drives to work in Cook County — or to school, or a grocery store, or a doctor's office, or a pharmacy, or a political rally, or a romantic encounter, or family gathering — every day, without any reason to suspect anyone of anything, and are holding onto those whereabouts just in case they decide in the future that some citizen might be an appropriate target of law enforcement."[264]

Consequently, the suit "challenges the warrantless, suspicion-less, and entirely unreasonable tracking as a violation of the Fourth and 14th amendments."[265] In Canada, the correlation of otherwise disparate breadcrumbs of our digital trail is also attracting judicial attention: see the sidebar below: "**How is Canadian Criminal Law Concerned for Data-based Surveillance? Implication of *Bykovets* for AI use by Law Enforcement."**

Critics of ALPR systems also point to developers' poor data security record, which is concerning considering the extent and sensitivity of the information collected. In June 2024, the Cybersecurity and Infrastructure Security Agency (CISA) of the US Department of Homeland Security released an advisory statement outlining major cybersecurity vulnerabilities in Motorola Solutions' Vigilant, a dominant player in the ALPR market.[266] For the private-sector developers of ALPR and similar systems, critics suggest that "the temptation to 'collect it all' continues to overshadow the responsibility to 'protect it all.'"[267]

All of that considered, many concerns about ALPRs arise from the potential that the system will retain all the information it obtains from scanning license plates and could be put to additional uses. In the alternative, ALPR could be implemented differently by, for example, checking each plate against a "hot list" of interest to police, and then discard information about any plate that is not a match, or having clear data retention and use policies in place and subject to annual audits and reporting. The issue highlights how well-founded concerns with AI-related technology may be ameliorated through operational implementation practices that balance or protect rights by design.

How is Canadian Criminal Law Concerned for Data-based Surveillance? Implication of *Bykovets* for AI use by Law Enforcement.

The concern for correlating disparate and otherwise innocuous piece of data for investigative and disclosure purposes is of live legal concern in Canada. Recent criminal law decision of the Supreme Court of Canda (SCC) indicates that courts are mindful of this "mosaic" and the privacy and civil liberty risks inherent in the age of "big data" investigations and may indicate trouble ahead for AI-assisted investigations.

In *R. v. Bykovets*,[268] the Supreme Court ruled that Canadians have a *Charter* section 8 privacy interest in their internet protocol (IP) addresses – digital identifiers used to track individual devices' internet activity – even when those IP addresses are not directly matched with users' biographical information.[269] This means law enforcement must obtain a search warrant to collect IP addresses from third parties such as websites,[270] which regularly log IP addresses and have historically provided them freely to police.[271] Although it does not address AI-powered policing tools explicitly, *Bykovets* has significant consequences for law enforcement's ability to collect and manage the data those tools rely on.

Key to the court's decision is its recognition that even information that is meaningless on its own (after all, an IP address by itself is only a "string of numbers") may "betray deeply personal information" when correlated with other seemingly innocuous data.[272] Justice Karakatsanis noted that

> [w]ithout the protection of s. 8, nothing prevents the state from pre-emptively collecting IP addresses and comparing that user's IP address against their database. Further, and significantly, the scope of information that an IP address can reveal is enormous if correlated against information held by a third party.[273]

For example, compiling various websites' IP address logs can reveal a device's online financial transactions, social media activity, and Google search history over a certain period of time.[274] This information is often sufficient to identify the individual user.[275]

Beyond specific police investigations, *Bykovets* substantially limits law enforcement's ability to collect data that could be used to train and operate AI-powered systems. A hallmark of AI is its ability to use minimal, anonymous data points to generate remarkably specific predictions and identifications – sometimes in ways that are not even understood by the tool's human developers. By prohibiting their collection of such data *en masse* from third parties, *Bykovets* makes it impossible for police to take full advantage of this functionality using their own in-house databases.

Overall, *Bykovets* may indicate the Supreme Court's willingness to regulate state-controlled AI systems judicially through a broad application of section 8. However, the *Charter*'s application only to state action may cause unintended consequences. For example, *Bykovets* may push police to rely on third-party AI tools powered by third-party databases (which may be subject to less government oversight or none at all), or to develop tools using exclusively police-generated data (which may exhibit greater bias than data possessed by third parties). The decision thus speaks both to the significant role of the courts in AI and privacy regulation and to the need for broader legislative and institutional reform.

2.6.2 ShotSpotter

ShotSpotter has been used in nearly 100 US cities. The technology uses thousands of microphones installed across cities with the goal of automating detection of gunshot sounds and dispatching police to the area.[276] When a loud sound is detected by at least three microphones, the ShotSpotter system uses algorithmic processes to determine if the sound was caused by a gunshot.[277]

ShotSpotter claims its system is 97% accurate, however this figure has been challenged by experts and described as unsubstantiated.[278] Numerous studies have suggested that the system is generally unreliable and is not designed to adequately differentiate gunshots from similar sounds such as fireworks or a car backfiring.[279] A ShotSpotter performance audit conducted by the comptroller of New York City over an 8-month period determined that the "gunshot detection technology rarely works and regularly dispatches police to locations where no shooting occurred" with 87% of police deployments finding "no evidence of a shooting."[280] A 2021 audit by Chicago's Office of Inspector General repots similar results: of more than 50,000 alerts there, only 9.1% resulted in evidence of a gun-related offense.[281]

Another consideration is how statistics are counted and categorized. For instance, the Toronto Police Service does not classify the "sound of gunshots" as "a shooting." Other agencies define "a shooting" only where a person has been shot, or other physical damage is noted. Nevertheless, overall, a 2021 study that analyzed almost 20 years of ShotSpotter's use in multiple cities concluded that the system had no significant impact on homicides, murder arrests, or weapon arrests.[282]

Critics have also flagged that ShotSpotter can violate people's basic civil and privacy rights. Many politicians have speculated about the impact of ShotSpotter's network of over 25,000 hidden microphones[283] on privacy rights. ShotSpotter reports tend to give police justification to harass and investigate people who happen to be in the vicinity of a ShotSpotter alert. For example, the State's Attorney's Office in Chicago found that nearly a third of arrests made following a ShotSpotter alert "had nothing to do with a gun."[284]

Further, a leaked document revealing the previously undisclosed locations of 25,580 ShotSpotter microphones across the United States confirms the microphones are disproportionately located in predominantly poor, Black, and Latino neighbourhoods.[285] As a result, ShotSpotter alerts identify and dispatch police to these neighbourhoods more frequently, and the harmful effects of both the increased police presence and the system's general unreliability are disproportionately borne by those residents. In response, ShotSpotter representatives have said that the system is only a tool, and "[I]t's up to the police to decide how they use it."[286]

As far as is known, there are no ShotSpotter systems deployed in Canada. At times, however, the technology has been given serious consideration. In 2019, Toronto City Counsel responded to a wave of gun violence incidents by approving an allocation of $44M for new police technology that could have included ShotSpotter.[287] The plan was scrapped when Toronto Police Services assessed the technology and concluded at the time that it brought "the potential to violate Section 8 of the Charter, which deals with unreasonable search and seizure, as well as the force's research and [the state of] the technology that currently exists."[288]

2.6.3 Drone Surveillance and AI

Drone-mounted cameras could use AI-powered object recognition to automatically identify carried objects associated with criminal activity and report the persons carrying them to law enforcement.[289] Drones are already used by over 1,400 US police departments.[290] Incorporating AI could exacerbate many of the issues with drone surveillance commentators have already identified in its current applications.

For instance, a Wired.com analysis of nearly 10,000 drone flights conducted over two years by the Chula Vista Police Department reveals several concerns.[291] Chula Vista is a border town suburb of San Diego, California and "the first in the nation to start a Drone as First Responder (DFR) program." [292] The drone flight paths "trace a map of the city's inequality, with poorer residents experiencing far more exposure to the drones' cameras and rotors than their wealthier counterparts." [293] Once in the sky, the drones make use of "cameras and zoom lenses powerful enough to capture faces clearly and constantly recording while in flight [and] have amassed hundreds of hours of video footage of the city's residents."[294] Consequently, "residents who encounter the technology day-to-day report feeling constantly watched" and "are afraid to spend time in their backyards." [295]

The Wired.com analysis found that, on average, "each drone flight passes above 13 census blocks and potentially exposes approximately 4,700 of the residents below to a drone's camera." [296] If drones are used for anticipatory surveillance[297] based on the findings of predictive policing systems, the latter could further compound the feedback loop in which already marginalized communities are subjected to disproportionate surveillance due to historical and present-day over-policing.[298] There is also the obvious concern of the potential "chilling effect" caused by residents' perception that they are constantly being watched by drones and other police surveillance.[299] Police in Chula Vista have argued that drone surveillance may in fact reduce civil liberties violations, for example by allowing drone operators to recognize when a situation is less threatening than reported before officers arrive on the scene.[300]

The New York Police Department has recently announced that drones will be deployed as first responders to incidents identified by the department's AI-powered ShotSpotter system.[301] Beverly Hills police already use drones for routine patrols, and several large cities authorize the use of police drone surveillance for parades or protests.[302]

Canadian criminal jurisprudence includes many cases establishing the conditions for lawful use of video surveillance in public and private spaces. Nevertheless, a set of key question arise as to:

- the robustness and responsiveness of procedures for obtaining judicial authorization;
- accounting for the new and automated characteristics AI0-enabled systems bring to the rights analysis; and
- ensuring there are adequate disclosure, transparency, reporting and auditing systems in place to establish public trust in the regular use of automated surveillance systems.

While case-by-case jurisprudence may, over the course of many years, eventually develop a comprehensive series of precedents to govern the use of AI-enabled systems, the potential for mass deployment of such systems suggests a more proactive approach to developing systemic procedural and regulatory requirements may have merit.

3. Key Concerns, Issues, and Questions

3.1 Limited Regulation and Governance Policies of Law Enforcement Use of AI

LCO AI in Criminal Justice Project Paper 1: Introduction and Summary summarizes existing legislation, policies, and frameworks that may regulate the use of AI. However, there are several significant gaps specific to law enforcement described below in greater detail.

3.1.1 Proposed Canadian and Ontario AI Legislation has Limited or Unclear Application to Law Enforcement

In June 2022, the Government of Canada tabled the *Artificial Intelligence and Data Act* (AIDA), as part of a Bill designed to modernize Canada's legislative framework for the digital age. The legislation is currently stalled at second record in a prorogued Parliament. It nevertheless highlights the direction future governments might take and some of the key regulatory considerations when addressing the use of AI by law enforcement.

AIDA as drafted reflects an effort to:

> (1) "regulate international and interprovincial trade and commerce in artificial intelligence systems by establishing common requirements, applicable across Canada, for the design, development and use of systems;" and
>
> (2) "to prohibit certain conduct in relation to artificial intelligence systems that may result in serious harm to individual or harm to their interests."[303]

Artificial intelligence systems are defined in the proposed legislation as, "a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions."[304]

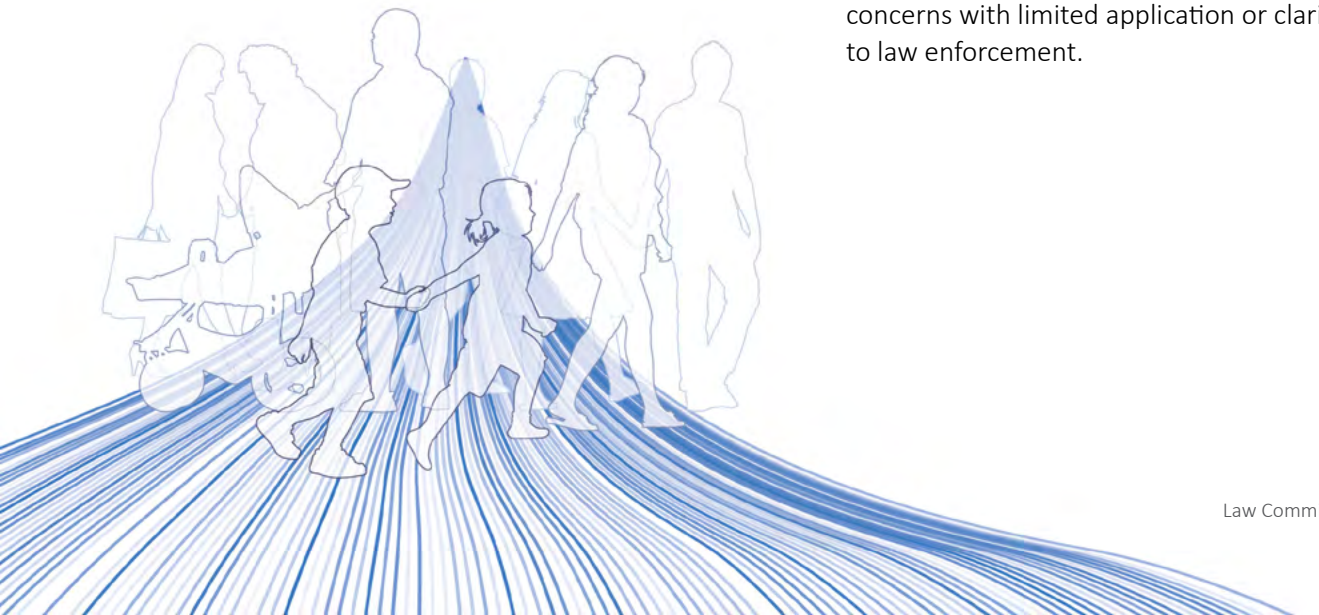
AIDA does not directly regulate the use of AI in the criminal justice system. Rather, it applies to private sector organizations responsible for "designing, developing, using or making available for use an artificial intelligence system," and not government institutions.[305]

AIDA does not apply to a "product, service or activity under the direction or control of" the Minister of National Defence, the Director of the Canadian Security Intelligence Service, the Chief of the Communications Security Establishment, and any others to be defined in regulation.[306]

The proposed legislation contemplates the development of a set of regulatory, oversight and enforcement mechanisms on private sector entities that develop certain AI-enabled products. AIDA applies to the AI system itself, in addition to regulating the "processing or making available for use any data relating to human activities for the purpose of designing, developing or using an AI system", including the ongoing management of the operation of an AI system.[307]

If enacted as proposed, the legislation seeks to set baseline standards to protect individuals from potential "serious harm"[308] associated with AI and "biased output."[309] "Harm" in this context is defined as including physical or psychological harm to an individual, damage to an individual's property, or economic loss to an individual.[310] "Biased" output is output "that adversely differentiates, directly or indirectly and without justification, in relation to an individual on one or more of the prohibited grounds of discrimination" in s. 3 of the *Canadian Human Rights Act*.[311]

Linkage to human right law is important. However, how human rights codes (provincial and federal) apply to the design and assessment of AI systems is an open question and actively under development.



Among these efforts, the LCO recently published its *Human Rights AI Impact Assessment* paper. The paper is a joint project with the Ontario Human Rights Commission with the goal to:

> create an AI impact assessment tool to provide organizations a method to assess AI systems for compliance with human rights obligations. The purpose of this human rights AI impact assessment ("HRIA" or "the tool") is to assist developers and administrators of AI systems to identify, assess, minimize or avoid discrimination and uphold human rights obligations throughout the lifecycle of an AI system.[312]
>
> [...]
>
> The HRIA is intended to:
>
> - Strengthen knowledge and understanding of human rights impacts;
> - Provide practical guidance on specific human rights impacts, particularly in relation to non-discrimination and equality of treatment; and
> - Identify practical mitigation strategies and remedies to address bias and discrimination from AI systems.[313]

The HRIA identifies the difficulty in applying Canadian and Ontario human rights law to AI systems. Nonetheless, it illustrates the depth and specificity required before AI tools can be assessed for compliance.

The Government of Ontario also recognizes the need to act on AI regulation, but again, there are significant concerns with limited application or clarity in regards to law enforcement.

In May 2024, Ontario introduced Bill 194, *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*.[314] Schedule 1 under Bill 194 would enact the *Enhancing Digital Security and Trust Act, 2024*[315] and establish legislation and regulations recognizing "that artificial intelligence systems in the public sector should be used in a responsible, transparent, accountable and secure manner that benefits the people of Ontario."[316] After very short consideration and limited debate in the Legislature, Bill 194 received Royal Assent on November 25, 2024 with no significant changes.

The purpose of Bill 194 is to "…[s]et a definition of artificial intelligence (AI) to create consistency across the public sector and establish protections to ensure responsible use of AI systems."[317]

With such a broad mandate, Bill 194 has the potential to regulate public sector AI systems effectively. Indeed at s. 5(1) Bill 194 states that its provisions respecting AI systems "applies to such public sector entitles as may be prescribed if they use or intend to use an artificial intelligence system in prescribed circumstances."

This section includes two important Bill 194 limitations.

First, s. 1(1) identifies which "public sector entities" will be subject to Bill 194. "Public sector entity" is defined as

> (a) an institution within the meaning of **subsection 2 (1) of the Freedom of Information and Protection of Privacy Act**,
>
> (b) an institution within the meaning of **subsection 2 (1) of the Municipal Freedom of Information and Protection of Privacy Act**,
>
> (c) a children's aid society,
>
> (d) a school board; ("entité du secteur public").

[Emphasis added.]

Second, s. 5(1) allows the province to prescribe AI "uses" or "circumstances" that are subject to Bill 194. Neither "use" nor "circumstances" is defined in the Act.

Notably, neither s. 2(1) of *Freedom of Information and Protection of Privacy Act* nor *s.* 2(1) of the *Municipal Freedom of Information and Protection of Privacy Act* include police services, courts, or tribunals. As a result, these institutions are not subject to Bill 194 governance or requirements.

Outside of these provisions, Bill 194 leaves almost all details up to regulations which have not been introduced nor given any early preview by the current government of Ontario. Left on the cutting room floor are fundamental elements like which public sectors entities will be covered; how they will be covered; what the "risk assessment" scheme may entail (if one is proposed); and how the legislation will be overseen and enforced.

Among many other groups, the Law Commission of Ontario (LCO) has written at length about Bill 194. They conclude that Bill 194, as drafted, fails to establish a trustworthy AI framework for public sector AI systems in Ontario. "Most critically," they write, "the Bill is brief and lacks key provisions needed to ensure public sector AI use is beneficial, lawful, and accountable."[318]

More specifically, the Bill does not address several widely acknowledged regulatory priorities for AI, including AI systems used in the criminal justice system; judicial and administrative tribunal decision making; risk assessments; and other high-risk contexts.[319]

Furthermore, the LCO writes that "AI systems are increasingly considered for adoption – and in some cases have already been deployed – by the full spectrum of criminal justice institutions and participants."[320] This may include:

> "courts, law enforcement, prosecutors, defense counsel, accused, victims, and corrections. Importantly, it also includes justice-adjacent services and institutions that frequently intersect with criminal justice. This may include health care, housing, immigration, and social supports, as well as an array of institutions responsible for systemic oversight of the criminal justice system."[321]

The LCO's submission further clarifies that:

> "… the Bill is brief and lacks key provisions needed to ensure public sector AI use is beneficial, lawful, and accountable. More specifically, the Bill does not address several widely acknowledged Trustworthy AI priorities, including:
>
> - Human rights and procedural fairness.AI systems used in the criminal justice system.
> - AI systems used in courts and tribunals.
> - Public AI registries.
> - Risk categories and mitigation strategies.
> - Impact assessments.
> - Explainability requirements.
> - Governance."

Bill 194 does not include provisions addressing human rights, civil liberties, non-discrimination, equality, or fairness. Nor does Bill 194 include provisions requiring explanations or guaranteeing a process to challenge decisions.[322]

3.1.2 Voluntary Law Enforcement Governance Policy may be Less Effective than Other Approaches

Effective governance frameworks ideally mitigate risks before a technology is used. However, recent examples suggest that law enforcement agencies do not uniformly scrutinize technology before its use. For example, the U.S. Government Accountability Office found that over 90% of enforcement agencies using non-federal FRT systems failed to track which systems were being used. Without tracking, the agencies could not assess the potential privacy implications and accuracy/bias risks, nor could they take steps to address these issues before deployment.

This raises the question of how AI systems are being governed by voluntary policies. Two major law enforcement agencies represent the leading examples of internal assessment and review procedures for AI: the Toronto Police Services Board "Use of AI Technology Policy"[323] and the RCMP's National Technology Onboarding Program (NTOP).[324]

TPS "Use of AI Policy"

The TPS Board introduced the "Use of AI Policy" in February 2022. At the time of writing, the Policy is the leading example of AI use by municipal law enforcement in Canada, and among the few that have been promulgated or publicly discussed.[325]

The TPS Policy acknowledges that advances in technology can pose new concerns for privacy, *Charter* rights, and the dignity and equality of those targeted or monitored by technology. The Policy adopted a broad definition of AI technology, which included "...any goods or services whose procurement, deployment or use require that a privacy impact assessment be conducted in advance of its deployment or use"[326], and sets out the process by which Service Members can use new AI technologies, depending on their perceived "risk category."[327]

The Policy requires that all use of technology, including AI technology, must adhere to the following guiding principles:

1. Legality: All technology used, and all use of technology, must comply with applicable law, including the *Police Services Act* (and its regulations, as well as successor legislation), Ontario's *Human Rights Code*, and the *Charter of Rights and Freedoms*, and be compatible with applicable due process and accountability obligations.

2. Fairness: Use of AI technology must not result in the increase or perpetuation of bias in policing and should diminish such biases that exist.

3. Reliability: AI technology must result in consistent outputs or recommendations and behave in a repeatable manner.

4. Justifiability: The use of AI technology must be shown to further the purpose of law enforcement in a manner that outweighs identified risks.

5. Personal Accountability: Service Members are accountable, through existing professional standards processes, for all the decisions they make, including those made with the assistance of AI technology or other algorithmic technologies.

6. Organizational Accountability: All use of AI technology must be auditable and transparent, and be governed by a clear governance framework.

7. Transparency: Where the Service uses AI technology that may have an impact on decisions that affect members of the public, the use of that technology must be made public to the greatest degree possible. Where full transparency may unduly endanger the efficacy of investigative techniques or operations, the Service will endeavour to make publicly available as much information about the AI technology as possible, to assure the public of the reliability of the AI technology and the justifiability of its use. Where a decision assisted by AI technology may lead to the laying of criminal or other charges against an individual, the possible influence of the AI technology must be included in the disclosure provided to the Crown.

8. Privacy: Use of AI technology must, to the greatest degree practicable, preserve the privacy of the individuals whose information it collects in line with 'privacy by design' principles.

9. Meaningful Engagement: The adoption of specific AI technologies must be preceded by meaningful public engagement commensurate with the risks posed by the technology contemplated.

Self-regulatory efforts are laudatory but also limited. This is particularly evident in the context of law enforcement.

For instance, the Toronto Police Services recently attracted criticism of the Ontario Human Rights Commission and the Information and Privacy Commissioner of Ontario for categorizing their use of AI technologies – including automated license plate readers and fingerprint identification – as "low risk technologies" with fewer assessment and oversight requirements. This is despite candid acknowledgement by police that such technologies "could be used to assist in the identification of individuals for the purpose of their arrest, detention or questioning."[328]

This example may further evidence how AI complicates traditional rights analysis that all institutions will need to re-examine with fresh eyes. For instance, under existing law, drivers arguably have no expectation of privacy in the information on their license plates, so police might assume this means automated license plate reading is a "low risk technology." At the same time, automated license plate readers don't necessarily just identify license plates. As discussed above in section 2.6.2, ALRP systems may additionally correlate other data to a license plate, such as recording the location and time of day observed, where and how long a vehicle was at a particular destination, and patterns of travel and frequency of destinations visited, as well as building up such profiles over time – making such data available to use in other investigations or correlated

to yet other data sources (for instance, recording IP address on public WiFi networks). Such practices are obviously much greater risk to rights and are not adequately accounted for in the presumption that license plate information itself attracts no expectation of privacy.

Another example of how TPS apply their policy is highlighted by adoption of an AI-enabled systems called "NeoFace Reveal by NEC." The application uses a static algorithm to provide images from the database of lawfully obtained criminal record images (arrest photos) that may match a criminal suspect image captured in relation to an alleged criminal occurrence. Any potential image matches are reviewed by a "Facial Recognition Analyst" and subsequently provided to the investigator for additional review.

The service listed a series of factors described as "steps towards mitigating risks", which included:

- database used is a highly controlled set of images;
- database is populated with lawfully obtained criminal record images;
- request to use application is supported by governance and various forms and documentation (the meaning of this step is not clarified nor is any additional detail provided);
- Two authorized and trained users;
- application designed to show possible matches and does not suggest any actions. All results are documented;
- investigators must conduct own actions to continue investigation; and
- use of application and following investigative steps are disclosed for purposes of prosecution (although it is not clear from this list whether the TPS is willing to or has disclosed the algorithm used by the program to generate potential matches).

It is unclear if the TPS analyzed whether the steps described as "mitigating risk" are sufficient to address concerns about the "high risk" NeoFace technology. It is equally unclear whether the use of NeoFace technology has been the subject of any disclosure challenges, or whether the technology has led to any arrests and/or convictions. As of the date of writing, there are no reported Ontario decisions considering the use of NeoFace.

The relevant evidence and standard necessary to satisfy each of these principles is unclear. Further, the policy does not set out any penalties or consequences if the TPS does not comply with the enumerated principles. Defence counsel may argue that the TPS's failure to comply with the AI policy renders the use of a specific technology unlawful, improper, or unreasonable, thus resulting in a constitutional violation.

The policy also suggests that a defendant who brings a constitutional challenge in the context of an AI-based investigation is entitled to disclosure of whether and how the TPS ensured that the technology met each of the guiding principles. While the TPSB's AI Policy requires that the procedures related to AI procurement and use are posted publicly, the Crown may still assert investigative privilege over some items of relevant disclosure. One can reasonably anticipate litigation over what constitutes *Stinchcombe* disclosure, whether privilege applies, and if privilege does apply, the appropriate parameters (see discussion below in s. 3.2.3).

Self-regulatory approaches are also problematized by various public interest legal research groups as failing to address systemic ripple-effects, particularly as they construct an outsized role for courts as the bottom-line check-and-balance on AI. In addition to the LCO's AI in Criminal Justice Project, the Citizen Lab published *To Surveil and Protect*, outlining the human rights and constitutional law implications of the use of algorithmic policing technologies by law enforcement authorities.[329]

Read together, these papers suggest that leaving AI to "regulation by courts" has several drawbacks, namely that:

- Existing criminal case law necessarily has significant gaps in relation to a new technology like AI while cases often turn on narrow facts, specific technology, and contextual use cases that limit the reach of precedent.
- Criminal justice litigation is an intensive and expensive process and comes with significant access to justice limitations including equitable access to experts, funding for defence counsel, and availability of court time.
- Criminal justice litigation is certain to lag the use of AI technology by several years, and only ameliorates the lack of proactive governance and regulation.
- The 50+ distinct and overlapping jurisdictions for both law enforcement agencies and criminal courts across Ontario suggest a patchwork approach will contribute to a variegated system with competing precedents and technologies.

RCMP NTOP

In 2021, the Office of the Privacy Commissioner (OPC) released a special report regarding the RCMP's use of the facial recognition technology by Clearview AI.[330] Clearview created a database of billions of images gathered from public Internet sources such as social media, employment, and educational websites, and then licensed its facial recognition software to Canadian law enforcement agencies and private organizations. The OPC concluded that since Clearview's practices regarding collection of personal information were not compliant with privacy legislation, the RCMP's subsequent collection of that information "falls outside its legitimate operating programs and activities, thus representing a contravention of Section 4 of the *Privacy Act*."[331]

The OPC also noted that the RCMP did not have adequate systems in place to track, identify, assess, and control the collection of this personal information, and recommended that the RCMP institute systemic measures and pertinent training to address these issues.[332]

In response the OPC's special report, the RCMP created the National Technologies Onboarding Program (NTOP). RCMP policy requires that any RCMP unit considering the use of a technology-based tool, technique, device software, application or dataset used to support investigations or intelligence gathering must consult the NTOP before testing, purchasing, developing or deploying any operational technology that is primarily intended to collect or use personal for investigation and/or intelligence gathering. Artificial intelligence and privacy intrusive technologies are the highest priorities.[333]

The NTOP's first ever transparency report, *Transparency Blueprint: Snapshot of Operational Technologies*, was released in the summer of 2024.[334] The report aims to outline how the institution is implementing a more proactive approach to establishing technology assessment and transparency to better achieve responsible use of technology including AI.

The report describes how NTOP conducts evaluations and assessments of operational technologies before procurement and may evaluate certain technologies that were in use before the committee was formed. In the evaluation and assessment process includes an in-depth review of the technology including its intended use, effectiveness and compatibility with existing systems and policies, as well as *Charter* and *Privacy Act* compliance. The NTOP is also committed to consult with third party vendors to determine how personal information is collected, used, and disclosed, and how the technology is intended to function.[335]

The NTOP is mandated to promote transparency of the RCMP's use of operational technologies. The NTOP also consults with other Canadian police and law enforcement agencies to ensure that the RCMP's use of operational technologies is consistent.[336]

Approaches to Regulating Police Use of AI in Other Jurisdictions

In the meantime, other jurisdictions have enacted or proposed strong regulatory schemes governing AI in criminal justice and its use by law enforcement. Leading jurisdictions include the European Union's *Artificial Intelligence Act* (EU AIA),[337] and several instruments in the United States, including the *AI in Government Act of 2020*, the *Advancing American AI Act 2022*, and White House Executive Orders directing the "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" (2023) and "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence" (2024).[338]

These instruments provide lessons for Ontario on how AI in criminal justice could be effectively governed through a coordinated and multi-layered approach.

For example, the EU AIA presumptively prohibits uses of the highest-risk AI technologies including mass biometric identification, social scoring, and predictive policing (with some exceptions for emergencies including investigations into missing persons, child apprehension, and sex trafficking). At the same time, high-risk uses of AI – including in the law enforcement context – are subject to clear procedural requirements for judicial authorization in combination with reporting requirements that foster transparency and public trust. The EU AIA also establishes an AI Office with a mandate to issue interpretive and policy guidelines, as well as a role to assess AI technologies and certify their performance and reliability – and streamlining their availability.

See section 2.4.5, "Restrictions and Prohibitions on the Use of FRT in Canada and Elsewhere" for more detailed outline of the EU AIA in relation to law enforcement technology.

The US Executive Order on "Safe, Secure and Trustworthy Development and Use of AI" is also illustrative of a comprehensive approach to law enforcement. Although promptly rescinded by the Trump administration in January 2025, this Executive Order is illustrative of baseline approaches to governing law enforcement use of AI.

The Executive Order makes it clear that AI systems must protect and strengthen equity and civil rights in several crucial areas where rights are at greatest risk or people are most vulnerable "to address unlawful discrimination and other harms that may be exacerbated by AI."[339] A variety of directives accordingly aim to govern AI use in sectors and among groups including:

- the criminal justice system (s. 7.1);
- protecting civil rights related to government benefits and programs (s. 7.2);
- strengthening AI and civil rights in the broader economy, including preventing unlawful discrimination from AI used for hiring (s. 7.3); and
- protecting consumers, patients, passengers, and students (s. 8);

Among these areas, the Order notably identifies specific high-risk practices as well as schemes to strengthen equity and civil liberties, including steps to govern the use of AI in:

- Sentencing, parole, supervised release, probation, bail, pretrial release, and pretrial detention;
- risk assessments, including pretrial, earned time, and early release or transfer to home-confinement determinations; and
- police surveillance, crime forecasting and predictive policing, and forensic analysis;
- supporting persons with disabilities by ensuring they may benefit from AI's promise while being protected from its risks, including unequal treatment from the use of biometric data like gaze direction, eye tracking, gait analysis, and hand motions.[340]

The 2024 Executive Order builds on the 2023 Order by setting out more detailed binding governance regulatory obligations on US government agencies. It aims to fulfill its purpose to "direct agencies to advance AI governance and innovation while managing risks from the use of AI in the Federal Government, particularly those affecting the rights and safety of the public."[341]

Most crucially, Appendix 1 to Order 2024 includes a long list of presumptively safety-impacting and rights-impacting AI systems.

Safety-impacting systems are those with purposes that include autonomously or semi-autonomously moving vehicles of all kinds, as well as systems that decide whether to summon first responders to an emergency, among others.[342]

Rights-impacting AI systems are those with purposes that include:

- Blocking, removing, hiding, or limiting the reach of protected speech;
- In law enforcement contexts, producing risk assessments about individuals; predicting criminal recidivism; predicting criminal offenders; identifying criminal suspects or predicting perpetrators' identities; predicting victims of crime; forecasting crime; detecting gunshots; tracking personal vehicles over time in public spaces, including license plate readers; conducting biometric identification (e.g., iris, facial, fingerprint, or gait matching); making determinations related to sentencing, parole, supervised release, probation, bail, pretrial release, or pretrial detention; among others;
- Deciding or providing risk assessments related to immigration, asylum, or detention status;
- Conducting biometric identification for one-to-many identification in publicly accessible spaces;
- Detecting or measuring emotions, thought, impairment, or deception in humans;
- Replicating a person's likeness or voice without express consent;
- Determining the terms or conditions of employment, including pre-employment screening, reasonable accommodation, pay or promotion, performance management, hiring or termination, or recommending disciplinary action; performing time-on-task tracking; or conducting workplace surveillance or automated personnel management.[343]

Accordingly, Order 2024 specifies actions that must be taken to achieve the following three objectives:

- Strengthen AI governance. "As required by [Order 2023], each agency must designate a Chief AI Officer (CAIO) within 60 days of the date of the issuance of this memorandum. [Order 2024] describes the roles, responsibilities, seniority, position, and reporting structures for agency CAIOs, including expanded reporting through agency AI use case inventories."[344] Initiatives include:
  - Designating Chief AI Officers;
  - Convening agency AI governance bodies, including designated roles and responsibilities for trustworthy AI;
  - Establishing compliance plans, including AI risk assessment and risk management;
  - Prepare AI use-case inventories and make these publicly available at least on an annual basis; and
  - Prepare reports to the Office of Management and Budget with use-case inventories exempt from public disclosure, such as those used by the Department of Defense and intelligence agencies.[345]
- Advance Responsible AI Innovation. "[Order 2024] provides recommendations for how agencies should reduce barriers to the responsible use of AI, including barriers related to IT infrastructure, data, cybersecurity, workforce, and the particular challenges of generative AI."[346] Initiatives include:
  - Publication within one year of the agency's strategy for identifying and removing barriers to the responsible use of AI, including mature AI-enabling infrastructure for the data, computing, development, testing, cybersecurity compliance, deployment, and continuous-monitoring infrastructure necessary to build, test, and maintain AI;
  - adequate infrastructure and capacity to sufficiently share, curate, and govern agency data for use in training, testing, and operating AI;

- sharing and releasing AI code and models, including releasing and maintaining that code as open-source software on a public repository;
- procuring code for sharing and release, where agencies are encouraged to do so in a manner that allows for the sharing and public release of the relevant code, models, and data.[347]

- Manage Risks from the Use of AI. "[Order 2024] addresses the specific risks from relying on AI to inform or carry out agency decisions and actions, particularly when such reliance impacts the rights and safety of the public… [by requiring] agencies to follow minimum practices when using safety-impacting AI and rights-impacting AI; […] enumerates specific categories of AI that are presumed to impact rights and safety; […] [and] establishes a series of recommendations for managing AI risks in the context of Federal procurement."[348] These initiatives include:
  - Certifications and publication of determinations and waivers of safety-impacting and rights-impacting AI systems beginning December 1, 2024;
  - Implementing minimum-threshold risk-management plans and terminating non-compliant AI on the basis of safety-impacting or rights-impacting uses by December 1 2024;
  - AI impact assessments for safety- and rights-impacting systems, including purpose, potential risks, stakeholder views, the quality and appropriateness of training data, and the identification and assessment of AI's impact on equity and fairness, and related mitigation steps;
  - algorithmic discrimination when it is present
  - Performance testing of the AI in real-world use cases;
  - Independent evaluation of AI performance;
  - Regular and ongoing oversight, maintenance, performance evaluation, risk mitigation, and human oversight of AI systems;
  - Providing public notice and plain-language documentation of the uses of AI systems; and
  - Maintaining options to opt-out for AI-enabled decisions.[349]

Overall, the US executive orders share a great deal in common with the EU AIA. Both deploy a scalable risk-based approach to governing different uses of kinds of AI. Both identify risks to human safety and rights as paramount concerns. Both identify similar areas of highest risk, including policing, criminal justice, government administrative decision making, health care, employment and other areas. Both also accept that procedural fairness concerns are an important check and balance on AI, including mandatory transparency and disclosure requirements, rights of appeal and human-in-the-loop, safeguards against fettered discretion and algorithmic influence, requirements for explainability, and assessment and ongoing testing to control for bias and discriminatory outputs.

Most importantly, both accept that the best way to achieve the benefits of AI is to regulate the readily risks, performance limitations, and operational concerns

Together, the EU AIA and US executive orders demonstrate a largely harmonious approach to identifying and ameliorating risks associated with AI use.

3.1.3 Consultation Questions

1. The discussion suggests the need for provincial rules establishing key trustworthy criminal AI rules and criteria. The Issue Papers suggest many potential models, including:
   - Federal legislation or regulations (Criminal Code, federal ADM Directive?).
   - Provincial legislation or regulation (EDSTA, policing legislation, Ontario AI Directive?).
   - Criminal justice institutional policies (Police, courts, Crown Policy Manual?).

   a. Do you agree some kind of provincial framework is necessary? If so, which approach (or approaches) is best and why?

2. The EU AI Act, AIDA, and the Toronto Police Services AI policy all adopt some form of risk-based AI governance, including presumptive prohibited uses and/or presumptive "high risk" AI systems subject to stricter requirements and more oversight.

   a. In principle, do you agree with the prohibited/high risk framework? What criteria should be adopted to identify prohibited or high-risk systems? Does Canadian law suggest which, or how, different AI systems or uses ought to be categorized?

   b. If you agree some systems or uses should be prohibited or identified as "high-risk":
      - What AI systems or uses should be in these categories?
      - Should real time FRT or predictive policing be prohibited? If so, are there reasonable exceptions, such as FRT to assist missing persons investigations? What rules should apply?
      - What oversight rules or procedural requirements are appropriate for high-risk systems?

3. Disclosure is a consistent theme in trustworthy criminal AI legislation and frameworks. There are choices about the timing, form and substance of disclosure obligations.

   a. How and to what extent should criminal AI systems be disclosed?

   b. Should there be a mandatory AI register or public report? If so, what should be included:
      - A detailed or summary impact assessment?
      - Comprehensive or a summary description of training data?
      - Output data to facilitate independent auditing, oversight and performance monitoring?
      - How to promote disclosure while protecting other legitimate objectives, such as sensitive investigating techniques?

3.2 Constitutional Considerations

The use of AI engages multiple *Charter* considerations, only a few of which can be addressed in this paper. For instance, a person identified by FRT software may argue that their identification constituted a search, as they have a reasonable privacy interest in their anonymity. That person might also challenge the lawfulness of their arrest or detention under s. 9 of the *Charter* where grounds for a detention or arrest were generated solely from or in conjunction with AI technology.

The use of AI by law enforcement will result in a wide range of novel constitutional litigation, increasing the complexity of prosecutions.[350] Defence counsel should consider how to challenge the use of AI technology, including:

- learning about the underlying reliability of the technology;
- considering whether law enforcement required or received judicial authorization for the technology;
- considering whether the nature of the technology and potential privacy implications were explained sufficiently and accurately to the issuing justice; and
- considering whether there were implementation issues, including over-seizure or non-compliance with any execution terms.

If the defence can successfully establish that the use of AI technology was not constitutionally compliant, the Crown may be precluded from relying on the tip generated by technology to justify a detention or arrest, or from relying on AI generated evidence to establish guilt at trial. Law enforcement is wise to identify potential issues – particularly in relation to constitutional compliance – before deploying certain technology.

3.2.1 *Charter* s. 8 Privacy Rights

Section 8 of the *Charter* provides the right "to be secure against unreasonable search or seizure" – also characterized as the right to privacy. Section 8 protects three broad types of privacy: informational privacy, territorial privacy, and privacy of the person or body, and seeks to "protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state."[351] An individual has standing to assert a violation of their right to privacy where they can establish an objectively reasonable subjective expectation of privacy in respect of the subject matter of a search.[352]

The s. 8 jurisprudence recognizes the importance of an individual's anonymity and privacy in relation to the state. For instance, in *R. v. Spencer*, 2014 SCC 43, the Supreme Court of Canada recognized that maintaining anonymity can be integral to ensuring privacy.[353] To this point and addressing the context of anonymous activity on the Internet, Justice Cromwell, for the Court, held that "anonymity may, depending on the totality of the circumstances, be the foundation of a privacy interest that engages constitutional protection against unreasonable search and seizure."[354] Cromwell J. observed that "[a]nonymity permits individuals to act in public places but to preserve freedom from identification and surveillance."[355]

Similarly, in *R. v. Wise*, [1992] 1 S.C.R. 527, La Forest J. (dissenting with respect to remedy), observed that "[i]n a variety of public contexts, we may expect to be casually observed, but may justifiably be outraged by intensive scrutiny. In these public acts we do not expect to be personally identified and subject to extensive surveillance, but seek to merge into the 'situational landscape.'"[356] More recently, in *R. v. Bykovets,* 2024 SCC 3, the Supreme Court iterated the holding in *Jones* that, "...Canadians are not required to become digital recluses in order to maintain some semblance of privacy in their lives."[357]

The importance of protecting privacy and anonymity in relation to the state is an important consideration in assessing the constitutionality of AI investigative tools. For instance, FRT technology that enables intensive state scrutiny of a person's movements and presence in public spaces may violate a person's reasonable expectation of privacy. Individuals attending a public protest or going to a shopping mall, for example, reasonably expect that they will not be the subject of state surveillance, although individuals give up a significant number of constitutional protections by appearing publicly.[358] Nonetheless, individuals can still expect- reasonably- that they can merge "into the situational landscape". Thus, state use of technology that invades on that reasonable expectation of privacy without prior judicial authorization might be successfully challenged as unconstitutional.[359]

Practically, there is very little Canadian caselaw respecting constitutional challenges to the use of FRT. In *R. v. McPherson,* [2023] O.J. No. 546, Justice Code considered an omnibus constitutional challenge in a Project case. During the investigation, the Toronto Police Service ("TPS") had accessed facial recognition technology operated by the Forensic Identification Services. However, because none of the accused before the court were identified as a result of that technology, Justice Code described the issue as "of only academic interest".[360] Other cases highlight how police may obtain and make use of FRT identifications, including from other government systems. For instance:

- *R. v. Voong* (2018 ONCJ 352) in which the identification of persons using FRT in the Ministry of Transportation of Ontario drivers license photo database were later provided to police.
- *R. v. Roudiani* (2018 BCSC 1101) in which the use of FRT by the owner of a private bar produced information later shared with police.
- *R. v. Kawall* (2022 ONCJ 475) in which police used FRT to identify suspects out of the Toronto Police Services arrest photo database.

These examples suggest the many ways in which AI-analyzed information may come to the attention of police conducting and investigation. It raises the question of whether existing procedures and practices – dependent on police seeking judicial authorization – is likely to be sufficient and expedient in an era where AI-enabled analysis is commonplace. Even where judicial authorization is obtained to use invasive technology to further an investigation, investigators must ensure they provide a full, fair and frank description of the technology to the issuing justice. This is prone to errors and delays. For instance, where investigators obtain judicial authorization to use an AI based tool without understanding how the tool functions and/or understanding its limitations, that judicial authorization will be susceptible to a successful constitutional challenge.

3.2.2 *Charter* s. 9: The Risk of Arbitrary Detentions and Arrests Based on AI

The use of AI technology by law enforcement increases the potential for unconstitutional detentions or arrests. Criminal justice system participants must be alive to these potential concerns, particularly as the use of AI technology is more widely deployed or contemplated in policing.

Section 9 of the *Charter* provides to everyone "the right not to be arbitrarily detained or imprisoned." As the majority of the Supreme Court of Canada explained in *R. v. Le*, 2019 SCC 34, the prohibition on arbitrary detention, "is meant to protect individual liberty against unjustified state interference" by limiting "the state's ability to impose intimidating and coercive pressure on citizens without adequate justification."[361]

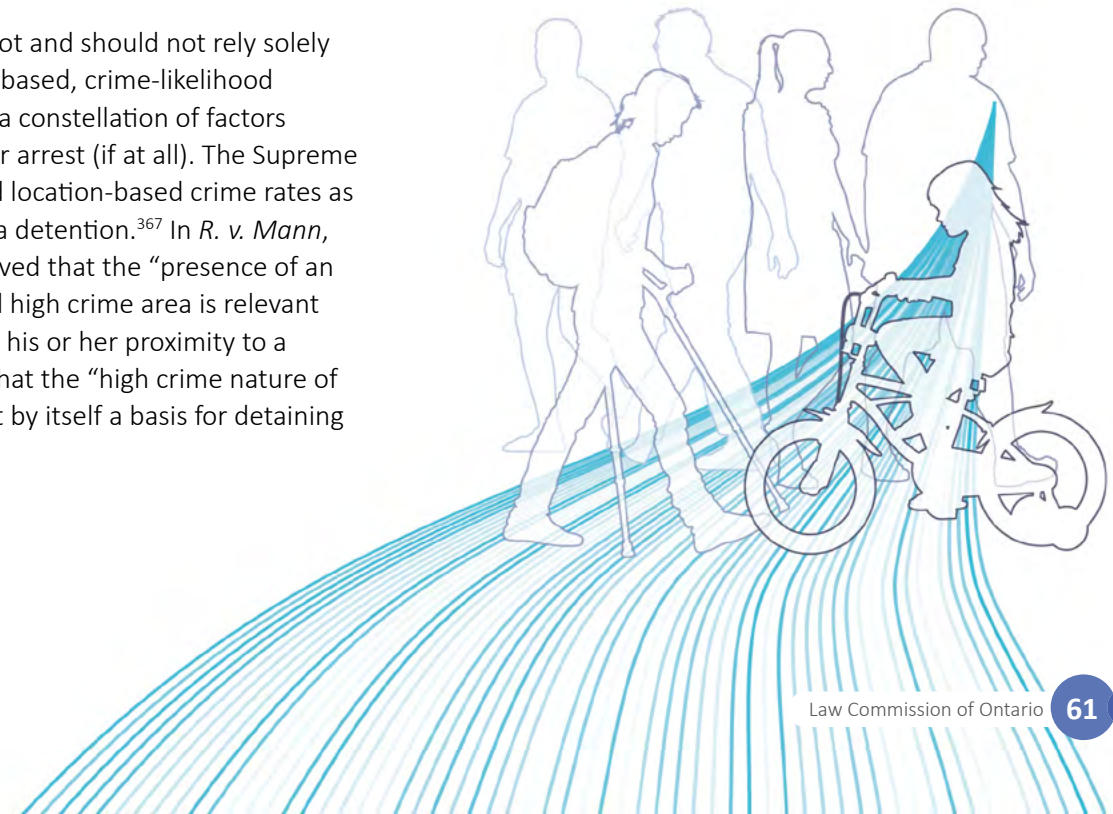
A detention will only be justified, and thus constitutional, where the state has a sufficient evidentiary basis. The constitutional minimum requirement to justify an investigative detention is that an officer has a reasonable suspicion that the person under detention is connected to a particular crime.[362] Reasonable suspicion "must be supported by factual elements which be adduced in evidence and permit an independent judicial assessment."

In R. *v. Ahmed*, 2020 SCC 11, the Court iterated that the "reasonable suspicion" standard compelled law enforcement "to disclose objective evidence that is amenable to exacting review, precluding them from relying on peremptory assertions of suspicion."[363] For a lawful arrest, the standard is reasonable and probable grounds. In determining whether these standards have been met, a court must assess whether there is a "constellation of objectively discernible facts" that support the detention or arrest.[364]

AI increases the threat of unlawful state interference with individual liberty. AI may be relied upon in several ways resulting in the detention or arrest of an individual. For example, law enforcement may rely on FRT to identify a suspect captured by photo or video surveillance. Law enforcement may also use AI technologies to provide real-time identification of criminal activity taking place, such as through technologies like ShotSpotter – an AI-driven system designed to report gunfire to police.[365] As well, police may conclude that an individual is more likely to have been involved in a specific offence because of their presence in an area that AI technology has deemed to be a high-risk crime area. Of particular interest, therefore, is how the courts will assess such AI-generated information when determining whether the constellation of objectively discernible facts known to an officer provided sufficient grounds for an investigative detention or arrest.[366]

Law enforcement cannot and should not rely solely on predictive, location-based, crime-likelihood assessments as one of a constellation of factors justifying a detention or arrest (if at all). The Supreme Court has long rejected location-based crime rates as a valid justification for a detention.[367] In *R. v. Mann*, Justice Iacobucci observed that the "presence of an individual in a so-called high crime area is relevant only so far as it reflects his or her proximity to a particular crime" and that the "high crime nature of a neighbourhood is not by itself a basis for detaining individuals."[368]

With respect to AI identifications from video and photo surveillance, the threat of arbitrary detention arises because of the recognized concerns surrounding the inability of FRT to reliably identify individuals, especially where the individual is: (1) not Caucasian, including those of African-Canadian, Asian or Indigenous descent; (2) female; or (3) elderly.[369] It may well be that FRT identifications are too unreliable, at least in certain contexts, to provide a sufficient basis to law enforcement for a detention. Future cases involving FRT identifications of non-Caucasian, female or elderly individuals will presumably draw constitutional scrutiny. The lawfulness of any AI generated arrest likely turns on the state's ability to demonstrate the reliability of the technology in question, including a robust role for a "human in the loop" to recommend final decisions and which accounts for "algorithmic deference" (the tendency or administrative pressures to uncritically accept what the AI system recommends). The state may struggle to demonstrate reliability, both because of the current limitations of the technology and because of the inherent difficulties in explaining algorithmic decision-making.[370]



3.2.3 *Stinchcombe* or Other Production Problems

Law enforcement assumes significant risk to the viability of an ensuing prosecution or piece of litigation where it relies on AI and at the same time refuses to disclose how the technology operates. For instance, in *Barre v. Canada (Citizenship and Immigration),* 2022 FC 1078, the Applicants successfully challenged the Minister's reliance on photo comparisons they alleged relied on Clearview AI. The Minister refused to disclose whether they had used the software to generate the photo comparisons, arguing that the *Privacy Act* allowed them to withhold evidence relating to "investigative methods".[371] On review, the Court set aside the Refugee Protection Division ("RPD") order vacating both of their refugee statuses, finding that:

> …the RPD reached a conclusion about the reliability of the photo comparisons based on the Minister's say-so with no further details about the "how." It then took the Minister's word that they must protect the details of their investigation under the *Privacy Act* without having to demonstrate whether the requirements for non-disclosure, as set out in the *Act*, were met. The RPD's conclusion, which was void of transparency, intelligibility, and justification, must be set aside.[372]

More recently, the Federal Court found a breach of procedural fairness where a request for disclosure regarding the potential use of FRT was denied.[373] The disclosure request occurred in the context of a decision of the Refugee Protection Division ("RPD") to vacate the applicant's status as a Convention refugee. The Minister of Public Safety and Emergency Preparedness had refused to divulge to the applicant the methodology used to obtain and compare photographs to identify the applicant, and merely provided to the applicant an assurance that FRT was not used.

The Federal Court held:

> The RPD breached procedural fairness when it denied [the Applicant's] request for further information about the source and methodology used by the Minister in obtaining and comparing the photographs, thereby blocking the Applicant's attempts to test the reliability of the evidence being used against him. The RPD also breached procedural fairness by accepting without further examination statements by counsel for the Minister that no facial recognition technology was used and the photographs were discovered and compared manually.[374]

The Federal Court concluded that such disclosure was necessary because it was relevant the reliability of the evidence to be used against the applicant.[375]

Disclosure and transparency are important underpinnings of procedural fairness, raising the question whether law enforcement must be prepared to share how underlying AI software is used and how it functions.

3.2.4 Experts, Explainability, Bias and Admissibility of Evidence

Judges and juries will need to be educated on the functioning of AI technologies, whether in the context of *Charter* challenges, admissibility assessments of evidence flowing from AI technologies, or assessments as to the weight to be afforded to AI-generated evidence. The state should be prepared to provide this education, including fairly explaining potential reliability and bias concerns. It is an important check and balance. Increasingly, police in Ontario prepare "technical briefs" to explain technology-based tools to Judges who consider them in the context of a judicial application. Those briefs are intended ensure the Judge understand how the technology works before deciding whether to grant the warrant or order. In some circumstances, a similar approach may be appropriate for AI-based tools. Judges and others should be well equipped to assess these reports critically.

It may be challenging to find experts who can explain the complexities of specific AI systems to judges and juries. As some commentators have pointed out, AI software can be a "black box" due to: (1) its limited ability to separate causation from correlation; and (2) the fact that it is often "proprietary and either unknowable or inscrutable to the public".[376] These limitations may rightly lead to inadmissibility determinations if the party seeking to adduce the evidence cannot establish its threshold reliability, or even if admitted, lead to courts putting less weight on AI-related evidence.

These issues are discussed in greater detail in the LCO AI in Criminal Justice Project Paper 3, ***AI and the Assessment of Risk in Bail, Sentencing, and Recidivism***, and in Paper 4, ***AI at Trial and on Appeal***.

3.2.5 Consultation Questions

4. The need for impact assessments is a consistent theme in criminal AI legislation and frameworks. There are choices about the timing, form and substance of impact assessments.
   a. Should the province require a mandatory impact assessment for criminal AI systems in Ontario? Do you agree an impact assessment should address privacy, human rights and procedural fairness and provide assurances about how an AI system will comply with other legal obligations?
   b. What other information or risks should be included?
   c. How best to ensure impact assessments are being used and reported consistently?

5. Many criminal AI systems have been criticized by communities who believe they were not consulted or informed about systems that affect them. Many trustworthy criminal AI initiatives, including the Toronto Police Service AI Policy, include public engagement requirements.
   a. How should the public be involved in criminal AI policymaking, evaluation or oversight?

3.3 Warrantless Requests by Law Enforcement for Private Information

This section discusses warrantless requests for private information made by law enforcement to third parties. It begins by summarizing the applicable law, including section 8 of the *Charter* and privacy legislation such as *PIPEDA*. Then, it discusses some American examples of warrantless access, the OPC's recent investigations in the RCMP's use of Clearview AI and other data services, and implications for possible future police practices.

Overall, this research suggests a significant gap between Canadian privacy law—which tends to place heavy restrictions in the way of police accessing even remotely sensitive personal information without a warrant—and police practices that may disregard or circumvent the law. Explicit regulation may be needed to close this gap, which is unlikely to be effectively addressed by the courts.

A notable additional insight is that Canadian law in this area is substantially different from American law. In the United States, the "third party doctrine" creates much less stringent requirements for law enforcement's ability to obtain personal information from third parties without a warrant. In Canadian jurisprudence, the third party doctrine has been consistently rejected.

3.3.1 AI and the Law of Warrantless Disclosure

a) Any warrantless police "search" is presumed to breach section 8 of the *Charter*

In Canada, section 8 of the *Charter of Rights and Freedoms*[377] prohibits police from the unreasonable search and seizure of an individual's private information. When police obtain information in relation to which there is a reasonable expectation of privacy, they have performed a "search" attracting Charter protection.[378] Judicial preauthorization is a presumptive requirement to search and seizure, but there are many exceptions that nevertheless comply with section 8. A leading case deliberated soon after the *Charter*'s coming into effect, *Hunter v. Southam*[379] ruled that s 8's protection against "unreasonable search and seizure" may be understood "positively as an entitlement to a 'reasonable' expectation of privacy."[380]

Police must establish that a search is reasonable before conducting it, which requires a judicial exercise balancing "the public's interest in being left alone" against the goals of law enforcement.[381] Any search conducted without prior authorization is presumed to be unreasonable.[382] Thus, a warrantless search will only be found lawful in "exceptional circumstances," such as when there is a need to protect the safety of those at the scene.[383] It is worth noting that there are many other exceptions, including:

- search incident to detention;
- search incident to arrest;
- dog sniff searches;
- roadside investigative search powers related to impaired driving and possession of alcohol and drugs in a vehicle;
- searches in exigent circumstances;
- emergency interceptions; and
- plain view seizures.

b) The *Charter* protects individuals' personal information and anonymity

Individuals may have a reasonable expectation of privacy pertaining to a "biographical core of personal information" including "information which tends to reveal intimate details of the lifestyle and personal choices of the individual."[384] Information that provides grounds for a "strong, immediate and direct inference" about those details is also protected.[385]

More recent cases such as *R. v. Spencer*[386] have explicitly extended section 8 protection to individuals' reasonable expectation of anonymity, which "permits individuals to act in public places but to preserve freedom from identification and surveillance."[387] Key to anonymity is the "link" between a person's identity and their public activity:[388] while the latter may be publicly known, attempts by the state to connect it to a particular individual will engage the *Charter*-protected privacy interest. Although *Spencer* and *R. v. Bykovets*[389] focused on anonymity in the context of internet use, their reasoning is closely related to earlier decisions prohibiting warrantless police video surveillance[390] and vehicle monitoring.[391]

c) When is there a reasonable expectation of privacy?

Whether an individual has a reasonable expectation of privacy in any given information—and thus, whether an attempt by police to seize that information constitutes a "search"—must be decided on a case-by-case basis with regard to "the totality of the circumstances."[392] *R. v. Tessling* noted that, "[g]iven the bewildering array of different techniques available to the police (either existing or under development), the alternative approach of a judicial 'catalogue' of what is or is not permitted by s. 8 is scarcely feasible."[393] As such, *Tessling* established four factors that must be considered uniquely in every circumstance:

1. the subject matter of the search
2. the claimant's interest in the subject matter
3. the claimant's subjective expectation of privacy
4. whether the claimant's expectation of privacy was objectively reasonable[394]

Analysis based on the *Tessling* test are fact-specific, making it difficult to draw general conclusions about an individual's privacy interests in relation to law enforcement. For example, there is no binding law establishing whether police seizure of surveillance footage of the common areas of a residential building constitutes a search.[395] In *R. v. Louie*, it was found that the accused did have a reasonable interest in the footage.[396] The judge relied in part on the SCC's statement in *R. v. Wong* that "there is an important difference between the risk that our activities may be observed by other persons, and the risk that agents of the state, in the absence of prior authorization, will permanently record those activities on videotape."[397] In *Louie*, video footage had recorded the accused with an object that appeared to be drugs. Meanwhile, the Supreme Court of British Columbia found that the accused in *R. v. Sanchez* did not have a reasonable expectation of privacy in video footage of his building's parking garage, since "[t]here would be little or no difference between the CCTV footage showing vehicles entering and exiting the parking garage and what a member of the public would be able to see from outside the complex."[398]

d) Third parties cannot consent to waive an individual's privacy rights

Canadian privacy law differs substantially from American privacy law in that Canadian courts have rejected the "doctrine of third party consent" or "third party doctrine."[399] Instead, Canadian courts require first party consent for any waiver of privacy rights.[400] This means that in order for the state to breach an individual's reasonable expectation of privacy, the individual themselves must give voluntary and informed consent. A third party with access to sensitive personal information cannot consent to disclose it to law enforcement on the affected person's behalf.

R. v. Reeves[401] is an instructive example of the requirement for first party consent. In *Reeves*, the accused and his co-habiting common-law spouse shared a personal computer. The spouse alleged to the accused's parole officer that the computer contained child pornography, then consented to have a police officer enter their home to seize the computer without the accused's knowledge and without a warrant. The SCC found that the seizure had violated the accused's privacy rights. Even though the spouse had an "equal and overlapping" privacy interest in the computer, she, being a third party, could not waive the accused's privacy rights on his behalf.[402] While this is clear in context of using a computer, it is not yet conclusive how this applies to a conversation. The SCC has not yet decided whether a party to a conversation can turn the conversation over to the police without the police having to get a warrant. However, lower courts have considered the issue. Many courts in Ontario and other provinces where courts have held that one party to a text conversation can turn it over to police, who can lawfully use it despite the lack of consent of the other participant in the conversation.

e) *R. v. Bykovets* affirmed a broad scope of protection

The decision in *Bykovets* extends section 8 protection to a relatively broad range of information, prohibiting law enforcement from requesting that information from third parties without a warrant. The decision requires police to obtain some form of prior judicial authorization to collect internet protocol (IP) addresses linked to internet activity, even when those IP addresses are not directly matched with a user's biographical information.[403] This means that protection may extend to information that appears anonymous on its face.

Key to the court's decision was its recognition that even information that is meaningless on its own (after all, an IP address by itself is only a "string of numbers") may "betray deeply personal information" when correlated with other seemingly innocuous data.[404] Justice Karakatsanis noted that

> [w]ithout the protection of s. 8, nothing prevents the state from pre-emptively collecting IP addresses and comparing that user's IP address against their database. Further, and significantly, the scope of information that an IP address can reveal is enormous if correlated against information held by a third party.[405]

For example, compiling various websites' IP address logs can reveal a device's online financial transactions, social media activity, and Google search history over a certain period of time.[406] This information is often sufficient to identify the individual user.[407]

Law enforcement agencies indicate that a warrant requirement that each individual IP address at issue in an investigation is very onerous. The LCO understands that some provinces have adopted "bulk IP" warrant application policies in an attempt to balance the privacy principles at issue in *Bykovets* while ensuring investigative efficiency. The LCO is very interested in hearing more about this as a potential area for legal, regulatory or policy reform.

f) Legislation grants police limited authority to request personal information from third parties

i. PIPEDA

The *Personal Information Protection and Electronic Documents Act* (*PIPEDA*),[408] which is the key privacy legislation targeted at non-state actors, allows organizations holding individuals' personal information to disclose it without the affected person's consent in certain situations. However, *PIPEDA* has been interpreted to provide little if any authority for police to lawfully request this information without a warrant.

On its face, section 7(3)(c.1) appears to allow organizations to disclose personal information without the affected individual's consent to law enforcement that has "identified its lawful authority" to obtain it.[409] However, *Spencer* ruled that "lawful authority" in the context of the Act depended on whether a *Charter*-protected reasonable expectation of privacy was present.[410] Further, the fact that *PIPEDA*'s purpose is to *protect* individuals' right to privacy weighed against its allowing for disclosure.[411] Thus, *PIPEDA* has no bearing on the standard procedure for authorizing a police search.

Other *PIPEDA* provisions do not directly empower law enforcement. Section 7(3)(d) allows disclosure of personal information without consent to law enforcement if the organization has "reasonable grounds" to believe the information relates to a crime;[412] however, this provision must be used "on the initiative of the organization" holding the information[413] and cannot be invoked in response to a request by police.[414] Outside of this, there does not appear to be any reported cases in which section 7(3)(d) was invoked to justify the transfer of personal information to police on the organization's initiative. Meanwhile, sections 7(3)(d.1) and (d.2) allow disclosure of personal information to other organizations (such as professional regulatory bodies or banks) investigating crime or fraud,[415] but not to law enforcement.[416]

Other legislation may provide authorization in specific contexts. For instance, the federal *Income Tax Act* includes a provision that is used when police want taxpayer information from the Canada Revenue Agency (at section 241(9.5)).

ii. FIPPA

The *Freedom of Information and Protection of Privacy Act*[417] governs the disclosure of personal information by public institutions and contains similar provisions as *PIPEDA*. These include provisions allowing for the disclosure of personal information to law enforcement without a warrant.[418] For example, section 42(1)(g)(ii) allows an institution to disclose personal information to law enforcement if the institution has "a reasonable basis to believe that an offence may have been committed."[419] Like with *PIPEDA* section 7(3)(d), the institution must decide to disclose and should not merely be responding to a police request.

FIPPA section 42(1)(g)(i) allows for the disclosure of personal information to law enforcement without a warrant under somewhat less stringent circumstances than *PIPEDA*. The provision allows disclosure to "aid in an investigation" undertaken by a law enforcement agency "with a view to a law enforcement proceeding."[420] This authorization has been used in at least one case, *R. v. Noftall*, in which the Ontario Superior Court found that the Ministry of Community Safety and Correctional Services had lawfully disclosed the accused's medical records to the Toronto Police Service upon the latter's warrantless request for use in a sentencing proceeding.[421] Nevertheless, it may be more difficult for public institutions under *FIPPA* to *collect* personal information in the first place

compared to private organizations under *PIPEDA*, since consent alone cannot authorize collection under *FIPPA*.[422]

iii. Bill C-27

Some commentators have expressed concern that the Bill C-27, if passed by Parliament, could enhance police powers to request disclosure of personal information.[423] Specifically, the proposed *Consumer Privacy Protection Act* contains language that would allow for the non-consensual disclosure of personal information in response to requests made by law enforcement.[424] However, the provision uses language very similar to that found in *PIPEDA* section 7(3)(c.1), including the "lawful authority" requirement that *Spencer* ruled had no impact on *Charter* protections.[425]

3.3.2 Comparison and Critique of Warrantless Disclosure Practices

a) **United States**

In the United States, police frequently request and obtain access to personal information from third parties without the affected individuals' knowledge or consent. For example, many law enforcement agencies enlist the support of data brokers to aid in investigations,[426] websites have historically provided IP address logs freely when requested,[427] and private and public video surveillance footage may be managed by the same companies and shared between businesses and police.[428]

As judicially authorized orders, "geofence warrants" compel companies like Google, Apple, and Amazon to provide police with unprecedented amounts of surveillance data.[429] Using information gleaned from cell phone location data, responses to these warrants include information about every person who was present in a specific area during a specified period of time.[430]

The existence and treatment of the third-party doctrine in United States privacy law is a major reason why these kinds of investigative techniques are considered lawful under the Fourth Amendment.[431] Since the third-party doctrine is not recognized in Canada,[432] these techniques would be subject to a substantially different legal analysis if used by Canadian law enforcement. Whereas third-party doctrine permits US agencies to obtain certain forms of geofence data without judicial authorization, police in Ontario have long sought geofence information via judicial authorization (for example, cell tower records to identify unknown devices near a crime scene). Guidelines for this are set out in case law.[433]

Of further interest is that this area of US law appears to be unsettled and may be ripe for law reform. In January 2025, the long-awaited ruling in *United States v. Hasbajrami* was released by a Brooklyn district court. The court's decision adjudicates the US 4th Amendment in context of warrantless disclosures made under *Foreign Intelligence Surveillance Act of 1978.* As characterized by the American Civil Liberties Union Deputy Director of National Security, the judgment of the court "recognized the FBI's rampant [warrantless] digital searches of Americans are an immense invasion of privacy and trigger the bedrock protections of the Fourth Amendment. [Consequently,] Section 702 is long overdue for reform by Congress, and this opinion shows why."[434]

Indeed, the judgement specifically clarifies that "balancing the substantial degree of intrusion with the powerful public interest, the Court finds that the queries conducted as to Defendant were unreasonable under the Fourth Amendment even had an exception to the warrant requirement applied."[435] Building on earlier precedent established in 2019, this suggests a judicial trajectory in the United States increasingly skeptical of indiscriminate warrantless disclosures as inconsistent with a general public interest in privacy.

b) OPC investigations into the RCMP's use of Clearview AI and other services

In Canada, warrantless collection of personal information by law enforcement—whether connected to AI-powered systems or not—is less frequently documented and appears to be less common than in the United States. Some of the most widespread examples, such as police requesting IP addresses and internet subscriber information from websites and internet service providers, have been heavily scrutinized by the courts, such as in *Bykovets*.[436]

At the same time, other judicial cases suggest various approaches to using digital search tools, like those used in "open-source intelligence" investigations, may fairly balance the needs of investigators with the publics interest in protecting privacy.

This is further complicated by the positions taken by other agencies, such as the Office of the Privacy Commissioner (OPC). The OPC has conducted high-profile investigations into the RCMP's practice of accessing allegedly protected personal information through their use of Clearview AI and other services and made clear findings in relation to privacy violations, but also as regards the privacy interests relevant to "publicly available information," which may also be treated distinctly as the subject of "search tools" or where it is subject to mass scraping, analyzing, and storing.

An exploration of this topic, which follows below, suggests it might be helpful to consider this area as ripe for legislative, regulatory or policy development.

In June 2021, the OPC issued a special report to Parliament in which they found that the RCMP's use of Clearview AI's FRT contravened section 4 of the *Privacy Act*,[437] which governs government institutions' collection of personal information.[438] Significantly, the OPC's conclusion flowed from their findings in a previous investigation[439] that Clearview had contravened its own governing authority as a private organization under *PIPEDA*. Clearview had failed to seek consent from the individuals whose information it had collected, and were wrong in asserting that the information (sourced largely from social media and public websites) was "publicly available" under *PIPEDA*.[440] They had also used and disclosed the information for "inappropriate purposes," as their stated goals "represent[ed] the mass identification and surveillance of individuals by a private entity in the course of commercial activity."[441]

In regard to the RCMP's accessing Clearview's services, the OPC thus found that "since Clearview's personal information collection practices were not compliant with its legal obligations [under *PIPEDA*], the RCMP's subsequent collection of that information falls outside its legitimate operating programs and activities, thus representing a contravention of Section 4 of the *Privacy Act*."[442]

Technically, the OPC's findings left open the possibility that the RCMP could lawfully request, and access, information connected to FRT if the technology's supplier was compliant with *PIPEDA*. The OPC specifically did not make any findings into the RCMP's compliance with the *Charter*.[443]

The RCMP also disputed the OPC's contention that it had a legal obligation under the *Privacy Act* to ensure its third-party partners' compliance with *PIPEDA*.[444] The RCMP ceased using Clearview AI in 2020 when the company ended its operations in Canada.[445] However, as suggested in the reading of the OPC report, the RCMP's ongoing disagreement with the OPC motivates further allegations that they have not properly investigated the *PIPEDA* compliance of other data collection services they continue to employ.[446]

c) Discussion

Despite the OPC declining to make a finding as to whether the RCMP's use of Clearview AI was *Charter*-compliant,[447] it is difficult to imagine how Canadian law enforcement could make a *Charter*-compliant request for any information connected to FRT or AI-powered surveillance without judicial authorization. If it can be established that a target of investigation had a reasonable expectation of privacy, any police "search" (defined how?) is presumed to be unreasonable, and thus in violation of section 8, without judicial authorization.[448] Meanwhile, the fact-specific nature of the *Tessling* test[449] makes it difficult to predict whether information accessed by law enforcement (including through a third-party agency such as an AI service provider) will attract a reasonable expectation of privacy without detailed knowledge of the circumstances in which it was collected.

This poses significant challenges for police use of AI applications, since the latter typically draw from massive data sets scraped from a huge variety of sometimes difficult-to-trace sources. Alternatively, various "open-source intelligence tools" do not "scrape" or store information, rather, relying on publicly available sources and infrastructure (including potentially the "dark web") to conduct live searchers. Further complicating this, the most recent SCC guidance in *Bykovets* suggests that even seemingly innocuous data as fundamental to the operation of digital communication as is an IP address, could, when linked to vast publicly available and for-sale data sets, nevertheless support detailed inferences about personal information and detailed personal profiles that would attract section 8 protection. [450]

Nevertheless, it is informally known that police may make requests for information without judicial authorization and despite the likelihood that it would breach the affected individual's *Charter* rights for them to obtain it, or that it would be unlawful for the party possessing the information to disclose it.[451] As the Clearview AI scandal suggests, new investigative technologies, particularly tools made freely available online and to the public (like GeoSpy),[452] may directly or indirectly encourage police to overlook or disregard existing privacy law.

For instance, law enforcement officials regularly assume or assert that information provided by unregulated mass surveillance technologies is publicly available and therefore not protected by privacy rights.[453] More recently, York police Constable Kevin Nebrija, commenting on the privacy implications of integrating FRT tools like Clearview AI into police operations, said that "nothing has changed because security cameras are all around… [and] the images police will acquire will be "obtained lawfully," either with the co-operation of security camera owners or by obtaining court orders for the images."[454] His comment reflects a concerning disregard for the nuanced prohibitions supplied by section 8 jurisprudence and legislation such as *PIPEDA*. The absence of a more systematic and specific law, regulation or policy governing disclosure of AI-enabled information from third parties and other sources may invite a wide variation in regional practices with little public transparency or oversight.

Unsurprisingly perhaps, in 2022, the federal, provincial and territorial heads of Canada's privacy commissions "called on lawmakers to establish a legal framework for appropriate use of facial recognition technology, including empowering independent oversight bodies, prohibiting mass surveillance and limiting how long images can be retained in databases."[455]

A few other recent court cases can also be read as supporting a less restrictive balance favoring investigative over privacy interests. For example:

- In the 2023 decision *R. v. Rahi*, the Ontario Superior Court of Justice found that escort advertisements retrieved by the Toronto Police Service's Human Trafficking Enforcement Team using "Traffic Jam" software was admissible as evidence at trial.[456] In the written decision, Nakatsuru J. described Traffic Jam as "an internet search engine searching the internet for past and current sexual services advertisements on various websites" with "The only added feature of Traffic Jam is that the digital universe it scours includes deleted advertisements."[457]

- The 2023 decision *R. v. Hughes* examined Charter section 8 and *Garofoli* applications by the OPP to investigate the trading of child pornography on peer-to-peer ("P2P") networks.[458] The Court recognized, in part, that while it is possible for law enforcement agents to conduct manual surveillance on P2P networks such manual labour is neither efficient nor particularly effective given the scope of the undertaking. Instead, it is expected that law enforcement agencies will utilize sophisticated software tools that have been developed to survey P2P networks in an automated manner, looking for individuals trading in files known to contain child sexual abuse materials.

Overall, the legal regulatory picture this situation paints is concerning. It is unlikely, however, that the apparent gap between privacy law and police conduct can be effectively narrowed by the courts alone. It is telling that the OPC, in their investigations into the RCMP's use of Clearview AI and other data-driven services, chose to focus on the relatively vague provisions of the *Privacy Act* rather than the rich vein of *Charter* jurisprudence. One reason may be the difficulty and inefficiency of resolving law enforcement-related privacy issues through the courts. Recently, the OPC went so far as to admit that the RCMP may be able to circumvent "evidentiary" issues with information gathered from the social media-scraping service Babel X by carefully tailoring how they incorporate this information into the investigative record.[459] Moreover, police surveillance could have significant deleterious effects on many individuals who are never accused of a crime, and thus have no opportunity to assert their rights apart from cost-prohibitive private litigation. Against this background, the OPC has pushed for changes to the RCMP's practices on a regulatory and legislative, rather than a jurisprudential basis.

The situation further emphasizes that privacy law may only be suited to addressing some aspects involved int eh use of AI. AI systems are indeed reliant on the processing of large data sets, both in training their algorithms and in giving them specific problems and evidence to analyze. But AI systems have many other problems outside of privacy related to issues like biased decision making, a lack of transparency, a lack of explainability, and significant shortcomings in fulfilling various others well established principles of procedural fairness.

Technological progress in AI-driven policing has made *Tessling*'s observation of the "bewildering array of different techniques available to the police"[460] truer now than ever. Nevertheless, legislatures' failure to provide the "'catalogue' of what is or is not permitted by s. 8" that the judiciary rejected[461] has empowered law enforcement to assert that an ever-expanding range of warrantless access to personal information is allowable under the *Charter*.[462] Without explicit, authoritative regulation, this situation is unlikely to change.

3.4 Crown Advice to Law Enforcement

The specific subject of this section considers the unique role of the provincial Crown in assessing the impact of AI-enabled investigative tools on potential criminal charges.

A charge may only proceed if there is a reasonable prospect of conviction, and it is in the public interest. Assessing a reasonable prospect of conviction involves a consideration of the admissibility of evidence implicating the accused. This includes an assessment of whether the evidence was obtained in a manner consistent with constitutional, legislative, and common law standards. These have been established over a series of key cases and the findings of several inquiries and studies.[463]

This discussion suggests a crucial opportunity for close police and Crown collaboration in assessing the validity of AI-enabled systems prior to investigations taking place. Applied consistently, this important advice function could significantly lessen the need for courts to routinely wade-in to the assessment of different technologies.

Crucially, this relationship must respect the constitutional convention of independence between police and prosecutorial decision-making. It can also take several forms, such as legal advice about constitutional compliance, minimization techniques, disclosure, technical briefs, or cost-benefit analyses. These long-standing initiatives often involve police / crown consultation in advance of police use of new technology, not just after the fact.

This discussion further suggests how any collaboration and any after-the-fact scrutiny of police and prosecutorial decision-making in relation to AI-enabled technologies must account for the details of the specific technology and the specific use at issue. The capacity for flexible, on-demand assessment of these questions will be critical to assessing AI in the criminal lifecycle.

Understanding the current environment of police / crown interactions and compliance requirements will help guide the conversation on future AI applicability – and recognize that AI technologies are unlikely to be given *carte-blanche* in these interactions.

3.4.1 What is the Mandate and Role of the Crown in Reviewing Charges and Assessing Evidence?

The mandate, role, and conventional relationship between the Crown and law enforcement is based in the Crown's role in assessing charges. The Prosecutor assesses all charges to determine whether there is a reasonable prospect of conviction, and if it is in the public interest. The obligation applies at all stages of the prosecution. For example, if the Prosecutor determines there is no longer a reasonable prospect of conviction at any stage of the proceedings, the prosecution must be discontinued. In assessing whether there is a reasonable prospect of conviction, Prosecutors must consider several factors, including the admissibility of evidence implicating the accused.

Many of these criteria are defined and developed in the *Crown Prosecution Manual*, a "soft law" document that sets important practice standards for Crowns to follow on a wide variety of matters.[464] Federal prosecutors follow a similar guide, the *Public Prosecution Services of Canada Deskbook*.[465]

In cases involving the use of novel AI technology in evidence gathering the Prosecutor will consider whether the collection of that evidence was in accordance with constitutional, legislative and common law standards.

When the Crown may play a role in assessing technology – at either the **Investigative and Pre-Charge Stage** or at the **Post-Charge and Litigation Stage** – the relationship between law enforcement and the crown is governed by both law and a set of conventions based in a mix of legal, Constitutional, and practical ongoing practices. Cooperation between the police and the Crown is essential, but both remain mutually independent. The police may seek the advice of the Crown but are not bound to follow any advice that may be provided.[466]

This relationship is subject to a set of legal and constitutional guardrails on police decision-making, prosecutorial decision-making, and police-prosecutor interactions. These have been established over a series of key cases and the findings of several inquiries and studies.[467] In summary, these cases and reports affirm various principles guiding the relationship between law enforcement and the Crown. Chief among these is that:

- collaboration should respect the constitutional convention of independence between police and prosecutorial decision-making;
- collaboration can take various forms, e.g. legal advice about constitutional compliance, minimization techniques, disclosure, cost-benefit analyses; and
- that any collaboration and any after-the-fact scrutiny of police and prosecutorial decision-making in this arena has to account for the details of the specific technology and the specific use at issue.

3.4.2 How does the Crown Evaluate Technologies at the Investigative and Pre-charge Stage?

Accordingly, the role of the Crown in the investigative and pre-charge stage is multivariate and may include the following:

Identification of specific categories of potential investigative uses of AI technology by law enforcement. This can include:

- intelligence-led policing (e.g. information gathering, information sharing);
- operational planning and direction (e.g. resource management, predictive policing);
- evidence gathering (e.g. electronic surveillance, databases); and
- file management (e.g. e-discovery tools, disclosure redaction, audio/video analysis, audio transcription).

Outlining the applicable legal, constitutional and policy considerations to these categories. This can include:

- privacy legislation and policy guidance;
- privacy impact assessments;
- feedback from public and stakeholder consultations; and
- key provisions in the Charter of Rights including section 7 (abuse of process, full answer and defence), section 8 (reasonable expectations of privacy/reasonable expectation of non-interception of privacy communications), and section 11(d) (full answer and defence).

Identifying other potential litigation risks, which can include:

- public interest privilege;
- investigative privilege related to international cooperation (such as the Five Eyes tools and governance by memorandums of understanding);
- investigative privilege related to private corporations (such as assertions akin to US-style "trade secrets" arguments); and
- the fallout that can come with an unfavorable privilege ruling.

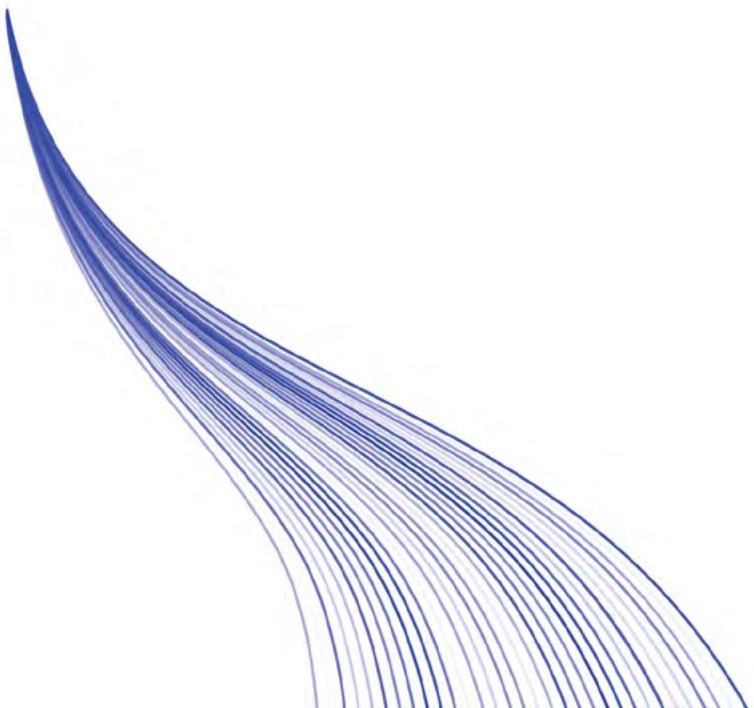
Pre-charge assessment in the police / Crown collaborative model evidently needs to adapt for new investigative tech as it has for other markers of complexity in the criminal justice system. It might be expected that prosecutors will move into a more proactive and inquisitorial role with technical details. For instance, being clear about what is meant by "open source" software, and what specifically was done and how to maintain the transparency of the software and it's use. Similarly, it might be expected that there will be an increased need for documentation in support of after-the-fact review, judicial or otherwise (an issue navigated by analogy in cases including *R. v. Vu* and *R. v. Fearon*).[468]

Finally, none of this analysis can be conducted meaningfully without an understanding of the technical details, since that is what drives scale of impact on any legal and constitutional interests. This might include discussions about:

- specific capabilities of the technology
- purpose for which the technology was deployed
- specific manner of deployment (e.g. judicial authorization, training, minimization techniques) and
- whether the use can be demonstrated by reference to existing technologies (e.g. MDI/CSS, ALPRs).

In these discussions there will be a premium on consistent lexicon and use of plain-language glossary to reduce room for misunderstanding between lay and high-end user. Forms of judicial authorization suggest how this might be done effectively. For instance, judicial authorization applications may be reviewed by a technical officer, with disclosable material included in the body of an affidavit along with a disclosable technical brief that is plan language but with full, fair and frank disclosure about:

- the capabilities and limitations of the tools in question;
- the manner in which they were deployed;
- any issues related to the generated evidence (such as if any of it needs to be sealed).



3.4.3 How does the Crown Evaluate Technologies at the Post-charge and Litigation Stage?

This section discusses how the Crown satisfies disclosure obligations where evidence is generated from the investigative use of AI technology. It then discusses how the Crown can adduce and rely on that evidence at a bail hearing, preliminary inquiry and/or trial.

This is split into two phases below:

- Disclosure and Case Management phase, and
- Pre-trial phase.

Disclosure and Case Management Phase

When litigation is contemplated where the state has used AI in criminal and quasi-criminal cases, the first stage is the disclosure obligation of the Crown. Upon request by defence, the right to full answer and defence under s.7 of the *Canadian Charter of Rights and Freedoms* requires the Crown to disclose all inculpatory and exculpatory evidence in its possession or control that is not "clearly irrelevant" or subject to privilege.[469]

The extent of the material(s) disclosed will depend on how the AI was used in the police investigation, i.e., are the materials requested considered to be first party disclosure or third-party disclosure? First party disclosure includes all relevant, non-privileged information in possession or control of the Crown, including the 'fruits of the investigation'. Relevant information includes not only the information that the Crown intends to adduce in evidence as part of the case against the accused, but also any information that may assist the accused in making full answer and defence.[470]

However, the Crown is not obligated to disclose information that is beyond its control. And the crown may refuse to disclose material that is clearly irrelevant or subject to privilege.[471] The Crown's discretion to refuse disclosure on the grounds it is irrelevant or subject to privilege is reviewable by the Court.[472]

The police generally investigate crime and gather evidence. Therefore, the police have a duty to disclose to the Crown all material pertaining to their investigation of the accused. The Crown also has a corresponding duty to make reasonable inquiries when put on notice of potentially relevant material in the hands of the police or other Crown entities. The Crown cannot rely on the failure to disclose relevant material on the basis that the police failed to disclose it to the Crown.[473]

The "fruits of the investigation" means the investigative files of the police, not their operational records or background information. Police may also be required to disclose information beyond the fruits of the investigation where the information is "obviously relevant" to the case against the accused.[474] Obviously relevant refers to information, which is not in the investigative file, but must be disclosed because it relates to the accused's ability to meet the Crown's case, raise a defence, or otherwise consider the conduct of the defence.[475]

Any records which are not considered first party disclosure are characterized as third-party disclosure. A defence request for third party disclosure will proceed through an *O'Connor* or third-party records application. Disclosure is subject to a two-stage application. First, the accused must establish that the records sought are "likely relevant". If the records are likely relevant, the application proceeds to the second stage. At the second stage, the applications judge will review the records in issue and determine whether, and to what extent, they should be produced to the accused.[476] To ensure that only relevant material is produced, the Court may make redactions or impose other conditions.[477]

Whether an accused seeks disclosure through a first-party disclosure request or a third-party records application, the responding party may resist the disclosure based on an assertion of privilege. As indicated in the section above, investigative privilege is the most applicable form of privilege in cases of new investigative techniques or new technologies employed by the police. Investigative privilege is a qualified privilege attached to evidence involving police investigative techniques, as a form of public interest privilege.[478] Investigative privilege may be invoked either at common law or under s.37 of the *Canada Evidence Act*. In contrast to informer privilege or solicitor-client privilege, it is not a class privilege and therefore must be assessed on a case-by-case basis. Under common law, the Crown must establish informer privilege on a balance of probabilities.[479] In order to assess the claim, the Court must determine whether the public interest in effective police investigation outweighs the interests of the accused in disclosure of the technique.[480]

In *R. v. Hughes*, the Court concluded that the following factors, among others, should be considered:

1. The nature of the technique in question. Is it one used by police in the exercise of their law enforcement functions?
2. Is the technique publicly known?
3. What will the impact of production be? Will publication of the technique enable offenders to interfere or defeat police investigations?
4. How serious are the charges before the court?
5. How probative is the evidence to the live issues in the case? Will it likely establish a fact which is crucial to the defence?
6. To what extent will sustaining the privilege impair the accused's ability to make full answer and defence?[481]

If the Crown is not successful in asserting investigative privilege over a technique under the common law, the Crown may invoke s.37 of the *Canada Evidence Act* and seek a ruling under s.37(2). If the Court orders production of evidence relating to the investigative technique, the Crown may enter a stay of proceedings in order to safeguard the privileged information.

In *R. v. Hughes*, Justice Boswell considered the Crown's disclosure obligation in relation to the digital tools that police employed to investigate Mr. Hughes' IP address, his digital devices and his online activities. In 2019, Ontario Provincial Police (OPP) used a licensed software program "Torrential Downpour" to investigate Mr. Hughes' online activity. It was alleged

that Mr. Hughes used a version of the "Torrent" software to download and share child pornography on the BitTorrent peer-to-peer file-sharing network, which connects devices directly without a central server, allowing large numbers of personal computers to connect and share files over the internet.[482]

The Torrential Downpour software communicated with Mr. Hughes' Torrent account and the OPP downloaded files containing child pornography from an electronic device controlled by Mr. Hughes and running the Torrent software. The tandem software Torrent Downpour receptor identified the IP address associated with the file share and a subsequent production order identified Mr. Hughes' mother as the subscriber. After the download, the OPP obtained a search warrant for the Hughes residence and seized Mr. Hughes' computer. A forensic examination of his computer revealed an installed copy of the version of Torrent software as well as copies of the files the OPP downloaded from Mr. Hughes' Torrent account. Mr. Hughes was charged with possession of child pornography and making child pornography available.

At trial, Mr. Hughes sought disclosure of the software, source code, user manuals and training materials for the software. At the first stage of the disclosure application, Justice Boswell concluded that the fruits of the investigation, which included the records generated by the software, and the contents of the hard drive seized from Mr. Hughes bedroom, had been disclosed. He concluded that the user manuals, in the possession of the OPP, were obviously relevant first party disclosure as they would be useful to defence in understanding how software functioned in the investigation. Justice Boswell found that the training manuals were not obviously relevant and therefore did not form part of first party disclosure.[483] On the first stage of the third-party disclosure application, he concluded that the software tools were central to the investigation against Mr. Hughes as well as the grounds the OPP relied on in the information to obtain the search warrant for the Hughes' residence. He was not persuaded that the source codes were likely relevant to the functioning of the software, the s.8 motion or a potential *Garofoli* application.[484]

In a second ruling, Justice Boswell held that the public interest in effective investigation of child pornography through the use of the software tools outweighed Mr. Hugh's interest in disclosure of operational copies of the software. The probative value of the evidence was low and conditions to mitigate the prejudice flowing from its production was not warranted. The private information in the manuals, validation test reports and logs, which included the IP address of the server, the peer ID used by the software, the way that the software identifies itself to other uses on the network, and the use of severity ratings for identifying child pornography could be redacted.

In *R. c. Mirarchi*, the court similarly considered the application of investigative privilege to advanced technological evidence with different results.[485] In *Mirarchi*, several co-accused were charged with first degree murder and conspiracy to commit murder in the context of a large-scale investigation of organized crime. The defence sought disclosure of the global encryption code used by Blackberry to secure its peer-to-peer communications, which Blackberry allowed the RCMP to access. This in turn allowed them to challenge the accuracy of the decoded messages that were essential to the prosecution. Defence also sought disclosure of information relating to the use of a mobile device identifier (MDI) which captured information and identified cell phones within a range.

The court rejected the Crown's claim of investigative privilege and ordered that the global encryption code be disclosed as well as most of the information sought by defence regarding the use of the MDI. In response, the Crown invoked s.37 of the *Canada Evidence Act*. The judge affirmed the disclosure order, except for the global encryption key, as the parties and amicus curiae jointly submitted that it should be protected by privilege and not disclosed.[486] Ultimately, the Crown did not disclose the material. The seven accused pled guilty to conspiracy to commit murder and the Crown stayed the charges against several other accused relating to their alleged involvement in organized crime.[487]

Pre-Trial Phase

The rules of evidence which most likely apply to litigation of AI techniques are authentication, best evidence rule and expert evidence.

The requirement for authentication is codified in the *Canada Evidence Act.* Section 31.1-31.8 codifies the common law test for authentication of electronic documents (which include audio and video recordings stored in a computer system): "Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be". The requirement can be established through direct or circumstantial evidence.

Authentication is of particular concern in relation to deep fakes.

In *R. v. Analib-Goortani*, Justice Trotter (as he then was), considered the admissibility of a photograph taken of an officer during the G20 Summit in Toronto. The photograph showed the officer winding up and poised to strike a female protestor with a baton. In addressing the admissibility of the photograph, Justice Trotter held that the Crown had failed to establish that the image was not tampered with or altered before it came into the Crown's possession. The evidence established that the image was downloaded from a website and there was no evidence as to who uploaded the image to that site.

The expert witnesses called by the Crown and defence could not determine how many websites or computers the image had been uploaded to or downloaded from before it was obtained. The expert witnesses were also not able to determine whether the image had been automatically stripped of its metadata during the uploading process or it was intentionally removed. Therefore, Justice Trotter was concerned that the image had been manipulated. This case demonstrates the importance of evidence, direct or circumstantial, that the electronic document is what it purports to be.

From the foregoing, it is evident how AI raises questions that may be too complex and serious to be left to ad hoc or conventional Crown / police interactions. In summary, the questions this raises are areas where clearer policies or more formalized procedures may assist in both specific cases and investigations, and more broadly, as a systemic approach to setting standard approaches to cases and investigations across the province. For instance, developing a centralized advice function or police / Crown discussion table may set standards of practice that are broadly applicable and set precedents that can be followed. The Crown Policy Manual could also update several sections to account for AI, such as [list a couple of the really outdated sections], as well as adding in new sections for managing challenges specific to AI-enabled technologies.

Among the key questions that may be considered are the following:

- What are "internal uses" of AI for automating routine tasks vs investigative use? Does the use of AI for expediting results through scanning have the same restrictions as AI for a more intrusive use – as in 24/7 FRT in the streets?
- Define what exactly is investigative use of AI
- Should AI assessment policies specifically include a requirement that any AI technology being considered for investigative use should have a crown/prosecution consultation and input prior to acquisition/use?
- Facilitating structural and operational discussions between police and Crowns on how to develop effective disclosure plans and paths to illustrate authentication and admissibility.
- Guidelines on using free AI services in an investigation that may not be part of a formal technology assessment and procurement process.
- Standards for the disclosure of AI use for investigative purposes. How for instance could this be standardized in officer's notes as part of a record management system that would be supplied to the Crown

- How will the provenance of data sets be proven, and how will training datasets and algorithms be frozen or preserved as "version in time" for the purposes of production during a trial, or subsequent investigation or review? Similarly, what retention and destruction practices should be accorded?
- What expectations or standards of explainability should be demanded for AI models in the law enforcement and investigation process?
- What continuous training and expertise will be required of judges, lawyers, and police personnel to understand, assess, discuss and disclose AI technology effectively?

3.4.4 Consultation Questions

6. Criminal AI systems raise new and complex procedural, evidential and litigation challenges, including:
   - Admissibility and reliability of AI evidence and whether AI is "expert evidence"
   - Use of AI to generate incident reports, summarize or analyze body cam data, etc.
   - AI-assisted submissions to court or disclosure summaries.
   - Deep fake evidence.
   - AI-generated witness statements, victim impact statements, Gladue reports, etc.
   - Litigating assertions of "trade secrets," "investigative privilege" or routine vs. investigative uses
   - Warrants or O'Connor Applications for third-party evidence.

   a. How can we regulate, formalize or streamline frequently litigated AI-related issues like the above?

   b. Would a routine requirement for full disclosure of an AI system and its components be mitigated by objective AI performance measures, such as independent technical audits that validate the reliability and performance of AI systems?

   c. Do we need standards or practices governing AI-generated statements/reports to ensure reliability and admissibility?

7. Criminal AI systems raise new challenges for Ontario's criminal justice institutions.

   a. Does the provincial justice system have sufficient institutional capacity to respond to these challenges? If not, what tools or supports are needed to help institutions to proactively respond to these challenges?

8. In addition to the measures discussed above, many believe there is a need for independent oversight of public sector AI system, including in criminal justice.

   a. Given that many criminal justice institutions have or are subject to forms of oversight, how would AI oversight work?

   b. Does Ontario need a new, independent oversight office or can this function be built into existing organizations?

3.5 AI For Good

Theoretically, by automating certain routine tasks and recognizing patterns in crime data, law enforcement agencies can more efficiently allocate resources. Proponents of AI argue that algorithmic systems may improve equality and fairness in law enforcement.[488] However, this conclusion relies on the premise that AI systems are neutral, computational arbitrators for law enforcement, and not biased and irrational human decision-makers. AI programming is necessarily the product of human developers and thinking. It is not immune from bias or partiality. The use of AI technology standing alone will not reduce bias in policing.

Nevertheless, there are many proposed uses of AI in policing that could mitigate bias or enable unique forms of law enforcement or police oversight. Although each should be evaluated individually, these uses may be less impacted by the problems posed by more common applications like FRT and predictive policing.

Generally, Jon Kleinberg *et al* have theorized how the use of AI in screening tasks such as predictive policing could make it easier for institutions such as law enforcement to be held accountable for discrimination.[489] Crucially, they do not assert that AI systems are inherently less biased than human decision-makers, but that certain aspects of AI-driven decision-making could be more amenable to scrutiny than their human analogues: "when algorithms are involved, proving discrimination will be easier—or at least it should be, and can be made to be."[490] Algorithmic processes can be subjected to technical experimentation – such as inputting counterfactuals, reconstructing and comparing training data, and reprogramming to screen for different "labels" or outcomes – that could precisely identify and even suggest solutions to discrete sources of bias in the system.[491] However, Kleinberg *et al* recognize this conclusion relies on two conditions that are currently lacking in the Canadian policing context: authoritative oversight by non-police entities, and full transparency on the part of law enforcement as to the data and processes employed in algorithmic decision-making.[492] Notably, police may be unable to provide full transparency if AI product vendors are unwilling to share pertinent details related to training data, models used, etc. This could be an area where procurement policies or other regulatory instruments may further public interest goals in potentially adopting AI products.

Another generally positive view of the use of AI by law enforcement is taken by Tzu-Wei Hung and Chun-Ping Yen, who have asserted that discriminatory outcomes are not inherent to AI systems and can be mostly corrected for by structural changes to their role in law enforcement.[493] In particular, Hung and Yen propose a social safety net approach in which AI predictions would be used by police in conjunction with other service providers to identify vulnerable populations and proactively deliver needed social and economic support. Rather than justifying increased police presence and operations in areas deemed high risk, predictive policing would reduce crime by proactively mitigating its root causes.

Yen and Hung point to the "hub model" employed by the Saskatchewan Police Predictive Analytics Lab as one example of a social safety net approach.[494] In the hub model, police share data with partner agencies who then use algorithmic systems similar to predictive policing to perform individual and community interventions before crime takes place.[495] One potential barrier to the success of this model, however, is its reliance on destigmatizing populations identified as "high-risk" by predictive policing algorithms.[496] Indeed, the association of police data with social services may have the opposite effect, criminalizing vulnerability factors that are not inherently related to crime or encouraging police intervention where it is unnecessary or unhelpful.

AI- and data-driven tools have shown some promise in helping to review, analyze, and ultimately improve police conduct, especially when applied to the vast stores of data created during police operations. One of the longest-standing applications of AI to police internal monitoring is use in enhancing early intervention systems (EIS).[497] EIS systems use a wide range of data to assign individual police officers a risk score indicating their likelihood of engaging in problematic conduct such as excessive use of force, allowing supervisors to intervene pre-emptively.[498] While EIS systems based on data analysis have been in use since the 1990s,[499] the addition of machine learning models has greatly improved their effectiveness.[500]

Software has also been developed to assess and predict other dimensions of police officers' behaviour that may be linked to human rights abuses. For example, while not powered by AI, LEFTA Systems' data-driven Profiling Accountability Software Solution (PASS) correlates officer civilian contact with the demographics of their patrol area to detect and report possible enforcement bias.[501]

In recent years, dozens of US police forces have begun using machine-learning software such as Truleo to scan thousands of hours of body cam footage for risky and unprofessional officer conduct.[502] These systems can use AI to analyze and classify officers' use of force, pursuits, and frisks, as well as officers' language use

and general respectfulness.[503] While these programs show some promise in helping improve officer training and reduce discriminatory policing, one drawback is that they are usually internal to the police department engaging in the review, so their findings and outcomes are rarely publicized.[504] Similar but distinct software called JusticeText has been designed for defence counsel to efficiently transcribe body cam footage and analyze the police interactions captured therein, for example to determine whether police read a person their Miranda rights.[505]

At arm's length from police forces themselves, AI has helped some scholars derive novel insights from police records that could inform law enforcement practices. For example, one study sponsored by the National Institute of Justice applied AI sentiment analysis to rape-related police incident reports to characterize officers' assessments of victim credibility, which the authors then compared to case outcomes.[506] Among other insights, the study found that "[t]he rape cases with the most successful prosecution outcomes tended to have significant positive officer sentiment and subjectivity in the police incident reports compared to reports with negative or neutral (non-significant) officer sentiment."[507] Another study used machine learning to reveal clusters of traits linked to home-grown extremist terrorism, challenging existing stereotypes.[508] Finally, Rahul Kumar Dass et al developed specialized FRT to "fill in" missing data on offenders' race based on catalogued arrest photos; theoretically, more complete data could fuel more accurate analyses of discriminatory policing.[509]

More broadly, AI has been instrumental in opening a variety of new capabilities for law enforcement, particularly in areas where traditional methods are limited or have failed. One example is the application of AI to cold cases: as in the extensively publicized Mark Himebaugh missing child case,[510] AI can help find new leads for unsolved cases through methods like facial aging[511] and uncovering patterns indicating a serial killer.[512] AI is also expected to greatly increase the predictive power of numerous forensic science disciplines,[513] such as the field of DNA analysis discussed above.

Other diverse law enforcement applications for which AI-powered tools have been developed or deployed include:

- digital accident scene reconstruction[514]
- minimally invasive "virtual" autopsies[515]
- assessing the confidence of verbal eyewitness statements without contextual bias[516]
- detecting crime-related social media activity[517]
- exposing deepfakes that may contribute to election disinformation[518]
- monitoring the dark web for cyber-security threats[519]
- automatically reporting live-streamed suicide attempts[520]
- locating missing children[521]
- identifying child pornography without human operators having to view the suspected images[522]
- investigating modern slavery by analyzing patterns in financial transactions, communication, transportation, and satellite imagery.[523]

While many of these applications are promising, they are also presumably vulnerable to many of the same human rights issues that accompany better-known AI-powered police technology such as FRT and predictive policing. Any new application should therefore be analyzed critically, and regulation should be structured to capture a broad range of existing and emerging technologies.

4. Next Steps and Summary of Consultation Questions

4.1 Consultation Process

The LCO's consultation process starts with the release of this Issues Paper.

The LCO wants to hear from a broad range of stakeholders including lawyers and legal organizations, NGOs, industry representatives, academics, government and justice system leaders, and individual Ontarians interested in the operation of the criminal justice system.

The LCO will be organizing several consultation processes over the next several months. The LCO is strongly committed to partnering with interested organizations and stakeholders to develop consultation initiatives. Individuals or organizations interested in working with the LCO are encouraged to contact our Project Lead.

The LCO also encourages written submissions, which can be sent to the LCO's general email address at LawCommission@lco-cdo.org.

The deadline for written submissions is **July 7, 2025**.

The LCO is committed to sharing ideas and building constructive dialogue. Accordingly, the LCO expects to post written submissions on our project webpage, subject to limited exceptions. Individuals or organizations wishing to provide a written submission may want to contact the LCO for further information prior to their submission.

Project Lead and Contacts

The LCO's Project Lead is Ryan Fritsch. Ryan can be contacted at rfritsch@lco-cdo.org.

The LCO can also be contacted at:

Law Commission of Ontario
2032 Ignat Kaneff Building
Osgoode Hall Law School, York University
4700 Keele Street
Toronto, Ontario, Canada
M3J 1P3

LawCommission@lco-cdo.org

4.2 Consultation Questions

1. The discussion suggests the need for provincial rules establishing key trustworthy criminal AI rules and criteria. The Issue Papers suggest many potential models, including:
   - Federal legislation or regulations (Criminal Code, federal ADM Directive?).
   - Provincial legislation or regulation (EDSTA, policing legislation, Ontario AI Directive?).
   - Criminal justice institutional policies (Police, courts, Crown Policy Manual?).

   a. Do you agree some kind of provincial framework is necessary? If so, which approach (or approaches) is best and why?

2. The EU AI Act, AIDA, and the Toronto Police Services AI policy all adopt some form of risk-based AI governance, including presumptive prohibited uses and/or presumptive "high risk" AI systems subject to stricter requirements and more oversight.
   a. In principle, do you agree with the prohibited/high risk framework? What criteria should be adopted to identify prohibited or high-risk systems? Does Canadian law suggest which, or how, different AI systems or uses ought to be categorized?
   b. If you agree some systems or uses should be prohibited or identified as "high-risk":
      - What AI systems or uses should be in these categories?
      - Should real time FRT or predictive policing be prohibited? If so, are there reasonable exceptions, such as FRT to assist missing persons investigations? What rules should apply?
      - What oversight rules or procedural requirements are appropriate for high-risk systems?

3. Disclosure is a consistent theme in trustworthy criminal AI legislation and frameworks. There are choices about the timing, form and substance of disclosure obligations.
   a. How and to what extent should criminal AI systems be disclosed?
   b. Should there be a mandatory AI register or public report? If so, what should be included:
      - A detailed or summary impact assessment?
      - Comprehensive or a summary description of training data?
      - Output data to facilitate independent auditing, oversight and performance monitoring?
      - How to promote disclosure while protecting other legitimate objectives, such as sensitive investigating techniques?

4. The need for impact assessments is a consistent theme in criminal AI legislation and frameworks. There are choices about the timing, form and substance of impact assessments.
   a. Should the province require a mandatory impact assessment for criminal AI systems in Ontario? Do you agree an impact assessment should address privacy, human rights and procedural fairness and provide assurances about how an AI system will comply with other legal obligations?
   b. What other information or risks should be included?
   c. How best to ensure impact assessments are being used and reported consistently?

5. Many criminal AI systems have been criticized by communities who believe they were not consulted or informed about systems that affect them. Many trustworthy criminal AI initiatives, including the Toronto Police Service AI Policy, include public engagement requirements.
   a. How should the public be involved in criminal AI policymaking, evaluation or oversight?

6. Criminal AI systems raise new and complex procedural, evidential and litigation challenges, including:
    - Admissibility and reliability of AI evidence and whether AI is "expert evidence"
    - Use of AI to generate incident reports, summarize or analyze body cam data, etc.
    - AI-assisted submissions to court or disclosure summaries.
    - Deep fake evidence.
    - AI-generated witness statements, victim impact statements, Gladue reports, etc.
    - Litigating assertions of "trade secrets," "investigative privilege" or routine vs. investigative uses
    - Warrants or O'Connor Applications for third-party evidence.

    a. How can we regulate, formalize or streamline frequently litigated AI-related issues like the above?

    b. Would a routine requirement for full disclosure of an AI system and its components be mitigated by objective AI performance measures, such as independent technical audits that validate the reliability and performance of AI systems?

    c. Do we need standards or practices governing AI-generated statements/reports to ensure reliability and admissibility?

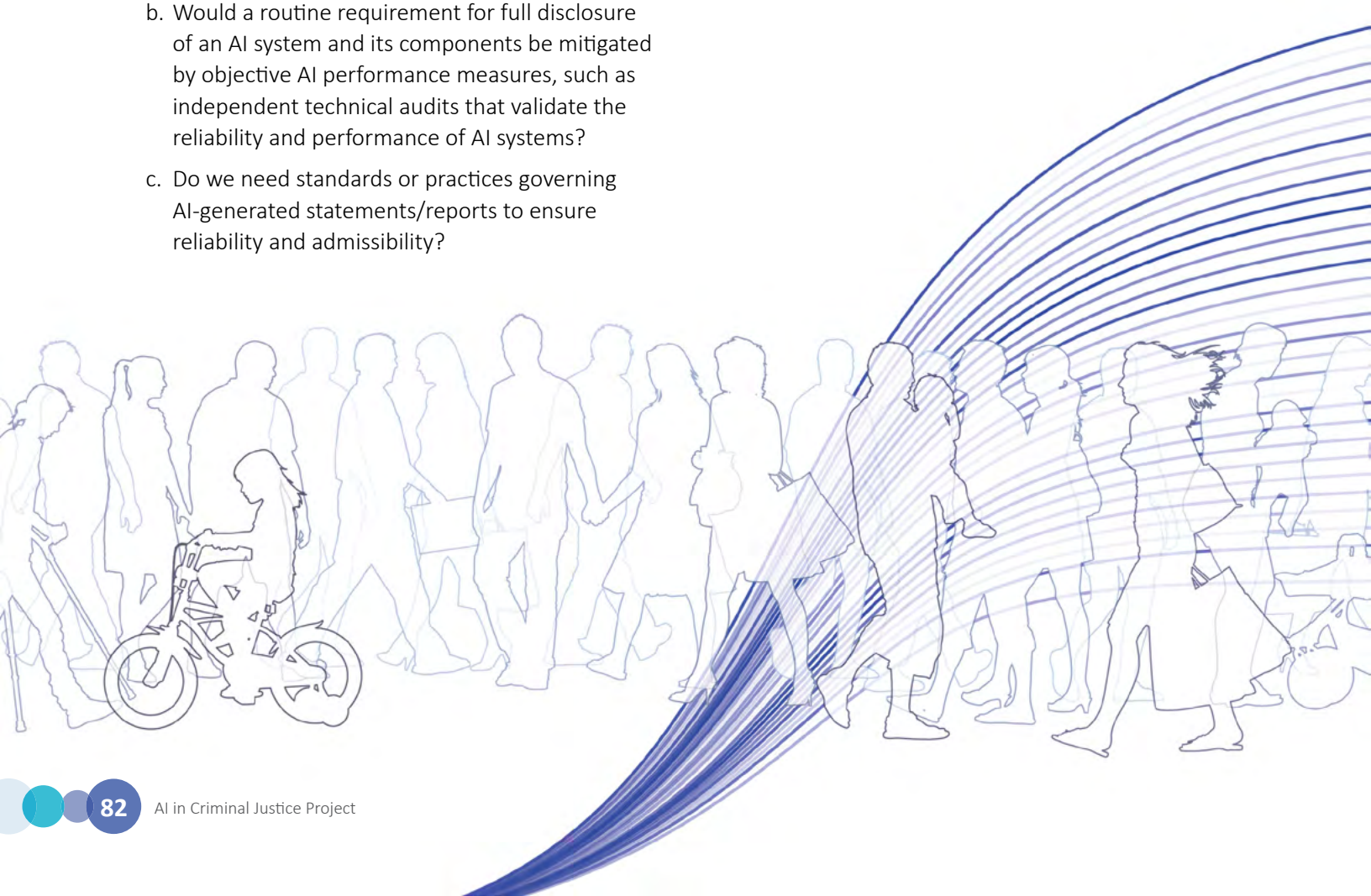
7. Criminal AI systems raise new challenges for Ontario's criminal justice institutions.

    a. Does the provincial justice system have sufficient institutional capacity to respond to these challenges? If not, what tools or supports are needed to help institutions to proactively respond to these challenges?

8. In addition to the measures discussed above, many believe there is a need for independent oversight of public sector AI system, including in criminal justice.

    a. Given that many criminal justice institutions have or are subject to forms of oversight, how would AI oversight work?

    b. Does Ontario need a new, independent oversight office or can this function be built into existing organizations?



5. Endnotes

1 The author thanks the many hands who contributed to this paper, including members of the criminal defense bar, criminal prosecutors, criminal justice policy experts, law enforcement, and the many law students who dedicate their summers to further the work of the LCO.

2 See for instance: Office of the Privacy Commissioner of Canada, "RCMP's use of Clearview AI's facial recognition technology violated Privacy Act, investigation concludes" (June 10, 2021), online: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210610/; RCMP, National Technology Onboarding Program, *Transparency Blueprint: Snapshot of Operational Technologies* (2024), at p 21, online: https://rcmp.ca/sites/default/files/doc/national-technology-onboarding-program-transparency-blueprint.pdf; Information and Privacy Commissioner of Ontario, "Facial Recognition and Mugshot Databases: Guidance for Police in Ontario" (February 1, 2024), online: https://www.ipc.on.ca/en/resources-and-decisions/facial-recognition-and-mugshot-databases-guidance-police-ontario; Information and Privacy Commissioner of Ontario, "Letter to the Toronto Police Services Board about facial recognition mugshot database program" (January 10, 2024), online: https://www.ipc.on.ca/en/resources-and-decisions/letter-toronto-police-services-board-about-facial-recognition-mugshot-database-program; Vancouver Police Department, "Vancouver Police Adopt New Technology to Predict Property Crime" (July 21 2017), online: https://vpd.ca/news/2017/07/21/vancouver-police-adopt-new-technology-to-predict-property-crime/; Globe and Mail, "RCMP wants to use AI to learn passwords in investigations, but experts warn of privacy risks" (November 25, 2021), online: https://www.theglobeandmail.com/business/article-rcmps-plan-to-use-ai-to-learn-passwords-in-investigations-has-privacy/; and Toronto Star, "A plan to separate out high-risk inmates is leading to violence at this Toronto jail, sources say " (July 5 2022), online: https://www.thestar.com/news/gta/a-plan-to-separate-out-high-risk-inmates-is-leading-to-violence-at-this-toronto/article_a9eb292e-997b-516b-9ca6-e210e418bfc6.html.

3 The Guardian, "Revealed: the software that studies your Facebook friends to predict who may commit a crime" (November 17, 2021), online: https://www.theguardian.com/us-news/2021/nov/17/police-surveillance-technology-voyager; Chicago Sun-Times, "Illinois' use of cameras that read license plates amounts to 'dragnet surveillance,' lawsuit alleges" (June 2, 2024), online: https://chicago.suntimes.com/crime/2024/06/02/illinois-lawsuit-license-plate-readers-alpr-police-surveillance-police-pritzker-raoul-police-isp; Wired.com, "The Age of the Drone Police Is Here" (June 5, 2024), online: https://www.wired.com/story/the-age-of-the-drone-police-is-here/; OSINT Combine, NexusXplore, online: https://www.osintcombine.com/platform; and 404media.com, "The Powerful AI Tool That Cops (or Stalkers) Can Use to Geolocate Photos in Seconds" (January 20, 2025), online: https://www.404media.co/the-powerful-ai-tool-that-cops-or-stalkers-can-use-to-geolocate-photos-in-seconds/.

4 See for instance: https://www.lco-cdo.org/wp-content/uploads/2020/10/Criminal-AI-Paper-Final-Oct-28-2020.pdf.

5 Parliament of Canada, BillC-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts (first reading June 16, 2022), online: https://www.parl.ca/legisinfo/en/bill/44-1/c-27.

6 Canada, Directive on Automated Decision-Making (updated April 25, 2023), online: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592

7 Canada, Directive on Automated Decision-Making (2021) at s. 5.4, online: https://publications.gc.ca/collections/collection_2021/sct-tbs/BT48-31-2021-eng.pdf.

8 Letter from François-Philippe Champagne (Minister of Innovation, Science and Economic Development Canada) to the House of Commons' Standing Committee on Industry and Technology (November 28, 2023), online: https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12751351/12751351/MinisterOfInnovationScienceAndIndustry-2023-11-28-Combined-e.pdf at 38.

9 Ontario, Bill 194, *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024* (introduced for first reading May 13, 2024; royal assent received November 25, 2024): https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194.

10 Bill 194, *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024* (introduced for first reading May 13, 2024; second reading May 28, 2024): https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194 at Schedule 1, *Enhancing Digital Security and Trust Act, 2024* (May 13, 2024): https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194#BK3.

11 Preamble to Ontario, Bill 194, *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024* (introduced for first reading May 13, 2024; second reading May 28, 2024): https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194.

12 For a comprehensive analysis of Bill 194, see: Law Commission of Ontario, "Submission to Ontario re Bill 194" (June 2024): https://www.lco-cdo.org/wp-content/uploads/2024/06/LCO-Submission-to-Government-of-Ontario-Bill-194-Consultations-June-2024.pdf. The LCO also recently testified on Bill 194 and is frequently cited in legislative debates. See Legislature of Ontario, "Submissions of MPP Tom Rakocevic re LCO Recommendations," 3rd Reading of *Consumer Protection Act, 2023* (December 4 2023), online: https://www.ola.org/en/legislative-business/house-documents/parliament-43/session-1/2023-12-04/hansard#P1303_287298.

13 Law Commission of Ontario, "Submission to Ontario re Bill 194" (June 2024): https://www.lco-cdo.org/wp-content/uploads/2024/06/LCO-Submission-to-Government-of-Ontario-Bill-194-Consultations-June-2024.pdf.

14 Ontario, Management Board of Cabinet, Ministry of Public and Business Service Delivery and Procurement, "Responsible Use of Artificial Intelligence Directive" (December 1, 2024) (on file with the LCO). The Ontario AI Directive has not been made public, but the provincial government has provided the LCO with a copy.

15 Ontario, Management Board of Cabinet, Ministry of Public and Business Service Delivery and Procurement, "Responsible Use of Artificial Intelligence Directive" (December 1, 2024) (on file with the LCO), at 3.

16 Ontario, Management Board of Cabinet, Ministry of Public and Business Service Delivery and Procurement, "Responsible Use of Artificial Intelligence Directive" (December 1, 2024) (on file with the LCO), at 4.

17 Ontario, Management Board of Cabinet, Ministry of Public and Business Service Delivery and Procurement, "Responsible Use of Artificial Intelligence Directive" (December 1, 2024) (on file with the LCO), at 4-5.

18 Provincial Responsible AI Directive, s. 4 creates the possibility of ministries or agencies obtaining an exemption to the Directive. However, there is no information, guidance or criteria for why or how an exemption would be granted. This power could effectively exempt AI systems used in policing and other high-risk applications

19 For example, the Provincial Responsible AI Directive does not include explicit provisions respecting: a public AI registry; mitigation strategies; Impact assessments; third party audits; consultations; and explainability.

20 The Provincial Responsible AI Directive does not include risk categories or guidance or metrics for how AI risks are to be identified or assessed. Most obviously, the Directive does not identify prohibited AI systems or criteria to determine if a system should be prohibited. Section 6 introduces "risk management obligations" where Ministries must "identify risks" and "assess risks" and "report and monitor risk assessments". However, it is unclear how and what risks are to be assessed/identified or what information needs to be reported.

21 Provincial Responsible AI Directive, sections 6.2 and 6.3 include disclosure obligations. However, there is no detail about what information is required to be disclosed or where or how it is to be disclosed. Or how or where individuals are to "seek information" about the use of an AI system? Perhaps most importantly, the Directive does not establish a public AI registry.

22 The Provincial Responsible AI Directivedoes not specify a right for an individual to appeal a decision made or influenced by an AI system. On the contrary, the Directive explicitly states that there is no new form of recourse for seeking review of decisions. Existing legislative avenues to appeal apply (sections 6.2 and 6.3). Nor does the Directive mention if or how the Directive will be enforced.

23 See the discussion, for instance, in Sino Esthappan, "Assessing the Risks of Risk Assessments: Institutional Tensions and Data Driven Judicial Decision-Making in U.S. Pretrial Hearings" (Journal of Social Problems, Spae060 (October 10 2024)), online: https://doi.org/10.1093/socpro/spae060.

24 On micro-directives, see for instance: Slate.com (Jonathon W. Penney and Bruce Schneier), "A.I. Micro-directives Could Soon Be Used for Law Enforcement And they're terrifying" (July 17 2023), online: https://slate.com/technology/2023/07/artificial-intelligence-microdirectives.html.

25 See the discussion, for instance, in Sino Esthappan, "Assessing the Risks of Risk Assessments: Institutional Tensions and Data Driven Judicial Decision-Making in U.S. Pretrial Hearings" (Journal of Social Problems, Spae060 (October 10 2024)), online: https://doi.org/10.1093/socpro/spae060.

26 For instance, see Canada's Department of Justice annual report which includes a discussion on the use of AI tools: Department of Justice (Canada), Results: What We Achieved: 2022-2023 Departmental Report, online: https://www.justice.gc.ca/eng/rp-pr/cp-pm/dpr-rr/2022_2023/rep-rap/results-resultats.html?wbdisable=true.

27 See RCMP, National Technology Onboarding Program, *Transparency Blueprint: Snapshot of Operational Technologies* (2024), at p 19, online: https://rcmp.ca/sites/default/files/doc/national-technology-onboarding-program-transparency-blueprint.pdf.

28 For example, the Sophia.chat website offers "a chatbot to help people suffering from abuse. 24/7, anonymous, wherever you are in the world." See: https://sophia.chat/. See also Matt Reynolds, "Locked in: Criminal Justice Startups Tap into Generative AI's Early Promise," *ABA Journal* (1 February 2024), online: <https://www.abajournal.com/legalrebels/article/locked-in-criminal-justice-startups-tap-into-generative-ais-early-promise>; Rasa Legal, *rasa-legal.com* (accessed 20 June 2024).

29 Correspondence from Laila Martin, A. Director, National Technology Onboarding Program Technical Operations, Royal Canadian Mounted Police (RCMP) to Law Commission of Ontario (May 2024), on file with the LCO. Also see: RCMP, "National Technology Onboarding Program – Transparency Blueprint: Snapshot of operational technologies" (July 16 2024), online: https://rcmp.ca/en/corporate-information/publications-and-manuals/national-technology-onboarding-program-transparency-blueprint.

30 Toronto Police Services Board, "Use of Artificial Intelligence Technology" (February 28, 2022; updated January 11, 2024): https://tpsb.ca/policies-by-laws/board-policies/195-use-of-artificial-intelligence-technology.

31 Durham Regional Police Service Board, "Use of Artificial Intelligence" (October 15 2024), online: https://durhampoliceboard.ca/wp-content/uploads/2024/10/Policy-Use-of-AI.pdf.

32 Federal Court of Canada, "Interim Principles and Guidelines on the Court's Use of Artificial Intelligence" (December 20, 2023), online: https://www.fct-cf.gc.ca/en/pages/law-and-practice/artificial-intelligence; and Federal Court of Canada, "Notice to the Parties and the Profession: The Use of Artificial Intelligence in Court Proceedings" (December 20, 2023), online: https://www.fct-cf.gc.ca/Content/assets/pdf/base/2023-12-20-notice-use-of-ai-in-court-proceedings.pdf.

33 Alberta, "Notice to the Profession & Public- Ensuring the integrity of court submissions when using Large Language Models" (October 2023): https://www.albertacourts.ca/kb/resources/announcements/notice-to-the-profession-public---use-of-ai-in-citations-submissions; Manitoba, "RE: USE OF ARTIFICIAL INTELLIGENCE IN COURT SUBMISSIONS (June 2023): https://www.manitobacourts.mb.ca/site/assets/files/2045/practice_direction_-_use_of_artificial_intelligence_in_court_submissions.pdf; Qubec, "Integrity of Court Submissions When Using Large Language Models" (October 2023): https://coursuperieureduquebec.ca/fileadmin/cour-superieure/Communiques_and_Directives/Montreal/Avis_a_la_Communite_juridique-Utilisation_intelligence_artificielle_EN.pdf.

34 Canadian Judicial Council, *Guidelines for the Use of Artificial Intelligence in Canadian Courts, 1st Edition* (September 2024), online: https://cjc-ccm.ca/sites/default/files/documents/2024/AI%20Guidelines%20-%20FINAL%20-%202024-09%20-%20EN.pdf.

35 Communication on file with the LCO.

36 See Ontario Bar Association, "Justice of Ontario's Top Court Urges Lawyers and Judges to Prepare for AI in Court" (October 8 2024), online: https://www.oba.org/JUST/Practice_List/2024/November-2024/Justice-of-Ontarios-Top-Court-Urges-Lawyers-and-J. See also Ontario Court of Appeal, Civil Rules Committee, "Changes Regarding Civil Appeal Factum Requirements" (not dated), online: https://www.ontariocourts.ca/coa/about-the-court/civil-rules-committee/#Changes_Regarding_Civil_Appeal_Factum_Requirements.

37 See Ontario Bar Association, "Justice of Ontario's Top Court Urges Lawyers and Judges to Prepare for AI in Court" (October 8 2024), online: https://www.oba.org/JUST/Practice_List/2024/November-2024/Justice-of-Ontarios-Top-Court-Urges-Lawyers-and-J.

38 Law Society of Ontario, "Licensee's use of generative artificial intelligence" (April 2024): https://lawsocietyontario.azureedge.net/media/lso/media/about/convocation/2024/convocation-april-2024-futures-committee-report.pdf.

39 Law Society of British Columbia: "Guidance on Professional Responsibility and Generative AI" (October 2023): https://www.lawsociety.bc.ca/Website/media/Shared/docs/practice/resources/Professional-responsibility-and-AI.pdf; Law Society of Alberta "The Generative AI Playbook" (not dated): https://www.lawsociety.ab.ca/resource-centre/key-resources/professional-conduct/the-generative-ai-playbook/; Law Society of Saskatchewan, "Guidelines for the Use of Generative Artificial Intelligence in the Practice of Law" (updated February 2024): https://www.lawsociety.sk.ca/wp-content/uploads/Law-Society-of-Saskatchewan-Generative-Artificial-Intelligence-Guidelines.pdf.

40 European Bars Federation, "Guidelines on how lawyers should take advantage of the opportunities offered by large language models and generative AI" (June 2023): https://www.fbe.org/wp-content/uploads/2023/06/European-lawyers-in-the-era-of-ChatGPT-FBE-Guidelines-on-how-lawyers-should-take-advantage-of-the-opportunities-offered-by-large-language-models-and-gene-kopia.pdf; Law Societies of England and Wales, "Generative AI – The Essentials" (November 2023): https://www.lawsociety.org.uk/topics/ai-and-lawtech/generative-ai-the-essentials.

41 United Kingdom Courts and Tribunals Judiciary, "Artificial Intelligence (AI) – Judicial Guidance" (December 2023): https://www.judiciary.uk/guidance-and-resources/artificial-intelligence-ai-judicial-guidance/.

42 See: Information and Privacy Commissioner of Ontario, "Letter to the Toronto Police Services re AI Policy and Risk Classification Report" (January 10, 2024) online: https://www.ipc.on.ca/resource/letter-to-the-toronto-police-services-board-about-facial-recognition-mugshot-database-program/; and Ontario Human Rights Commission, "Approval of high-risk technologies under the Toronto Police Services Board's Policy on the use of artificial intelligence technology" (January 10 2024): https://www.ohrc.on.ca/en/news_centre/approval-high-risk-technologies-under-toronto-police-services-boards-policy-use-artificial.

43 The Citizen Lab, *To Surveil and Predict A Human Rights Analysis of Algorithmic Policing in Canada* (September 1, 2020), online: https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/.

44 European Union, Artificial Intelligence Act (Regulation (EU) 2024/1689 of the European Parliament and of the Council (June 13, 2024), online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

45 See for instance: the *AI in Government Act of 2020* (Pub. L. No. 116-260, div. U, title 1, § 104 (codified at 40 U.S.C. § 11301): https://www.congress.gov/116/plaws/publ260/PLAW-116publ260.pdf); *Advancing American AI Act* (Pub. L. No. 117-263, div. G, title LXXII, subtitle B, §§ 7224(a), 7224(d)(1)(B), and 7225 (codified at 40 U.S.C. 11301): https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf; United States, Office of the President, Executive Order 14110 "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" (November 1 2023): https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence; and the United States, Executive Office of the President, Office of Management and Budget, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence" (March 28 2024): https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf. Readers are further alerted to the fact that these Executive Orders were rescinded by the Trump administration in January 2025.

46 The scheme for breathalyzers is set out in the Criminal Code of Canada, "Investigative Matters – Testing for presence of alcohol or drug" at s. 320.27-320.34, online: https://laws-lois.justice.gc.ca/eng/acts/C-46/page-47.html#docCont. See LCO AI in Criminal Law Project, Annex C, Project Case Studies, and Paper 4, AI at Trial and On Appeal, for further discussion of breathalyzers in this context.

47 Slate.com (Jonathon W. Penney and Bruce Schneier) "A.I. Micro-directives Could Soon Be Used for Law Enforcement And they're terrifying" (July 17 2023), online: https://slate.com/technology/2023/07/artificial-intelligence-microdirectives.html. Micro-directives are already here. The authors suggest micro-directives are already used in examples where enforcement proceeds automatically, like automated speeding cameras, DMCA and copyright take-down notices, and breathalyzer tests. The belief is that AI could vastly scale-up the deployment of micro-directives in any number of cases, creating a creeping and pervasive state of surveillance and enforcement.

48 MIT Technology Review, "How the largest gathering of US police chiefs is talking about AI" (November 19 2024), online: https://www.technologyreview.com/2024/11/19/1106979/how-the-largest-gathering-of-us-police-chiefs-is-talking-about-ai/.

49 MIT Technology Review, "How the largest gathering of US police chiefs is talking about AI" (November 19 2024), online: https://www.technologyreview.com/2024/11/19/1106979/how-the-largest-gathering-of-us-police-chiefs-is-talking-about-ai/.

50 See Government of Canada / RCMP, "Algorithmic Impact Assessment Results- Griffeye Tool" (March 26, 2024), at p 4, online: https://open.canada.ca/data/en/dataset/89898244-aaae-4591-ba9b-fe5cd81d5924/resource/dd50ce04-3150-4f26-b8ab-0ad067489593.

51 ChatGPT was released in December 2022 and DALL-E around the same time. Four months later, dozens of similar tools became available and continue to multiply. See, for instance, Fast Company (Danica Lo), "What is generative AI? Your questions answered" (March 12, 2023), online: https://www.fastcompany.com/90867920/best-ai-tools-content-creation.

52 Robert Chesney and Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" in California Law Review (2019; Volume 107), online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954 at 1758.

53 Francesca Palmiotto, "Detecting Deep Fake Evidence with Artificial Intelligence: A Critical Look from a Criminal Law Perspective" on SSRN (March 10, 2023), online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4384122 at 2.

54 Robert Chesney and Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security" in California Law Review (2019; Volume 107), online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954 at 1753.

55 ArsTechnica, "Cops bogged down by flood of fake AI child sex images, report says; Investigations tied to harmful AI sex images will grow "exponentially"" (January 31 2024), online: https://arstechnica.com/tech-policy/2024/01/surge-of-fake-ai-child-sex-images-thwarts-investigations-into-real-child-abuse/.

56 ArsTechnica, "School athletic director arrested for framing principal using AI voice synthesis" (April 25 2024): https://arstechnica.com/information-technology/2024/04/alleged-ai-voice-imitation-leads-to-arrest-in-baltimore-school-racism-controversy/.

57 See NBC News, "Washington state judge blocks use of AI-enhanced video as evidence in possible first-of-its-kind ruling" (April 2 2024): https://www.nbcnews.com/news/us-news/washington-state-judge-blocks-use-ai-enhanced-video-evidence-rcna141932.

58 *R. v. Larouche,* 2023 QCCQ 1853 at paras 63-66. See also *R. v. Legault*, 2024 BCPC 29, where the accused used a deep fake program to create child pornography.

59 R. v. *Larouche*, 2023 QCCQ 1853 at para 68.

60 R. v. *Larouche*, 2023 QCCQ 1853 at para 69.

61 See The Canadian Press (Jacob Serebrin), "Quebec man who created synthetic, AI-generated child pornography sentenced to prison" (April 26, 2023), online: https://www.cbc.ca/news/canada/montreal/ai-child-abuse-images-1.6823808.

62 R. v. *Larouche*, 2023 QCCQ 1853 at paras 69-70. See, for example, ArsTechnica (Benj Edwards), "OpenAI confirms that AI writing detectors don't work" (September 8, 2023), online: https://arstechnica.com/information-technology/2023/09/openai-admits-that-ai-writing-detectors-dont-work/. There is also some evidence that image detectors may be better at identifying AI-generated images. These detectors have limited reliability. See ZD.net (Maria Diaz), "Google's new tool can detect AI-generated images, but it's not that simple" (September 1, 2023), online: https://www.zdnet.com/article/googles-new-tool-can-detect-ai-generated-images-but-its-not-that-simple/.

63 Ontario Bar Association, "Justice of Ontario's Top Court Urges Lawyers and Judges to Prepare for AI in Court" (October 8 2024), online: https://www.oba.org/JUST/Practice_List/2024/November-2024/Justice-of-Ontarios-Top-Court-Urges-Lawyers-and-J.

64 ArsTechnica, "Deepfakes in the courtroom: US judicial panel debates new AI evidence rules" (April 24 2024): https://arstechnica.com/information-technology/2024/04/deepfakes-in-the-courtroom-us-judicial-panel-debates-new-ai-evidence-rules/.

65 Among various industry efforts underway is the US AI Safety Institute Consortium of "AI creators and users, academics, government and industry researchers, and civil society organizations" working to develop "guidelines for red-teaming, capability evaluations, risk management, safety and security, and watermarking synthetic content." See US Department of Commerce, "Biden-Harris Administration Announces First-Ever Consortium Dedicated to AI Safety" (February 8, 2024), online: https://www.commerce.gov/news/press-releases/2024/02/biden-harris-administration-announces-first-ever-consortium-dedicated. The full list of consortium members includes Apple, Adobe, Anthropic, Canva, Boston Scientific, Microsoft and OpenAI.

66 See for example "watermarking," "labelling synthetic content" and "reasonable steps to watermark or otherwise label output from generative AI" in United States, Office of the President, Executive Order 14110 "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" (November 1 2023): https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence at sections 3(gg), 4.5(a)(ii), and 10.1(b)(viii)(C).

67 Toronto Police Services, Update on the Implementation of the Board's Policy on the Use of AI Technology (January 11 2024) online: https://tpsb.ca/jdownloads-categories?task=download.send&id=813:january-11-2024-public-agenda&catid=32

68 RCMP, National Technology Onboarding Program, Transparency Blueprint: Snapshot of Operational Technologies (2024), at p19-20, online: https://rcmp.ca/sites/default/files/doc/national-technology-onboarding-program-transparency-blueprint.pdf.

69 RCMP, National Technology Onboarding Program, Transparency Blueprint: Snapshot of Operational Technologies (2024), at p19-20, online: https://rcmp.ca/sites/default/files/doc/national-technology-onboarding-program-transparency-blueprint.pdf.

70 RCMP, National Technology Onboarding Program, Transparency Blueprint: Snapshot of Operational Technologies (2024), at p19-20, online: https://rcmp.ca/sites/default/files/doc/national-technology-onboarding-program-transparency-blueprint.pdf.

71 Canada, Department of Innovation, Science and Economic Development Canada, "AI decryption service" (November 4 2021): https://ised-isde.canada.ca/site/innovative-solutions-canada/en/ai-decryption-service. See also Globe and Mail, "RCMP wants to use AI to learn passwords in investigations, but experts warn of privacy risks" (November 5 2021): https://www.theglobeandmail.com/business/article-rcmps-plan-to-use-ai-to-learn-passwords-in-investigations-has-privacy/.

72 Globe and Mail, "RCMP wants to use AI to learn passwords in investigations, but experts warn of privacy risks" (November 5 2021): https://www.theglobeandmail.com/business/article-rcmps-plan-to-use-ai-to-learn-passwords-in-investigations-has-privacy/.

73 The Privacy Commissioner of Canada et. al., Joint Investigation of Clearview AI (February 2021): https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/.

74 RCMP, National Technology Onboarding Program, Transparency Blueprint: Snapshot of Operational Technologies (2024), at p 6-7, online: https://rcmp.ca/sites/default/files/doc/national-technology-onboarding-program-transparency-blueprint.pdf.

75 See RCMP, National Technology Onboarding Program, *Transparency Blueprint: Snapshot of Operational Technologies* (2024), at p 19-20, online: https://rcmp.ca/sites/default/files/doc/national-technology-onboarding-program-transparency-blueprint.pdf. See also RCMP, "Babel X platform: Overview and privacy impact assessment initiation" (October 25 2022), online: https://www.rcmp-grc.gc.ca/en/babel-x-platform.

76 Toronto Star, "As police increasingly use facial recognition technology, calls grow for regulations" (June 30 2024): https://www.thestar.com/news/canada/quebec/as-police-increasingly-use-facial-recognition-technology-calls-grow-for-regulations/article_60d524fa-4beb-5731-8a05-d9e4844da4e5.html.

77 Vancouver Police Department, "Vancouver Police Adopt New Technology to Predict Property Crime" (July 21 2017): https://vpd.ca/news/2017/07/21/vancouver-police-adopt-new-technology-to-predict-property-crime/.

78 Vancouver Police Department, "Vancouver Police Adopt New Technology to Predict Property Crime" (July 21 2017): https://vpd.ca/news/2017/07/21/vancouver-police-adopt-new-technology-to-predict-property-crime/.

79 See for example Andrew Guthrie Ferguson, "Predictive Policing Theory" published as Chapter 24 in Tamara Rice Lave and Eric J. Miller (eds.), The Cambridge Handbook of Policing in the United States (Cambridge Univ. Press (2019)), online: https://ssrn.com/abstract=3516382 at 492.

80 Palantir Platforms (Gotham): https://www.palantir.com/platforms/.

81 The Logic (David Reevely and Murad Hemmadi), "Ontario Provincial Police use controversial data-mining platform Palantir for crime analysis" (October 20, 2022), online: https://thelogic.co/news/exclusive/ontario-provincial-police-use-controversial-data-mining-platform-palantir-for-crime-analysis/.

82 Livewire Calgary (Aryn Toombs), "Calgary Police Service looking to public to govern use of policing technology" (April 28, 2022), online: https://livewirecalgary.com/2022/04/28/calgary-police-service-public-policing-tech-data/.

83 Toronto Star, "A plan to separate out high-risk inmates is leading to violence at this Toronto jail, sources say" (July 5, 2022): https://www.thestar.com/news/gta/a-plan-to-separate-out-high-risk-inmates-is-leading-to-violence-at-this-toronto/article_a9eb292e-997b-516b-9ca6-e210e418bfc6.html.

84 Toronto Star, "A plan to separate out high-risk inmates is leading to violence at this Toronto jail, sources say" (July 5, 2022): https://www.thestar.com/news/gta/a-plan-to-separate-out-high-risk-inmates-is-leading-to-violence-at-this-toronto/article_a9eb292e-997b-516b-9ca6-e210e418bfc6.html.

85 Toronto Police Services Board, "Use of Artificial Intelligence Technology" (February 28, 2022; updated January 11, 2024): https://tpsb.ca/policies-by-laws/board-policies/195-use-of-artificial-intelligence-technology.

86 Correspondence from Laila Martin, A. Director, National Technology Onboarding Program Technical Operations, Royal Canadian Mounted Police (RCMP) to Law Commission of Ontario (May 2024), on file with the LCO.

87 TechScape: How police use location and search data to find suspects – and not always the right ones https://www.theguardian.com/technology/2023/oct/03/techscape-geofence-warrants

88 See for example, Forbes.com, "Post-Roe, Your Period App Data Could Be Used Against You" (November 14, 2024), online: https://www.forbes.com/sites/abigaildubiniecki/2024/11/14/post-roe-your-period-app-data-could-be-used-against-you/.

89 Gizmodo.com, "Google Finally Stops Handing Your Location Data to Cops: A location privacy change will end Google's compliance with constitution-busting geofence warrants" (December 15, 2023), online: https://gizmodo.com/google-ends-geofence-warrants-location-data-tracking-1851102594.

90 EFF.org, "Adtech Surveillance and Government Surveillance are Often the Same Surveillance" (October 18, 2023), online: https://www.eff.org/deeplinks/2023/10/adtech-surveillance-and-government-surveillance-are-often-same-surveillance.

91 Forbes.com (Thomas Brewster), "FedEx's Secretive Police Force Is Helping Cops Build An AI Car Surveillance Network" (June 19, 2024), online: https://www.forbes.com/sites/thomasbrewster/2024/06/19/fedex-police-help-cops-build-an-ai-car-surveillance-network/.

92 Bloomberg.com, "NYC Surveillance Tech on Shootings Gives False Alarms 87% of Time, Audit Finds" (June 20, 2024), online: https://www.bloomberg.com/news/articles/2024-06-20/nyc-shotspotter-tech-wastes-nypd-police-time-and-money-audit-finds.

93 Bloomberg.com, "NYC Surveillance Tech on Shootings Gives False Alarms 87% of Time, Audit Finds" (June 20, 2024), online: https://www.bloomberg.com/news/articles/2024-06-20/nyc-shotspotter-tech-wastes-nypd-police-time-and-money-audit-finds.

94 EFF.org, "Street Level Surveillance: Biometric Surveillance" (October 1, 2023), online: https://sls.eff.org/technologies/biometric-surveillance.

95 Andrew Guthrie Ferguson, "Surveillance and the Tyrant Test" in The Georgetown Law Journal (December 2021; Volume 110:205).

96 Alexandra Kelley, "DHS looks to AI to help solve child abuse cases" (Nextgov/FCW (October 2, 2023), online: https://www.nextgov.com/artificial-intelligence/2023/10/dhs-looks-ai-help-solve-child-abuse-cases/390866/.

97 Alexandra Kelley, "DHS looks to AI to help solve child abuse cases", *Nextgov/FCW* (October 2, 2023), online: https://www.nextgov.com/artificial-intelligence/2023/10/dhs-looks-ai-help-solve-child-abuse-cases/390866/.

98 Tobi Jegede, "Lifting the Veil on the Design of Predictive Tools in the Criminal Legal System", *ACLU* (November 22, 2023), online: https://www.aclu.org/news/racial-justice/lifting-the-veil-on-the-design-of-predictive-tools-in-the-criminal-legal-system.

99 Dell Cameron, "US Lawmakers Tell DOJ to Quit Blindly Funding 'Predictive' Police Tools", *Wired* (January 29, 2024), online: https://www.wired.com/story/doj-predictive-policing-lawmakers-demand/.

100 Emmanuel Camarillo, "Illinois' use of cameras that read license plates amounts to 'dragnet surveillance,' lawsuit alleges", *Chicago Sun Times* (June 2, 2024), online: https://chicago.suntimes.com/crime/2024/06/02/illinois-lawsuit-license-plate-readers-alpr-police-surveillance-police-pritzker-raoul-police-isp.

101 Emmanuel Camarillo, "Illinois' use of cameras that read license plates amounts to 'dragnet surveillance,' lawsuit alleges", *Chicago Sun Times* (June 2, 2024), online: https://chicago.suntimes.com/crime/2024/06/02/illinois-lawsuit-license-plate-readers-alpr-police-surveillance-police-pritzker-raoul-police-isp.

102 Dave Maass and Cooper Quintin, "New ALPR vulnerabilities Prove Mass Surveillance Is a Public Safety Threat", *Electronic Frontier Foundation* (June 18, 2024), online: https://www.eff.org/deeplinks/2024/06/new-alpr-vulnerabilities-prove-mass-surveillance-public-safety-threat.

103 Dave Maass and Cooper Quintin, "New ALPR vulnerabilities Prove Mass Surveillance Is a Public Safety Threat", *Electronic Frontier Foundation* (June 18, 2024), online: https://www.eff.org/deeplinks/2024/06/new-alpr-vulnerabilities-prove-mass-surveillance-public-safety-threat.

104 Dhruv Mehrotra and Jesse Marx, "The Age of the Drone Police Is Here", *Wired* (June 5, 2024), online: https://www.wired.com/story/the-age-of-the-drone-police-is-here/.

105 Dhruv Mehrotra and Jesse Marx, "The Age of the Drone Police Is Here", *Wired* (June 5, 2024), online: https://www.wired.com/story/the-age-of-the-drone-police-is-here/.

106 See *State of Washington vs. Joshua Puloka* (Superior Court of Washington for King County, No. 21-1-04851-2 KNT) (March 29 2024), online: https://www.nacdl.org/getattachment/89dee8b2-c47d-49c0-89d4-e187efe76551/Washington-v-Puloka-(No-21-1-04851-2-KNT)-(Sup-Ct-WA-2024).pdf?lang=en-US.

107 *State of Washington vs. Joshua Puloka* (Superior Court of Washington for King County, No. 21-1-04851-2 KNT) (March 29 2024), online: https://www.nacdl.org/getattachment/89dee8b2-c47d-49c0-89d4-e187efe76551/Washington-v-Puloka-(No-21-1-04851-2-KNT)-(Sup-Ct-WA-2024).pdf?lang=en-US.

108 *State of Washington vs. Joshua Puloka* (Superior Court of Washington for King County, No. 21-1-04851-2 KNT) (March 29 2024), online: https://www.nacdl.org/getattachment/89dee8b2-c47d-49c0-89d4-e187efe76551/Washington-v-Puloka-(No-21-1-04851-2-KNT)-(Sup-Ct-WA-2024).pdf?lang=en-US.

109 See KOMONews.com, "AI-assisted police reports not welcome in King County due to potential errors" (September 27 2024), online: https://komonews.com/amp/news/local/king-county-prosecutor-tells-police-not-to-use-ai-artificial-intelligence-for-official-reports-for-now-errors-concerns-law-enforcement-perjury-criminal-justice.

110 See Brian L Cox, "Glenview Dispatch Partners with AI Company to Train 911 Dispatchers," *Chicago Tribune* (10 July 2023), online: <https://www.chicagotribune.com/2023/07/10/glenview-dispatch-partners-with-ai-company-to-train-911-dispatchers/>.

111 See Amanda Hernández, "AI Bots are Helping 911 Dispatchers with Their Workload," *Stateline* (16 October 2023), online: <https://stateline.org/2023/10/16/ai-bots-are-helping-911-dispatchers-with-their-workload/>.

112 Libor Jany, "LAPD to use AI to analyze body cam videos for officers' language use", *Los Angeles Times* (August 22, 2023), online: https://www.latimes.com/california/story/2023-08-22/lapd-to-use-ai-to-analyze-body-cam-videos-for-officers-language-use.

113 Information and Privacy Commissioner of Ontario, *Facial Recognition and Mugshot Databases: Guidance for Police in Ontario* (January 2024), online: https://www.ipc.on.ca/wp-content/uploads/2024/01/2024-01-19-facial-recognition-and-mugshot-databases-guidance-for-police-in-ontario-e.pdf at 1.

114 An array of the types of FRT that may be deployed is surveyed in INCLO, *Eyes on the Watchers: Challenging the Rise of Police Facial Recognition* (February 2025), online: https://inclo.net/pillars/surveillance-and-digital-rights/principles-for-use-of-frt/introduction/ at p 16-18.

115 Ontario Human Rights Commission, "OHRC comments on IPC draft privacy guidance on facial recognition for police agencies" (November 19, 2021), online: https://www.ohrc.on.ca/en/news_centre/ohrc-comments-ipc-draft-privacy-guidance-facial-recognition-police-agencies.

116 Financial Times, "Met police use of facial recognition in London surges- Force used the technology 117 times from January to August, up from 32 between 2020 and 2023, total of 770,966 people scanned over 5 years" (October 2 2024), online: https://www.ft.com/content/c33322a7-eba7-4299-8172-4ce1d4e88908.

117 Washington Post, "Police seldom disclose use of facial recognition despite false arrests: police in 15 US states used facial recognition in 1,000+ cases since 2020 and routinely failed to tell defendants about their use of the software" (October 6 2024), online: https://www.washingtonpost.com/business/2024/10/06/police-facial-recognition-secret-false-arrest.

118 Washington Post, "Police seldom disclose use of facial recognition despite false arrests: police in 15 US states used facial recognition in 1,000+ cases since 2020 and routinely failed to tell defendants about their use of the software" (October 6 2024), online: https://www.washingtonpost.com/business/2024/10/06/police-facial-recognition-secret-false-arrest.

119 See: YahooTech, "The FTC is cracking down on a firm that claims its AI-powered face recognition tech has 'zero' bias" (December 3 2024), online: https://www.yahoo.com/tech/ftc-cracking-down-firm-claims-173206637.html.

120 YahooTech, "The FTC is cracking down on a firm that claims its AI-powered face recognition tech has 'zero' bias" (December 3 2024), online: https://www.yahoo.com/tech/ftc-cracking-down-firm-claims-173206637.html. See also NIST, *Face Recognition Technology Evaluation: Demographic Effects in Face Recognition* (updated December 20 2024), online: https://pages.nist.gov/frvt/html/frvt_demographics.html.

121 New York Times (Natasha Singer and Cade Metz), "Many Facial-Recognition Systems Are Biased, Says U.S. Study" (December 19, 2019), online: https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html.

122 New York Times (Natasha Singer and Cade Metz), "Many Facial-Recognition Systems Are Biased, Says U.S. Study" (December 19, 2019), online: https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html.

123 New York Times (Natasha Singer and Cade Metz), "Many Facial-Recognition Systems Are Biased, Says U.S. Study" (December 19, 2019), online: https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html.

124 National Institute of Standards and Technology (Patrick Grother, Mei Ngan, and Kayee Hanaoka), *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (December 2019), online: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf at 3.

125 National Institute of Standards and Technology (Patrick Grother, Mei Ngan, and Kayee Hanaoka), *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* (December 2019), online: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf at 2. For a summary see also: Scientific American (Sophie Bushwick), "How NIST Tested Facial Recognition Algorithms for Racial Basis" (December 27, 2019), online: https://www.scientificamerican.com/article/how-nist-tested-facial-recognition-algorithms-for-racial-bias/.

126 The Guardian (Johana Bhuiyan), "TechScape: 'Are you kidding, carjacking?' – The problem with facial recognition in policing" (August 15, 2023), online: https://www.theguardian.com/newsletters/2023/aug/15/techscape-facial-recognition-software-detroit-porcha-woodruff-black-people-ai; see also The Washington Post (Kelly Kasulis Cho), "Woman sues Detroit after facial recognition mistakes her for crime suspect" (August 7, 2023), online: https://www.washingtonpost.com/nation/2023/08/07/michigan-porcha-woodruff-arrest-facial-recognition/.

127 The Guardian (Johana Bhuiyan), "TechScape: 'Are you kidding, carjacking?' – The problem with facial recognition in policing" (August 15, 2023), online: https://www.theguardian.com/newsletters/2023/aug/15/techscape-facial-recognition-software-detroit-porcha-woodruff-black-people-ai.

128 WXYZ Detroit (Brett Kast), "DPD pushes to enact changes to photo lineups after facial recognition lawsuit" (August 9, 2023), online: https://www.wxyz.com/news/dpd-pushes-to-enact-changes-to-photo-lineups-after-facial-recognition-lawsuit.

129 American Civil Liberties Union (Nathan Freed Wessler), "Police Say a Simple Warning Will Prevent Face Recognition Wrongful Arrests. That's Just Not True." (April 30, 2024), online: https://www.aclu.org/news/privacy-technology/police-say-a-simple-warning-will-prevent-face-recognition-wrongful-arrests-thats-just-not-true.

130 The New York Times (Kashmir Hill and Ryan Mac), "Thousands of Dollars for Something I Didn't Do" (March 31, 2023), online: https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html.

131 The New York Times (Kashmir Hill and Ryan Mac), "Thousands of Dollars for Something I Didn't Do" (March 31, 2023), online: https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html.

132 The New York Times (Kashmir Hill and Ryan Mac), "Thousands of Dollars for Something I Didn't Do" (March 31, 2023), online: https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html.

133 The Washington Post (Drew Harwell), "Man sues Macy's, saying false facial recognition match led to jail assault" (January 22, 2024), online: https://www.msn.com/en-us/news/crime/man-sues-macy-s-saying-false-facial-recognition-match-led-to-jail-assault/ar-BB1h63ye. See also Murphy v. EssilorLuxottica Inc. (Civil Action 4:24-cv-00801 (S.D. Tex. Jul. 18, 2024), online: https://casetext.com/case/murphy-v-essilorluxottica-inc.

134 United States Government Accountability Office, Report to Congressional Requesters, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks* (June 2021), online: https://www.gao.gov/assets/gao-21-518.pdf at 17-18.

135 United States Government Accountability Office, Report to Congressional Requesters, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks* (June 2021), online: https://www.gao.gov/assets/gao-21-518.pdf at 18.

136 United States Government Accountability Office, Report to Congressional Requesters, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks* (June 2021), online: https://www.gao.gov/assets/gao-21-518.pdf at 18.

137 United States Government Accountability Office, Report to Congressional Requesters, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks* (June 2021), online: https://www.gao.gov/assets/gao-21-518.pdf at 19.

138 Amnesty International, *USA: Facial recognition technology reinforcing racist stop-and-frisk policing in New York – new research* (February 15, 2022), online: https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/.

139 Amnesty International, *USA: Facial recognition technology reinforcing racist stop-and-frisk policing in New York – new research* (February 15, 2022), online: https://www.amnesty.org/en/latest/news/2022/02/usa-facial-recognition-technology-reinforcing-racist-stop-and-frisk-policing-in-new-york-new-research/.

140 New York City Police Department, *NYPD Questions and Answers Facial Recognition* (2024), online: https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page.

141 United States Government Accountability Office, Report to Congressional Requesters, *Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks* (June 2021), online: https://www.gao.gov/assets/gao-21-518.pdf at second page of PDF.

142 Brookings Institution (Nicol Turner Lee and Caitlin Chin-Rothmann), *Police surveillance and facial recognition: Why data privacy is imperative for communities of color* (April 12, 2022), online: https://www.brookings.edu/research/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/. Additionally, the Policing Project at New York University maintains an excellent database of legislative activities related to FRT. See NYU School of Law, Policing Project, "The Growing World of Face Recognition Legislation" online: https://www.policingproject.org/facereclaws-intro.

143 LCO research updated July 24, 2024, on file with the LCO.

144 Reuters (Byron Kaye), "Australia's two largest states trial facial recognition software to police pandemic rules," (September 17, 2021), online: https://www.reuters.com/world/asia-pacific/australias-two-largest-states-trial-facial-recognition-software-police-pandemic-2021-09-16/.

145 Reuters (Byron Kaye), "Australia's two largest states trial facial recognition software to police pandemic rules," (September 17, 2021), online: https://www.reuters.com/world/asia-pacific/australias-two-largest-states-trial-facial-recognition-software-police-pandemic-2021-09-16/.

146 The Guardian (Christopher Knaus), "South Australia facial recognition trial: Covid app blasted by Fox and Breitbart criticised over lack of safeguards" (September 4, 2021), online: https://www.theguardian.com/australia-news/2021/sep/04/south-australia-facial-recognition-trial-covid-app-blasted-by-fox-and-breitbart-criticised-over-lack-of-safeguards.

147 The Guardian (Josh Taylor), "Calls to stop NSW police trial of national facial recognition system over lack of legal safeguards" (June 30, 2021), online: https://theguardian.com/australia-news/2021/jul/01/calls-to-stop-nsw-police-trial-of-national-facial-recognition-system-over-lack-of-legal-safeguards.

148 Office of the Privacy Commissioner of Canada, *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta* (February 2, 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/;

149 Office of the Privacy Commissioner of Canada, *Police use of Facial Recognition Technology in Canada and the Way Forward* (June 10 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/.

150 Information and Privacy Commissioner of Ontario, *Facial Recognition and Mugshot Databases: Guidance for Police in Ontario* (January 2024), online: https://www.ipc.on.ca/wp-content/uploads/2024/01/2024-01-19-facial-recognition-and-mugshot-databases-guidance-for-police-in-ontario-e.pdf.

151 Office of the Privacy Commissioner of Canada, *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta* (February 2, 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/.

152 Office of the Privacy Commissioner of Canada, *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta* (February 2, 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/.

153 Office of the Privacy Commissioner of Canada, *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta* (February 2, 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/.

154 See for example: CBC News, "Toronto Police admit using secretive facial recognition technology Clearview AI" (February 13 2020), online: https://www.cbc.ca/news/canada/toronto/toronto-police-clearview-ai-1.5462785; and Toronto Star, "Facial recognition app Clearview AI has been used far more widely in Canada than previously known" (February 27 2020), online: https://www.thestar.com/news/canada/2020/02/27/facial-recognition-app-clearview-ai-has-been-used-far-more-widely-in-canada-than-previously-known.html.

155 Office of the Privacy Commissioner of Canada, *Police use of Facial Recognition Technology in Canada and the Way Forward* (June 10 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/.

156 In their joint reports, the Privacy Commissioners clarify how "Information from sources such as social media or professional profiles, collected from public websites and then used for an unrelated purpose, does not fall under the "publicly available" exceptions" defined in in section 7(1)(d) of PIPEDA; sections 12(1)(e), 15(1)(e) and 18(1)(e) of PIPA BC; and sections 14(e), 17(e) and 20(j) of PIPA AB. As such, "collection from these sources would only be authorized with consent and only if the purposes are what a reasonable person would consider appropriate." See: Office of Privacy Commissioner of Canada, *Joint Investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta* (February 2, 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/ at paras 44-45; and Office of the Privacy Commissioner of Canada, *Police use of Facial Recognition Technology in Canada and the Way Forward* (June 10 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/ at para 29.

157 See: Office of Privacy Commissioner of Canada, *Joint Investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta* (February 2, 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/; and Office of the Privacy Commissioner of Canada, Police use of Facial Recognition Technology in Canada and the Way Forward (June 10 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/.

158 Toronto Star, "Facial recognition app Clearview AI has been used far more widely in Canada than previously known" (February 27, 2020), online: https://www.thestar.com/news/canada/facial-recognition-app-clearview-ai-has-been-used-far-more-widely-in-canada-than-previously/article_2de39e45-4bf1-5b56-9f07-ad117454569e.html.

159 Office of the Privacy Commissioner of Canada, *Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology* (June 10, 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/#toc1 at para 15.

160 Office of the Privacy Commissioner, *Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology* (June 10, 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/#toc1. The Privacy Commissioner later determined that 85% of the Clearview searches were not accounted for at all by the RCMP (at para 18).

161 See the following: CP24 (Chris Herhalt), "Toronto cops using facial recognition software since March 2018" (May 28, 2019), online: https://www.cp24.com/news/toronto-cops-using-facial-recognition-software-since-march-2018-1.4440343.; Vice News (Nathan Munn), "Police Forces in Canada Are Quietly Adopting Facial Recognition Tech" (June 23, 2020), online: https://www.vice.com/en/article/xg8wp4/police-forces-in-canada-are-quietly-adopting-facial-recognition-tech; Global News (Emily Mertz), "Edmonton police using facial recognition software to search 'mugshot database'" (February 1, 2022), online: https://globalnews.ca/news/8586358/edmonton-police-facial-recognition-mugshots-2022/. See also: Information and Privacy Commissioner of Ontario, *Facial Recognition and Mugshot Databases: Guidance for Police in Ontario* (January 2024), online: https://www.ipc.on.ca/wp-content/uploads/2024/01/2024-01-19-facial-recognition-and-mugshot-databases-guidance-for-police-in-ontario-e.pdf.

162 *Identification of Criminals Act* (RSC, 1985, c. I-1), online: https://laws-lois.justice.gc.ca/eng/acts/I-1/.

163 Information and Privacy Commissioner of Ontario, *Facial Recognition and Mugshot Databases: Guidance for Police in Ontario* (January 2024), online: https://www.ipc.on.ca/wp-content/uploads/2024/01/2024-01-19-facial-recognition-and-mugshot-databases-guidance-for-police-in-ontario-e.pdf at 5, citing *R. v. Beare; R. v. Higgins*, [1988] 2 S.C.R. 387, *R. v. Doré*, [2002] O.J. No. 2845 (C.A.), *Lin v. Toronto Police Services Board*, [2004] O.J. No. 170 (S.C.), *R. v. Strickland*, 2017 BCPC 1, *R. v. Strickland*, 2017 BCPC 211, *R. v M.O.*, 2017 ONSC 1213, and *R. v. Fogah-Pierre*, [2023] O.J. No. 1999 (S.C.). The Privacy Commissioner's report suggests the implementation of privacy impact assessments to address privacy-related concerns arising from the use of mugshot databases for FRT purposes. A privacy impact assessment is a risk management tool to assess the "potential privacy risks of a program or activity" (at 9-10).

164 See R. v Collins (1 S.C.R. 265 1987 SCC 11).

165 Information and Privacy Commissioner of Ontario, "Facial Recognition and Mugshot Databases: Guidance for Police in Ontario" (January 2024), online: https://www.ipc.on.ca/wp-content/uploads/2024/01/2024-01-19-facial-recognition-and-mugshot-databases-guidance-for-police-in-ontario-e.pdf, at 9, 14, 15 and 18.

166 Information and Privacy Commissioner of Ontario, *Facial Recognition and Mugshot Databases: Guidance for Police in Ontario* (January 2024), online: https://www.ipc.on.ca/wp-content/uploads/2024/01/2024-01-19-facial-recognition-and-mugshot-databases-guidance-for-police-in-ontario-e.pdf at 12.

167 Ontario Human Rights Commission, *A Disparate Impact: Second interim report on the inquiry into racial profiling and racial discrimination of Black persons by the Toronto Police Service* (August 2020; corrected and revised January 2023), online: https://www.ohrc.on.ca/sites/default/files/A%20Disparate%20Impact%20-%20TPS%20inquiry%20%28updated%20January%202023%29.pdf.

168 *Ali v. Canada (Public Safety and Emergency Preparedness)* (2024 FC 1085), online: https://canlii.ca/t/k5qq7.

169 *Ali v. Canada (Public Safety and Emergency Preparedness)* (2024 FC 1085), online: https://canlii.ca/t/k5qq7 at 31, 33. See also Toronto Star, "Did Canada use facial recognition software to strip this refugee of his status? A court wants better answers" (July 18 2024), online: https://www.thestar.com/news/canada/did-canada-use-facial-recognition-software-to-strip-this-refugee-of-his-status-a-court/article_01495a3c-437c-11ef-8138-fb0dd8f7aafe.html.

170 Toronto Star, "Did Canada use facial recognition software to strip this refugee of his status? A court wants better answers" (July 18 2024), online: https://www.thestar.com/news/canada/did-canada-use-facial-recognition-software-to-strip-this-refugee-of-his-status-a-court/article_01495a3c-437c-11ef-8138-fb0dd8f7aafe.html.

171 Choice (Jarni Blakkarly), "Kmart, Bunnings and The Good Guys using facial recognition technology in stores" (July 12, 2022), online: https://www.choice.com.au/consumers-and-data/data-collection-and-use/how-your-data-is-used/articles/kmart-bunnings-and-the-good-guys-using-facial-recognition-technology-in-store.

172 CNET (Ben Fox Rubin), "Amazon's Ring takes heat for considering facial recognition for its video doorbells" (December 14, 2018), online: https://cnet.com/home/smart-home/amazons-ring-takes-heat-for-considering-facial-recognition-for-its-video-doorbells.

173 CNET (Ben Fox Rubin), "Amazon's Ring takes heat for considering facial recognition for its video doorbells" (December 14, 2018), online: https://www.cnet.com/home/smart-home/amazons-ring-takes-heat-for-considering-facial-recognition-for-its-video-doorbells/.

174 Office of the Privacy Commissioner of Canada, "Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia" (October 28 2020), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/.

175 Office of the Privacy Commissioner of Canada, "Joint investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia" (October 28 2020), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-004/.

176 Information and Privacy Commissioner of Ontario, *Facial Recognition and Mugshot Databases: Guidance for Police in Ontario* (January 2024), online: https://www.ipc.on.ca/wp-content/uploads/2024/01/2024-01-19-facial-recognition-and-mugshot-databases-guidance-for-police-in-ontario-e.pdf at 1.

177 See NYU School of Law, Policing Project, "General FRT / Surveillance Regulation" online: https://www.policingproject.org/general-regulations.

178 Research on file with the LCO.

179 StateScoop.com, "Maryland lawmakers approve 'strongest' facial recognition rules for law enforcement yet" (April 11, 2024), online: https://statescoop.com/maryland-facial-recognition-strongest-legislation/. The legislation was enacted as Senate Bill 182, *Criminal Procedure - Facial Recognition Technology - Requirements, Procedures, and Prohibitions* (cross-filed with House Bill 0338) signed May 5, 2024 and in force October 1, 2024, online: https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0182?ys=2024RS.

180 StateScoop.com, "Maryland lawmakers approve 'strongest' facial recognition rules for law enforcement yet" (April 11, 2024), online: https://statescoop.com/maryland-facial-recognition-strongest-legislation/.

181 Official Journal of the European Union, *Artificial Intelligence Act* ((Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)), online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689 at Chapter II, Art. 5, online: https://artificialintelligenceact.eu/article/5/.

182 See EU AIA, "Article 5: Prohibited AI Practices", online: https://artificialintelligenceact.eu/article/5/.

183 EU, "High-Level Summary of the AI Act" (February 24, 2024), online: https://artificialintelligenceact.eu/high-level-summary/.

184 Official Journal of the European Union, *Artificial Intelligence Act* ((Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)), online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689 at Chapter II, Art. 5, online: https://artificialintelligenceact.eu/article/5/.

185 Official Journal of the European Union, *Artificial Intelligence Act* ((Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024, laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)), online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689 at Chapter II, Art. 5, at paras 2-6, online: https://artificialintelligenceact.eu/article/5/.

186 Parliament of Canada, BillC-27, An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts (first reading June 16, 2022), online: https://www.parl.ca/legisinfo/en/bill/44-1/c-27.

187 See AIDA at section 5, 7-9.

188 See: Letter from François-Philippe Champagne (Minister of Innovation, Science and Economic Development Canada) to the House of Commons' Standing Committee on Industry and Technology (November 28, 2023), online: https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12751351/12751351/MinisterOfInnovationScienceAndIndustry-2023-11-28-Combined-e.pdf at 38.

189 Government of Canada, "The Artificial Intelligence and Data Act (AIDA) – Companion document" (dated March 13, 2023), online: https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document#s1.

190 Government of Canada, "The Artificial Intelligence and Data Act (AIDA) – Companion document" (dated March 13, 2023), online: https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document#s1.

191 Canada, Directive on Automated Decision-Making (updated April 25, 2023), online: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592 .

192 Legislative Assembly of Ontario, Bill 194, *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024* (introduced on first reading May 13, 2024), online: https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194.

193 See: Law Commission of Ontario, "Bill 194 Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024: Law Commission of Ontario Submission" (June 2024), online: https://www.lco-cdo.org/wp-content/uploads/2024/06/LCO-Submission-to-Government-of-Ontario-Bill-194-Consultations-June-2024.pdf.

194 Law Commission of Ontario, "Bill 194 Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024: Law Commission of Ontario Submission" (June 2024), online: https://www.lco-cdo.org/wp-content/uploads/2024/06/LCO-Submission-to-Government-of-Ontario-Bill-194-Consultations-June-2024.pdf at 2-3.

195 Office of the Privacy Commissioner of Canada, "Clearview AI ordered to comply with recommendations to stop collecting, sharing images" (December 14, 2021), online: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_211214/.

196 Office of the Privacy Commissioner of Canada, "Clearview AI ordered to comply with recommendations to stop collecting, sharing images" (December 14, 2021), online: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/an_211214/.

197 INCLO, *Eyes on the Watchers: Challenging the Rise of Police Facial Recognition* (February 2025), online: https://inclo.net/pillars/surveillance-and-digital-rights/principles-for-use-of-frt/introduction/ at p 16-18.

198 INCLO, *Eyes on the Watchers: Challenging the Rise of Police Facial Recognition* (February 2025), online: https://inclo.net/pillars/surveillance-and-digital-rights/principles-for-use-of-frt/introduction/ at p 5.

199 The Citizen Lab, *To Surveil and Protect: A Human Rights Analysis of Algorithmic Policing in Canada* (2020), online: https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf at 41.

200 The Citizen Lab, *To Surveil and Protect: A Human Rights Analysis of Algorithmic Policing in Canada* (2020), online: https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf at 45-46.

201 Andrew Guthrie Ferguson, "Predictive Policing Theory" published as Chapter 24 in Tamara Rice Lave and Eric J. Miller (eds.), *The Cambridge Handbook of Policing in the United States* (Cambridge Univ. Press (2019)), online: https://ssrn.com/abstract=3516382 at 491.

202 Andrew Guthrie Ferguson, "Predictive Policing Theory" published as Chapter 24 in Tamara Rice Lave and Eric J. Miller (eds.), *The Cambridge Handbook of Policing in the United States* (Cambridge Univ. Press (2019)), online: https://ssrn.com/abstract=3516382 at 491.

203 Andrew Guthrie Ferguson, "Predictive Policing Theory" published as Chapter 24 in Tamara Rice Lave and Eric J. Miller (eds.), *The Cambridge Handbook of Policing in the United States* (Cambridge Univ. Press (2019)), online: https://ssrn.com/abstract=3516382 at 491.

204 Andrew Guthrie Ferguson, "Predictive Policing Theory" published as Chapter 24 in Tamara Rice Lave and Eric J. Miller (eds.), *The Cambridge Handbook of Policing in the United States* (Cambridge Univ. Press (2019)), online: https://ssrn.com/abstract=3516382 at 492.

205 Andrew Guthrie Ferguson, "Predictive Policing Theory" published as Chapter 24 in Tamara Rice Lave and Eric J. Miller (eds.), *The Cambridge Handbook of Policing in the United States* (Cambridge Univ. Press (2019)), online: https://ssrn.com/abstract=3516382 at 492.

206 Andrew Guthrie Ferguson, "Predictive Policing Theory" published as Chapter 24 in Tamara Rice Lave and Eric J. Miller (eds.), *The Cambridge Handbook of Policing in the United States* (Cambridge Univ. Press (2019)), online: https://ssrn.com/abstract=3516382 at 492-493.

207 Wired.com, "US Lawmakers Tell DOJ to Quit Blindly Funding 'Predictive' Police Tools: Members of Congress say the DOJ is funding the use of AI tools that further discriminatory policing practices" (January 29 2024), online: https://www.wired.com/story/doj-predictive-policing-lawmakers-demand/, citing The Markup, "Predictive Policing Software Terrible At Predicting Crimes" (October 2 2023), online: https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes.

208 NASEM, "Law Enforcement Use of Predictive Policing Approaches Proceedings of a Workshop—in Brief" (2024), online: https://doi.org/10.17226/28037.

209 NASEM, "Law Enforcement Use of Predictive Policing Approaches Proceedings of a Workshop—in Brief" (2024), online: https://doi.org/10.17226/28037.

210 Andrew Guthrie Ferguson, "Predictive Policing Theory" published as Chapter 24 in Tamara Rice Lave and Eric J. Miller (eds.), *The Cambridge Handbook of Policing in the United States* (Cambridge Univ. Press (2019)), online: https://ssrn.com/abstract=3516382 at 492, citing David Robinson and Logan Koepke, "Stuck in a Pattern: Early Evidence on "Predictive Policing" and Civil Rights" (Upturn 17 (2016)).

211 National Institute of Justice (Craig Uchida), "A National Discussion on Predictive Policing: Defining Our Terms and Mapping Successful Implementation Strategies" (November 18-20, 2009), online: https://www.ncjrs.gov/PDFFILES1/NIJ/GRANTS/230404.PDF at 5.

212 The Verge (Matt Stroud), "Chicago's Predictive Policing Tool Just Failed a Major Test" (August 19, 2016), online: https://www.theverge.com/2016/8/19/12552384/chicago-heat-list-tool-failed-rand-test.

213 The Verge (Matt Stroud), "Chicago's Predictive Policing Tool Just Failed a Major Test" (August 19, 2016), online: https://www.theverge.com/2016/8/19/12552384/chicago-heat-list-tool-failed-rand-test.

214 The Verge (Ali Winston), "Palantir Has Secretly Been Using New Orleans to Test its Predictive Policing Technology" (February 27, 2018), online: https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd.

215 The Verge (Ali Winston), "New Orleans ends its Palantir predictive policing program" (March 15, 2018), online: https://www.theverge.com/2018/3/15/17126174/new-orleans-palantir-predictive-policing-program-end.

216 The Guardian (Johana Bhuiyan), "TechScape: Can AI Really Predict Crime?" (December 22, 2021), online: https://www.theguardian.com/technology/2021/dec/22/techscape-lapd-operation-laser. The Guardian (Johana Bhuiyan), "TechScape: Can AI Really Predict Crime?" (December 22, 2021), online: https://www.theguardian.com/technology/2021/dec/22/techscape-lapd-operation-laser.

217 The Guardian (Johana Bhuiyan), "TechScape: Can AI Really Predict Crime?" (December 22, 2021), online: https://www.theguardian.com/technology/2021/dec/22/techscape-lapd-operation-laser.

218 Complaint in *Meta Platforms, Inc v Voyager Labs Ltd* (December 1, 2023), US District Court for the Northern District of California (San Francisco/Oakland Division), Case No 3:23-CV-00154, at para 11, online: https://storage.courtlistener.com/recap/gov.uscourts.cand.407115/gov.uscourts.cand.407115.1.0.pdf

219 The Guardian (Johana Bhuiyan), "NYPD spent millions to contract with firm banned by Meta for fake profiles" (September 8, 2023), online: https://www.theguardian.com/us-news/2023/sep/08/new-york-police-tracking-voyager-labs-meta-contract.

220 The Guardian (Johana Bhuiyan), "NYPD spent millions to contract with firm banned by Meta for fake profiles" (September 8, 2023), online: https://www.theguardian.com/us-news/2023/sep/08/new-york-police-tracking-voyager-labs-meta-contract.

221 Letter from Meta's VP and Deputy General Counsel of Civil Rights (November 11, 2021), online: https://about.fb.com/wp-content/uploads/2021/11/LAPD-Letter.pdf.

222 Letter from Meta's VP and Deputy General Counsel of Civil Rights (November 11, 2021), online: https://about.fb.com/wp-content/uploads/2021/11/LAPD-Letter.pdf at 1.

223 Letter from Meta's VP and Deputy General Counsel of Civil Rights (November 11, 2021), online: https://about.fb.com/wp-content/uploads/2021/11/LAPD-Letter.pdf at 2.

224 Complaint in *Meta Platforms, Inc v Voyager Labs Ltd* (December 1, 2023), US District Court for the Northern District of California (San Francisco/Oakland Division), Case No 3:23-CV-00154, online: https://storage.courtlistener.com/recap/gov.uscourts.cand.407115/gov.uscourts.cand.407115.1.0.pdf at 18 (section H).

225 In its decision dated May 5, 2024, the court held against a motion by Voyager Labs for dismissal. See Order Denying Motion to Dismiss: *Meta Platforms, Inc v Voyager Labs Ltd* (May 5, 2024), US District Court for the Northern District of California (San Francisco/Oakland Division), Case No 3:23-CV-00154 , online: https://storage.courtlistener.com/recap/gov.uscourts.cand.407115/gov.uscourts.cand.407115.89.0.pdf.

226 Wired.com, "US Lawmakers Tell DOJ to Quit Blindly Funding 'Predictive' Police Tools: Members of Congress say the DOJ is funding the use of AI tools that further discriminatory policing practices" (January 29 2024), online: https://www.wired.com/story/doj-predictive-policing-lawmakers-demand/.

227 Wired.com, "US Lawmakers Tell DOJ to Quit Blindly Funding 'Predictive' Police Tools: Members of Congress say the DOJ is funding the use of AI tools that further discriminatory policing practices" (January 29 2024), online: https://www.wired.com/story/doj-predictive-policing-lawmakers-demand/.

228 Wired.com, "US Lawmakers Tell DOJ to Quit Blindly Funding 'Predictive' Police Tools: Members of Congress say the DOJ is funding the use of AI tools that further discriminatory policing practices" (January 29 2024), online: https://www.wired.com/story/doj-predictive-policing-lawmakers-demand/.

229 Wired.com, "US Lawmakers Tell DOJ to Quit Blindly Funding 'Predictive' Police Tools: Members of Congress say the DOJ is funding the use of AI tools that further discriminatory policing practices" (January 29 2024), online: https://www.wired.com/story/doj-predictive-policing-lawmakers-demand/.

230 The Citizen Lab (Kate Robertson et al), *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada* (2020), online: https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf at 42.

231 The Citizen Lab (Kate Robertson et al), *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada* (2020), online: https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf at 42.

232 The Citizen Lab (Kate Robertson et al), *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada* (2020), online: https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf at 43.

233 Palantir Platforms (Gotham): https://www.palantir.com/platforms/.

234 The Logic (David Reevely and Murad Hemmadi), "Ontario Provincial Police use controversial data-mining platform Palantir for crime analysis" (October 20, 2022), online: https://thelogic.co/news/exclusive/ontario-provincial-police-use-controversial-data-mining-platform-palantir-for-crime-analysis/.

235 Livewire Calgary (Aryn Toombs), "Calgary Police Service looking to public to govern use of policing technology" (April 28, 2022), online: https://livewirecalgary.com/2022/04/28/calgary-police-service-public-policing-tech-data/.

236 Ontario Human Rights Commission, *Policy on Eliminating Racial Profiling in Law Enforcement* (OHRC, online: https://www.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement at s. 4.2.6.1.

237 Ontario Human Rights Commission, *Policy on Eliminating Racial Profiling in Law Enforcement* (OHRC, online: https://www.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement at s. 4.2.6.1.

238 NAACP, "Artificial Intelligence in Predictive Policing Issue Brief" (2024), online: https://naacp.org/resources/artificial-intelligence-predictive-policing-issue-brief#:~:text=Bias%20and%20Discrimination%3A%20AI%20models,policing%20and%20resources%20are%20made.

239 See Duncan Purves, "Fairness in Algorithmic Policing" (2022 Journal of the American Philosophical Association 8(4): 741-761), online: https://www.cambridge.org/core/journals/journal-of-the-american-philosophical-association/article/fairness-in-algorithmic-policing/A93BD2FBA25DEDBC6620B25D1C9A8A26. See also: Will Douglas Heaven, "Predictive policing algorithms are racist. They need to be dismantled." (MIT Technology Review July 17, 2020), online: https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/; JSTOR Daily (Hope Reese), "What Happens When Police Use AI to Predict and Prevent Crime?" (February 23, 2022), online: https://daily.jstor.org/what-happens-when-police-use-ai-to-predict-and-prevent-crime/; Yale Law School's Media Freedom & Information Access Clinic, "Algorithms in Policing: An Investigative Packet" (March 2022), online: https://law.yale.edu/sites/default/files/area/center/mfia/document/infopack.pdf.

240 Paul W Grimm et al, "Artificial Intelligence as Evidence" in Northwestern Journal of Technology and Intellectual Property (December 2021; Volume 19, Issue 1), online: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1349&context=njtip at 37. See also: VentureBeat (Kyle Wiggers), "NIST Benchmarks Show Facial Recognition Technology Still Struggles to Identify Black Faces" (September 9, 2020), online: https://venturebeat.com/2020/09/09/nist-benchmarksshow-facial-recognition-technology-still-struggles-to-identify-black-faces; MIT News (Larry Hardesty), "Study Finds Gender and Skin-Type Bias in Commercial Artificial-Intelligence Systems" (February 11, 2018), online: https://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212; New York Times (Steve Lohr), "Facial Recognition is Accurate, if You're a White Guy" (February 9, 2018), online: https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

241 NAACP, "Artificial Intelligence in Predictive Policing Issue Brief" (2024), online: https://naacp.org/resources/artificial-intelligence-predictive-policing-issue-brief.

242 Paul W Grimm et al, "Artificial Intelligence as Evidence" in Northwestern Journal of Technology and Intellectual Property (December 2021; Volume 19, Issue 1), online: https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1349&context=njtip at 65-71.

243 Ontario Human Rights Commission, Policy on Eliminating Racial Profiling in Law Enforcement (OHRC, online: https://www.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement at s. 4.2.6.2. See also: Monika Zalnieriute and Tatiana Cutts, "How AI and New Technologies Reinforce Systemic Racism" (Submission to the United Nations Office of the High Commissioner for Human Rights) (October 3, 2022), online: https://www.ohchr.org/sites/default/files/documents/hrbodies/hrcouncil/advisorycommittee/study-advancement-racial-justice/2022-10-26/HRC-Adv-comm-Racial-Justice-zalnieriute-cutts.pdf.

244 Ontario Human Rights Commission, Policy on Eliminating Racial Profiling in Law Enforcement (OHRC, online: https://www.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement at s. 4.2.6.2.

245 NAACP, "Artificial Intelligence in Predictive Policing Issue Brief" (2024), online: https://naacp.org/resources/artificial-intelligence-predictive-policing-issue-brief#:~:text=Bias%20and%20Discrimination%3A%20AI%20models,policing%20and%20resources%20are%20made.

246 See Abdirahman Osman Hashi et al, "Deep Learning Models for Crime Intention Detection Using Object Detection" in Intl J Advanced Computer Science and Applications (2023; Volume 14, No 4), online: https://thesai.org/Downloads/Volume14No4/Paper_34-Deep_Learning_Models_for_Crime_Intention_Detection.pdf 300; Vishva Payghode et al, "Object Detection and Activity Recognition in Video Surveillance Using Neural Networks" International Journal of Web Information Systems (April 20, 2023; Volume 19, No 3/4) at 123.

247 Helton Agbewonou Yawovi, "Who Was Wrong? An Object Detection Based Responsibility Assessment System for Crossroad Vehicle Collisions" in AI (2022; 3), online: https://www.mdpi.com/2673-2688/3/4/51 at 844.

248 See Forensic Technology Centre of Excellence, "What FSSP Leaders Should Know About Artificial Intelligence and its Application to Forensic Science" (Research Triangle Park, NC: RTI International, December 2023), online: https://forensiccoe.org/private/65cfa81c601c4 at 5-7.

249 See Waterloo Regional Police Service, "Automated License Plate Recognition," online: https://www.wrps.on.ca/en/staying-safe/automated-license-plate-recognition.aspx; Information and Privacy Commissioner of Ontario, *Guidance on the Use of Automated Licence Plate Recognition Systems by Police Services* (July 2017), online: https://www.ipc.on.ca/sites/default/files/legacy/2016/09/alpr_systems.pdf at 2.

250 CTV News (Sean Davidson), "What Ontario drivers need to know about major rollout of licence plate scanning technology" (February 14, 2023), online: https://toronto.ctvnews.ca/what-ontario-drivers-need-to-know-about-major-rollout-of-licence-plate-scanning-technology-1.6273310.

251 CTV News (Sean Davidson), "What Ontario drivers need to know about major rollout of licence plate scanning technology" (February 14, 2023), online: https://toronto.ctvnews.ca/what-ontario-drivers-need-to-know-about-major-rollout-of-licence-plate-scanning-technology-1.6273310.

252 See John A Shjarback, "Examining Police Officers' Perceptions of Automated License Plate Readers Before Technology Expansion" in Criminal Justice Policy Review (2024; Volume 35, Issue 1) at 14.

253 See Chicago Sun Times (Emmanuel Camarillo), "Illinois' use of cameras that read license plates amounts to 'dragnet surveillance,' lawsuit alleges" (June 2, 2024), online: https://chicago.suntimes.com/crime/2024/06/02/illinois-lawsuit-license-plate-readers-alpr-police-surveillance-police-pritzker-raoul-police-isp.

254 Electronic Frontier Foundation (Dave Maass), "Data Driven 2: California Dragnet—New Data Set Shows Scale of Vehicle Surveillance in the Golden State" (April 22, 2021), online: https://www.eff.org/deeplinks/2021/04/data-driven-2-california-dragnet-new-dataset-shows-scale-vehicle-surveillance.

255 See The Toronto Star (Kate Allen), "Cadillac Fairview broke privacy laws by using facial recognition technology at malls, investigators conclude" (October 29, 2020), online: https://www.thestar.com/news/gta/cadillac-fairview-broke-privacy-laws-by-using-facial-recognition-technology-at-malls-investigators-conclude/article_8084f253-728a-5494-a1b6-9bd75e9e47d3.html; CNN (Brian Fung), "Texas man sues Macy's and Sunglass Hut parent over wrongful arrest linked to facial recognition" (January 23, 2024), online: https://edition.cnn.com/2024/01/23/tech/texas-man-sues-macys-sunglass-hut-facial-recognition/index.html; Politico (Alfred Ng), "The privacy loophole in your doorbell" (March 7, 2023), online: https://www.politico.com/news/2023/03/07/privacy-loophole-ring-doorbell-00084979; Forbes (Thomas Brewster), "FedEx's Secretive Police Force Is Helping Cops Build An AI Car Surveillance Network" (June 19, 2024), online: https://www.forbes.com/sites/thomasbrewster/2024/06/19/fedex-police-help-cops-build-an-ai-car-surveillance-network/.

256 "Criminal Procedure- Fourth Amendment- Massachusetts Supreme Judicial Court Holds That Use of Automated License Plate Readers May Constitute a Search- *Commonwealth v. McCarthy*, 142 N.E.3d 1090 (Mass. 2020)" in Harvard Law Review (June 2021; Volume 134, Issue 8), online: https://harvardlawreview.org/print/vol-134/commonwealth-v-mccarthy/ at 2891-94.

257 "Criminal Procedure- Fourth Amendment- Massachusetts Supreme Judicial Court Holds That Use of Automated License Plate Readers May Constitute a Search- *Commonwealth v. McCarthy*, 142 N.E.3d 1090 (Mass. 2020)" in Harvard Law Review (June 2021; Volume 134, Issue 8), online: https://harvardlawreview.org/print/vol-134/commonwealth-v-mccarthy/ at 2893.

258 See Nicole K McConlogue, "Discrimination on Wheels: How Big Data Uses License Plate Surveillance to Put the Brakes on Disadvantaged Drivers" in Stanford Journal of Civil Rights and Civil Liberties (2022; Volume 18), online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839726 at 285. Agencies contracting with Motorola Solutions, the largest provider of ALPR services in the US, enforce their own policies regarding which other organizations their data is shared with, meaning police data should not be shared with private actors. However, there is some evidence police-captured footage has been shared with private actors through other public-private surveillance systems; see Forbes (Thomas Brewster), "FedEx's Secretive Police Force Is Helping Cops Build An AI Car Surveillance Network" (June 19, 2024), online: https://www.forbes.com/sites/thomasbrewster/2024/06/19/fedex-police-help-cops-build-an-ai-car-surveillance-network/.

259 Andrew Guthrie Ferguson, "Persistent Surveillance" (Washington College of Law Research Paper No. 2022-10) (October 30 2022), online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4071189.

260 *Commonwealth v. McCarthy* (142 N.E.3d 1090 (Mass. 2020)), online: https://law.justia.com/cases/massachusetts/supreme-court/2020/sjc-12750.html at 2. See also: "Criminal Procedure- Fourth Amendment- Massachusetts Supreme Judicial Court Holds That Use of Automated License Plate Readers May Constitute a Search- *Commonwealth v. McCarthy*, 142 N.E.3d 1090 (Mass. 2020)" in Harvard Law Review (June 2021; Volume 134, Issue 8), online: https://harvardlawreview.org/print/vol-134/commonwealth-v-mccarthy/ at 2887.

261 "Criminal Procedure- Fourth Amendment- Massachusetts Supreme Judicial Court Holds That Use of Automated License Plate Readers May Constitute a Search- *Commonwealth v. McCarthy*, 142 N.E.3d 1090 (Mass. 2020)" in Harvard Law Review (June 2021; Volume 134, Issue 8), online: https://harvardlawreview.org/print/vol-134/commonwealth-v-mccarthy/ at 2890.

262 "Criminal Procedure- Fourth Amendment- Massachusetts Supreme Judicial Court Holds That Use of Automated License Plate Readers May Constitute a Search- *Commonwealth v. McCarthy*, 142 N.E.3d 1090 (Mass. 2020)" in Harvard Law Review (June 2021; Volume 134, Issue 8), online: https://harvardlawreview.org/print/vol-134/commonwealth-v-mccarthy/ at 2889.

263 See Chicago Sun Times (Emmanuel Camarillo), "Illinois' use of cameras that read license plates amounts to 'dragnet surveillance,' lawsuit alleges" (June 2, 2024), online: https://chicago.suntimes.com/crime/2024/06/02/illinois-lawsuit-license-plate-readers-alpr-police-surveillance-police-pritzker-raoul-police-isp.

264 See Chicago Sun Times (Emmanuel Camarillo), "Illinois' use of cameras that read license plates amounts to 'dragnet surveillance,' lawsuit alleges" (June 2, 2024), online: https://chicago.suntimes.com/crime/2024/06/02/illinois-lawsuit-license-plate-readers-alpr-police-surveillance-police-pritzker-raoul-police-isp.

265 See Chicago Sun Times (Emmanuel Camarillo), "Illinois' use of cameras that read license plates amounts to 'dragnet surveillance,' lawsuit alleges" (June 2, 2024), online: https://chicago.suntimes.com/crime/2024/06/02/illinois-lawsuit-license-plate-readers-alpr-police-surveillance-police-pritzker-raoul-police-isp.

266 See Electronic Frontier Foundation (Dave Maass and Cooper Quintin), "New ALPR vulnerabilities Prove Mass Surveillance Is a Public Safety Threat" (June 18, 2024), online: https://www.eff.org/deeplinks/2024/06/new-alpr-vulnerabilities-prove-mass-surveillance-public-safety-threat.

267 Electronic Frontier Foundation (Dave Maass and Cooper Quintin), "New ALPR vulnerabilities Prove Mass Surveillance Is a Public Safety Threat" (June 18, 2024), online: https://www.eff.org/deeplinks/2024/06/new-alpr-vulnerabilities-prove-mass-surveillance-public-safety-threat.

268 *R. v. Bykovets*, 2024 SCC 6 [*Bykovets*].

269 *Bykovets* thus expanded the protections mandated by *R. v. Spencer*, 2014 SCC 43, which required police to obtain warrants for the search and seizure of subscriber information (name, address, etc.) associated with an IP address, but not the IP address alone.

270 In the US, the "third party doctrine" dictates that there is no expectation of privacy for any information possessed by third parties. However, Canadian privacy jurisprudence does not recognize this doctrine. See *Bykovets* at para 47.

271 *Bykovets* at para 65.

272 *Bykovets* at para 9.

273 *Bykovets* at para 65.

274 See *Bykovets* at paras 61–66.

275 *Bykovets* at para 21.

276 Wired (Dhruv Mehrotra and Joey Scott), "Here Are the Secret Locations of ShotSpotter Gunfire Sensors" (February 22, 2024), online: https://www.wired.com/story/shotspotter-secret-sensor-locations-leak/.

277 Edward B Kang and Simogne Hudson, "Audible Crime Scenes: ShotSpotter as Diagnostic, Policing, and Space-making Infrastructure" in Science, Technology, and Human Values (May 2024; Volume 49, Issue 3) at 651. See also Harvey Gee, "Bang!": ShotSpotter Gunshot Detection Technology, Predictive Policing, and Measuring Terry's Reach" in University of Michigan Journal of Law Reform (2022; Volume 55), online: https://repository.law.umich.edu/mjlr/vol55/iss4/3/ at 771.

278 Wired (Dhruv Mehrotra and Joey Scott), "Here Are the Secret Locations of ShotSpotter Gunfire Sensors" (February 22, 2024), online: https://www.wired.com/story/shotspotter-secret-sensor-locations-leak/; Harvey Gee, "Bang!": ShotSpotter Gunshot Detection Technology, Predictive Policing, and Measuring Terry's Reach" in University of Michigan Journal of Law Reform (2022; Volume 55), online: https://repository.law.umich.edu/mjlr/vol55/iss4/3/ at 776.

279 Edward B Kang and Simogne Hudson, "Audible Crime Scenes: ShotSpotter as Diagnostic, Policing, and Space-making Infrastructure" in Science, Technology, and Human Values (May 2024; Volume 49, Issue 3) at 652. See also Harvey Gee, "Bang!": ShotSpotter Gunshot Detection Technology, Predictive Policing, and Measuring Terry's Reach" in University of Michigan Journal of Law Reform (2022; Volume 55), online: https://repository.law.umich.edu/mjlr/vol55/iss4/3/ at 774–75; Wired (Dhruv Mehrotra and Joey Scott), "Here Are the Secret Locations of ShotSpotter Gunfire Sensors" (February 22, 2024), online: https://www.wired.com/story/shotspotter-secret-sensor-locations-leak/.

280 Bloomberg (Fola Akinnibi), "NYC Surveillance Tech on Shootings Gives False Alarms 87% of Time, Audit Finds" (June 20, 2024), online: https://www.bloomberg.com/news/articles/2024-06-20/nyc-shotspotter-tech-wastes-nypd-police-time-and-money-audit-finds.

281 Bloomberg (Fola Akinnibi), "NYC Surveillance Tech on Shootings Gives False Alarms 87% of Time, Audit Finds" (June 20, 2024), online: https://www.bloomberg.com/news/articles/2024-06-20/nyc-shotspotter-tech-wastes-nypd-police-time-and-money-audit-finds.

282 Mitchell L Doucette et al, "Impact of ShotSpotter Technology on Firearm Homicides and Arrests Among Large Metropolitan Counties: a Longitudinal Analysis, 1999–2016" in Journal of Urban Health (2021; Volume 98) at 616–617.

283 Wired (Dhruv Mehrotra and Joey Scott), "Here Are the Secret Locations of ShotSpotter Gunfire Sensors" (February 22, 2024), online: https://www.wired.com/story/shotspotter-secret-sensor-locations-leak/; Harvey Gee, "Bang!": ShotSpotter Gunshot Detection Technology, Predictive Policing, and Measuring Terry's Reach" in University of Michigan Journal of Law Reform (2022; Volume 55), online: https://repository.law.umich.edu/mjlr/vol55/iss4/3/ at 776.

284 Wired (Dhruv Mehrotra and Joey Scott), "Here Are the Secret Locations of ShotSpotter Gunfire Sensors" (February 22, 2024), online: https://www.wired.com/story/shotspotter-secret-sensor-locations-leak/.

285 See Harvey Gee, "Bang!": ShotSpotter Gunshot Detection Technology, Predictive Policing, and Measuring Terry's Reach" in University of Michigan Journal of Law Reform (2022; Volume 55) , online: https://repository.law.umich.edu/mjlr/vol55/iss4/3/ at 775; Wired (Dhruv Mehrotra and Joey Scott), "Here Are the Secret Locations of ShotSpotter Gunfire Sensors" (February 22, 2024), online: https://www.wired.com/story/shotspotter-secret-sensor-locations-leak/.

286 Wired (Dhruv Mehrotra and Joey Scott), "Here Are the Secret Locations of ShotSpotter Gunfire Sensors" (February, 22 2024), online: https://www.wired.com/story/shotspotter-secret-sensor-locations-leak/.

287 CBCNews, "Toronto police scrap plans to acquire controversial gunshot-detection system" (February 14, 2019), online: https://www.cbc.ca/news/canada/toronto/toronto-police-scrap-plans-to-acquire-controversial-gunshot-detection-system-1.5019110.

288 CBCNews, "Toronto police scrap plans to acquire controversial gunshot-detection system" (February 14, 2019), online: https://www.cbc.ca/news/canada/toronto/toronto-police-scrap-plans-to-acquire-controversial-gunshot-detection-system-1.5019110.

289 See Nihar Patel et al, "Convolutional neural network and unmanned aerial vehicle-based public safety framework for human life protection" in International Journal of Communication Systems (2023; e5545) at 3.

290 ACLU (Jay Stanley), "Eye-in-the-Sky Policing Needs Stricter Limits" (July 26, 2023), online: https://www.aclu.org/documents/eye-in-the-sky-policing-needs-strict-limits at 1.

291 See Wired (Dhruv Mehrotra and Jesse Marx), "The Age of the Drone Police Is Here" (June 5, 2024), online: https://www.wired.com/story/the-age-of-the-drone-police-is-here/.

292 See Wired (Dhruv Mehrotra and Jesse Marx), "The Age of the Drone Police Is Here" (June 5, 2024), online: https://www.wired.com/story/the-age-of-the-drone-police-is-here/.

293 See Wired (Dhruv Mehrotra and Jesse Marx), "The Age of the Drone Police Is Here" (June 5, 2024), online: https://www.wired.com/story/the-age-of-the-drone-police-is-here/.

294 See Wired (Dhruv Mehrotra and Jesse Marx), "The Age of the Drone Police Is Here" (June 5, 2024), online: https://www.wired.com/story/the-age-of-the-drone-police-is-here/.

295 See Wired (Dhruv Mehrotra and Jesse Marx), "The Age of the Drone Police Is Here" (June 5, 2024), online: https://www.wired.com/story/the-age-of-the-drone-police-is-here/.

296 See Wired (Dhruv Mehrotra and Jesse Marx), "The Age of the Drone Police Is Here" (June 5, 2024), online: https://www.wired.com/story/the-age-of-the-drone-police-is-here/.

297 This possibility is suggested by Jay Stanley. See ACLU "Eye-in-the-Sky Policing Needs Stricter Limits" (July 26, 2023), online: https://www.aclu.org/documents/eye-in-the-sky-policing-needs-strict-limits at 3.

298 Even without the intervention of AI, Chula Vista police acknowledge that "[d]rones are sent more frequently to neighborhoods on the [poorer, immigrant-dense] west side because there is more crime reported there," which the *Wired* investigators characterize as a "circular explanation." See Wired (Dhruv Mehrotra and Jesse Marx), "The Age of the Drone Police Is Here" (June 5, 2024), online: https://www.wired.com/story/the-age-of-the-drone-police-is-here/.

299 Wired (Dhruv Mehrotra and Jesse Marx), "The Age of the Drone Police Is Here" (June 5, 2024), online: https://www.wired.com/story/the-age-of-the-drone-police-is-here/. See also ACLU (Jay Stanley), "Eye-in-the-Sky Policing Needs Stricter Limits" (July 26, 2023), online: https://www.aclu.org/documents/eye-in-the-sky-policing-needs-strict-limits.

300 See ACLU (Jay Stanley), "Eye-in-the-Sky Policing Needs Stricter Limits" (July 26, 2023), online: https://www.aclu.org/documents/eye-in-the-sky-policing-needs-strict-limits at 6.

301 Gothamist (Bahar Ostadan), "NYPD will deploy drones to respond to gunshots in 5 NYC precincts, officials say" (May 16, 2024), online: https://gothamist.com/news/nypd-will-deploy-drones-to-respond-to-911-calls-in-5-nyc-precincts-officials-say.

302 See ACLU (Jay Stanley), "Eye-in-the-Sky Policing Needs Stricter Limits" (July 26, 2023), online: https://www.aclu.org/documents/eye-in-the-sky-policing-needs-strict-limits at 4.

303 Proposed *Artificial Intelligence and Data Act* (AIDA) in Bill C-27, Parliament of Canada, online: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading, s. 4.

304 Proposed *Artificial Intelligence and Data Act* (AIDA) in Bill C-27, Parliament of Canada, online: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading, s. 2.

305 Proposed *Artificial Intelligence and Data Act* (AIDA) in Bill C-27, Parliament of Canada, online: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading, s. 38.

306 Proposed *Artificial Intelligence and Data Act* (AIDA) in Bill C-27, Parliament of Canada, online: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading, s. 3(2).

307 McMillan (Lyndsay A Wasser et al), "Privacy Reform is on the Table Once More: Canada Introduces the Digital Charter Implementation Act, 2022" (June 22, 2022), online: https://mcmillan.ca/insights/privacy-reform-is-on-the-table-once-more-canada-introduces-the-digital-charter-implementation-act-2022/.

308 Proposed *Artificial Intelligence and Data Act* (AIDA) in Bill C-27, Parliament of Canada, online: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading, ss. 4, 5(1).

309 See proposed *Artificial Intelligence and Data Act* (AIDA) in Bill C-27, Parliament of Canada, online: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading, ss. 5(1), 8, 14.

310 Proposed *Artificial Intelligence and Data Act* (AIDA) in Bill C-27, Parliament of Canada, online: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading, s. 5(1).

311 Proposed *Artificial Intelligence and Data Act* (AIDA) in Bill C-27, Parliament of Canada, online: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading, s. 5(1).

312 Law Commission of Ontario and Ontario Human Rights Commission, *Human Rights AI Impact Assessment* (November 2024), online: https://www.lco-cdo.org/wp-content/uploads/2024/11/LCO-Human-Rights-AI-Impact-Assessment-EN.pdf, at 2.

313 Law Commission of Ontario and Ontario Human Rights Commission, *Human Rights AI Impact Assessment* (November 2024), online: https://www.lco-cdo.org/wp-content/uploads/2024/11/LCO-Human-Rights-AI-Impact-Assessment-EN.pdf, at 3.

314 Ontario Bill 194, *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024* (introduced for first reading May 13, 2024; second reading May 28, 2024,royal assent November 25, 2024): https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194 at Schedule 1, *Enhancing Digital Security and Trust Act, 2024* (May 13, 2024): https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194#BK3.

315 Ontario Bill 194, *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024* (introduced for first reading May 13, 2024; second reading May 28, 2024,royal assent November 25, 2024): https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194 at Schedule 1, *Enhancing Digital Security and Trust Act, 2024* (May 13, 2024): https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194#BK3.

316 Preamble to Ontario Bill 194, *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024* (introduced for first reading May 13, 2024; second reading May 28, 2024,royal assent November 25, 2024): https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194 at Schedule 1, *Enhancing Digital Security and Trust Act, 2024* (May 13, 2024): https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194#BK3.

317 Ontario Bill 194, *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024* (introduced for first reading May 13, 2024; second reading May 28, 2024,royal assent November 25, 2024): https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194 at Schedule 1, *Enhancing Digital Security and Trust Act, 2024* (May 13, 2024): https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194#BK3.

318 For a comprehensive analysis of Bill 194, see: Law Commission of Ontario, "Submission to Ontario re Bill 194" (June 2024): https://www.lco-cdo.org/wp-content/uploads/2024/06/LCO-Submission-to-Government-of-Ontario-Bill-194-Consultations-June-2024.pdf.

319 Law Commission of Ontario, "Submission to Ontario re Bill 194" (June 2024): https://www.lco-cdo.org/wp-content/uploads/2024/06/LCO-Submission-to-Government-of-Ontario-Bill-194-Consultations-June-2024.pdf.

320 Law Commission of Ontario, "Submission to Ontario re Bill 194" (June 2024): https://www.lco-cdo.org/wp-content/uploads/2024/06/LCO-Submission-to-Government-of-Ontario-Bill-194-Consultations-June-2024.pdf.

321 Law Commission of Ontario, "Submission to Ontario re Bill 194" (June 2024): https://www.lco-cdo.org/wp-content/uploads/2024/06/LCO-Submission-to-Government-of-Ontario-Bill-194-Consultations-June-2024.pdf.

322 Law Commission of Ontario, "Submission to Ontario re Bill 194" (June 2024): https://www.lco-cdo.org/wp-content/uploads/2024/06/LCO-Submission-to-Government-of-Ontario-Bill-194-Consultations-June-2024.pdf.

323 Toronto Police Services Board, "Use of Artificial Intelligence Technology" (February 28, 2022; updated January 11, 2024): https://tpsb.ca/policies-by-laws/board-policies/195-use-of-artificial-intelligence-technology.

324 Correspondence from Laila Martin, A. Director, National Technology Onboarding Program Technical Operations, Royal Canadian Mounted Police (RCMP) to Law Commission of Ontario (May 2024), on file with the LCO.

325 LCO research in summer 2023 found that the TPSB policy was the only published AI policy among over a dozen municipal police forces considered. Since then, and other than the RCMP, the LCO is aware of only Ontario's Durham Police having developed an AI policy. See Durham Regional Police Service Board, "Use of Artificial Intelligence" (October 15 2024), online: https://durhampoliceboard.ca/wp-content/uploads/2024/10/Policy-Use-of-AI.pdf.

326 In December 2023, the Executive Director recommended that this "catch-all" portion of the definition be removed as requiring a full review of applications that fell under that definition--none of which used automated analytical problem-solving models--was viewed as being unnecessarily time-consuming: Toronto Police Services Board Public Meeting (January 11, 2024), online: https://tpsb.ca/jdownloads-categories?task=download.send&id=813:january-11-2024-public-agenda&catid=32 at 3.

327 Toronto Police Services Board, "Use of Artificial Intelligence Technology" (February 28, 2022; amended January 11, 2024), online: https://tpsb.ca/policies-by-laws/board-policies/195-use-of-artificial-intelligence-technology.

328 See: Information and Privacy Commissioner of Ontario, "Letter to the Toronto Police Services re AI Policy and Risk Classification Report" (January 10, 2024) online: https://www.ipc.on.ca/resource/letter-to-the-toronto-police-services-board-about-facial-recognition-mugshot-database-program/; and Ontario Human Rights Commission, "Approval of high-risk technologies under the Toronto Police Services Board's Policy on the use of artificial intelligence technology" (January 10 2024): https://www.ohrc.on.ca/en/news_centre/approval-high-risk-technologies-under-toronto-police-services-boards-policy-use-artificial.

329 The Citizen Lab, *To Surveil and Predict A Human Rights Analysis of Algorithmic Policing in Canada* (September 1, 2020), online: https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/.

330 Office of the Privacy Commissioner of Canada, Police use of Facial Recognition Technology in Canada and the way forward (June 10, 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/.

331 Office of the Privacy Commissioner of Canada, Police use of Facial Recognition Technology in Canada and the way forward (June 10, 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/.

332 Office of the Privacy Commissioner of Canada, Police use of Facial Recognition Technology in Canada and the way forward (June 10, 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/.

333 RCMP Communication with the Law Commission of Ontario, on file with the LCO.

334 RCMP, National Technology Onboarding Program, *Transparency Blueprint: Snapshot of Operational Technologies* (2024), at p 19-20, online: https://rcmp.ca/sites/default/files/doc/national-technology-onboarding-program-transparency-blueprint.pdf. See also RCMP, "Babel X platform: Overview and privacy impact assessment initiation" (October 25 2022), online: https://www.rcmp-grc.gc.ca/en/babel-x-platform.

335 RCMP Communication with the Law Commission of Ontario, on file with the LCO.

336 RCMP Communication with the Law Commission of Ontario, on file with the LCO.

337 European Union, Artificial Intelligence Act (Regulation (EU) 2024/1689 of the European Parliament and of the Council (June 13, 2024), online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689.

338 See for instance: the *AI in Government Act of 2020* (Pub. L. No. 116-260, div. U, title 1, § 104 (codified at 40 U.S.C. § 11301): https://www.congress.gov/116/plaws/publ260/PLAW-116publ260.pdf); *Advancing American AI Act* (Pub. L. No. 117-263, div. G, title LXXII, subtitle B, §§ 7224(a), 7224(d)(1)(B), and 7225 (codified at 40 U.S.C. 11301): https://www.congress.gov/117/plaws/publ263/PLAW-117publ263.pdf; United States, Office of the President, Executive Order 14110 "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" (November 1 2023): https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence; and the United States, Executive Office of the President, Office of Management and Budget, "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence" (March 28 2024): https://www.whitehouse.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.

339 EO1 at s. 7.

340 EO1 at s. 7-9.

341 EO2 at 1.

342 EO2 at 31.

343 EO2 at 32-33.

344 EO2 at 1.

345 EO2 at 4-5.

346 EO2 at 2.

347 EO2 at 9-14

348 EO2 at 2.

349 EO2 at 14-26.

350 And, of course, the potential for more regular assertions of "investigative privilege" or s. 37 *Canada Evidence Act* assertions of privilege, resulting in the bifurcation of criminal proceedings should the parties be required to litigate disclosure issues in the Federal Court.

351 See *R. v. Tessling*, 2004 SCC 67 at para 25 (quoting *R. v. Plant*, [1993] 3 SCR 281) at p 293.

352 *R. v. Bykovets,* 2024 SCC 6 at para 44. This means that the individual subjectively expected that the information would remain private and that their expectation was objectively reasonable in the circumstances: see, for example, *R. v. Marakah*, 2017 SCC 59 at paras 12, 15.

353 *R. v. Spencer*, 2014 SCC 43 at paras 41-42.

354 *R. v. Spencer*, 2014 SCC 43 at para 48. See also *R. v. Ward*, 2012 ONCA 660 at paras 71, 75.

355 *R. v. Spencer,* 2014 SCC 43 at para 43.

356 *R. v. Wise*, [1992] 1 SCR 527 at 558 (emphasis added), quoting Melvin Gutterman, "A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance" in Syracuse Law Review (1988; Volume 39) at 706.

357 *R. v. Bykovets,* 2024 SCC 6 at para 48, citing *R. v. Jones*, 2017 SCC 60 at para 45.

358 *R. v. Hoang,* 2021 ONSC 6054 at paras 61-66; *R. v. Ngo,* 2022 ONSC 3700 at paras 27, 51, 60; *R. v. Kang,* 2020 BCSC 1616 at para 67.

359 The *Charter* only protects a person against state actions.

360 *R. v. McPherson,* [2023] OJ No 546 at para 105.

361 *R. v. Le*, 2019 SCC 34 at para 25, per Brown and Martin JJ, citing *R. v. Grant*, 2009 SCC 32 at para 20.

362 *R. v. Mann*, 2004 SCC 52 at para 34.

363 *R. v. Ahmed*, 2020 SCC 11 at para 30.

364 *R. v. Chehil*, 2013 SCC 39 at para 29; *R. v. McKenzie*, 2011 ONCA 42 at para 8; *R. v. Hall*, 22 OR (3d) 289 (CA).

365 SoundThinking, ShotSpotter, online: https://www.soundthinking.com/law-enforcement/leading-gunshot-detection-system/.

366 *R. v. Grant*, 2009 SCC 32 at para 55.

367 *R. v. Mann*, 2004 SCC 52 at para 47; see also *R. v. Smeltzer*, 2021 ONCA 472 at paras 22-23. For an in-depth analysis of s. 9 and predictive policing, see Kaitlynd Hiller, "Predictive Policing and the Charter" in Manitoba Law Journal (2021; Volume 44-6), online: 2021 CanLIIDocs 13416.

368 *R. v. Mann*, 2004 SCC 52 at para 47.

369 The New York Times (Natasha Singer and Cade Metz), "Many Facial-Recognition Systems Are Biased, Says U.S. Study" (December 19, 2019), online: https://www.nytimes.com/2019/12/19/technology/facial-recognition-bias.html.)

370 Kaitlynd Hiller, "Predictive Policing and the Charter" in Manitoba Law Journal (2021; Volume 44-6), online: 2021 CanLIIDocs 13416 at 242.

371 *Barre v Canada (Citizenship and Immigration)*, 2022 FC 1078 at para 28.

372 *Barre v Canada (Citizenship and Immigration)*, 2022 FC 1078 at para 59.

373 *Ali v. Canada (Public Safety and Emergency Preparedness)*, 2024 FC 1085.

374 *Ali v. Canada (Public Safety and Emergency Preparedness)*, 2024 FC 1085 at para. 28.

375 *Ali v. Canada (Public Safety and Emergency Preparedness)*, 2024 FC 1085 at para. 33.

376 Kaitlynd Hiller, "Predictive Policing and the Charter" in Manitoba Law Journal (2021; Volume 44-6), online: 2021 CanLIIDocs 13416 at 242, citing: Fabio Arcila Jr, "Nuance, Technology, and the Fourth Amendment: A Response to Predictive Policing and Reasonable Suspicion" Emory Law Journal (2014; Volume 63), online: https://scholarlycommons.law.emory.edu/elj-online/30/ at 2088; and The Citizen Lab (Kate Robertson et al), *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada* (2020), online: http://www.citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf at 130–31.

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

378 *R. v. Spencer* (2014 SCC 43) at para 16.

379 *Hunter et al v Southam Inc* ([1984] 2 SCR 145).

380 *Hunter et al v Southam Inc* ([1984] 2 SCR 145) at 159.

381 *Hunter et al v Southam Inc* ([1984] 2 SCR 145) at 159-60.

382 *Hunter et al v Southam Inc* ([1984] 2 SCR 145) at 161.

383 *R. v. Golub* (1997 CanLII 6316 (ONCA), 1997 CarswellOnt 2448) at para 43.

384 *R. v. Plant* ([1993] 3 SCR 281) at 293.

385 *R. v. Kang-Brown* (2008 SCC 18) at para 175. Here, the use of a police sniffer dog to identify drugs constituted a search: police inferred the contents of the accused's backpack by obtaining information about the air surrounding the backpack.

386 *R. v. Spencer* (2014 SCC 43).

387 *R. v. Spencer* (2014 SCC 43) at para 43.

388 See *R. v. Spencer* (2014 SCC 43) at paras 42, 46.

389 *R. v. Bykovets* (2024 SCC 6).

390 See *R. v. Duarte* ([1990] 1 SCR 30); *R. v. Wong* ([1990] 3 SCR 36).

391 See *R. v. Wise* ([1992] 1 SCR 527). See also *R. v. Spencer* (2014 SCC 43) at paras 43–44.

392 *R. v. Tessling* (2004 SSC 67) at para 19.

393 *R. v. Tessling* (2004 SSC 67) at para 19.

394 *R. v. Tessling* (2004 SSC 67) at para 32.

395 *R. v. Louie* (2023 ABKB 352) at Appendix 1, para 35. For binding law in Ontario see *R. v. Yu* (2019 ONCA 942).

396 *R. v. Louie* (2023 ABKB 352) at Appendix 1, paras 33–58.

397 *R. v. Wong* (1990 CanLII 56 (SCC), [1990] 3 SCR 36).

398 *R. v. Sanchez* (2020 BCSC 1917) at para 121.

399 *R. v. Cole* (2012 SCC 53) at para 75; *R. v. Bykovets* (2024 SCC 6) at para 47.

400 See *R. v. Cole* (2012 SCC 53) at paras 74–79.

401 *R. v. Reeves* (2018 SCC 56).

402 *R. v. Reeves* (2018 SCC 56) at para 48.

403 *Bykovets* thus expanded the protections mandated by *Spencer*, which required police to obtain warrants for the search and seizure of subscriber information (name, address, etc.) associated with an IP address, but not the IP address alone.

404 *R. v. Bykovets* (2024 SCC 6) at para 9.

405 *R. v. Bykovets* (2024 SCC 6) at para 65.

406 See *R. v. Bykovets* (2024 SCC 6) at paras 61–66.

407 *R. v. Bykovets* (2024 SCC 6) at para 21.

408 *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5), online: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-1.html.

409 *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5), online: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-1.html at s 7(3)(c.1).

410 *R. v. Spencer* (2014 SCC 43) at para 62.

411 *R. v. Spencer* (2014 SCC 43) at para 62.

412 *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5), online: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-1.html at s 7(3)(d).

413 *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5), online: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-1.html at s 7(3)(d).

414 See *R. v. Spencer* (2014 SCC 43) at para 64; *R. v. Orlandis-Habsburgo* (2017 ONCA 649) at paras 109–10.

415 *Personal Information Protection and Electronic Documents Act* (S.C. 2000, c. 5), online: https://laws-lois.justice.gc.ca/eng/acts/p-8.6/page-1.html at ss 7(3)(d.1)–(d.2).

416 Office of the Privacy Commissioner of Canada, "Applying paragraphs 7(3)(d.1) and 7(3)(d.2) of PIPEDA" (March 2017), online: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/gd_d1-d2_201703/.

417 *Freedom of Information and Protection of Privacy Act* (RSO 1990, c F31), online: https://www.ontario.ca/laws/statute/90f31 [*FIPPA*]. In Ontario, municipal institutions are governed by the *Municipal Freedom of Information and Protection of Privacy Act* (RSO 1990, c M56), online: https://www.ontario.ca/laws/statute/90m56 [*MFIPPA*]. Note that s 32(g) of the *MFIPPA* contains language identical to the language of *FIPPA* s 42(1)(g), discussed below.

418 See Information and Privacy Commissioner of Ontario, *Guidelines for the Use of Video Surveillance* (IPC Ontario, 2015) at 14.

419 *Freedom of Information and Protection of Privacy Act* (RSO 1990, c F31), online: https://www.ontario.ca/laws/statute/90f31 at 42(1)(g)(ii).

420 *Freedom of Information and Protection of Privacy Act* (RSO 1990, c F31), online: https://www.ontario.ca/laws/statute/90f31 at 42(1)(g)(i).

421 *R. v. Noftall* (2019 ONSC 4241) at para 27.

422 Information and Privacy Commissioner of Ontario, *Guidelines for the Use of Video Surveillance* (IPC Ontario, 2015) at 4.

423 See Kate Robertson, "Submission to the Standing Committee on Industry and Technology Study of Bill C-27, *The Digital Charter Implementation Act*, 2022" (Toronto: Citizen Lab), online: https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12605754/br-external/RobertsonKate-Combined-e.pdf at 9.

424 Bill C-27, *Digital Charter Implementation Act, 2022* (1st Sess, 44th Parl) (first reading 16 June 2022), online: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading at cl 44.

425 Bill C-27, *Digital Charter Implementation Act, 2022* (1st Sess, 44th Parl) (first reading 16 June 2022), online: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading at cl 44; *R. v. Spencer* (2014 SCC 43) at para 62.

426 Rahul Kanwal & Keven Walby, *Tracking the Surveillance and Information Practices of Data Brokers: A Report* (Winnipeg: Centre for Access to Information and Justice, 2024) at 13–14. See also Ashley Belanger, "NSA finally admits to spying on Americans by purchasing sensitive data," *Ars Technica* (26 January 2014), online: https://arstechnica.com/tech-policy/2024/01/nsa-finally-admits-to-spying-on-americans-by-purchasing-sensitive-data/.

427 *R. v. Bykovets* (2024 SCC 6) at para 65. The SCC cited *State v. Simmons* (190 Vt. 141 (2011)). In this case, police asked the social media website MySpace to provide them with a list of IP addresses that had accessed a suspect's profile. MySpace responded by providing not only the list of IP addresses, but complete documentation of when and how often each IP address had accessed the page.

428 Thomas Brewster, "FedEx's Secretive Police Force Is Helping Cops Build An AI Car Surveillance Network," *Forbes* (19 June 2024), online: https://www.forbes.com/sites/thomasbrewster/2024/06/19/fedex-police-help-cops-build-an-ai-car-surveillance-network/.

429 Josh A Roth, "Drawing Lines: geofence warrants and the third-party doctrine" (2023) 4 Intl Cybersecurity L Rev 213 at 214.

430 Thomas Germain, "Google Finally Stops Handing Your Location Data to Cops," *Gizmodo* (15 December 2023), online: https://gizmodo.com/google-ends-geofence-warrants-location-data-tracking-1851102594.

431 See Tonja Jacobi & Dustin Stonecipher, "A Solution for the Third-Party Doctrine in a Time of Data Sharing, Contact Tracing, and Mass Surveillance" (2022) 97 Notre Dame L Rev 823; Josh A Roth, "Drawing Lines: geofence warrants and the third-party doctrine" (2023) 4 Intl Cybersecurity L Rev 213.

432 *R. v. Bykovets* (2024 SCC 6) at para 47.

433 For instance, see *R. v. Rogers Communications Partnership* (2016 ONSC 70).

434 See American Civil Liberties Union, "Court Rules Warrantless Section 702 Searches Violated the Fourth Amendment" (January 22 2025), online: https://www.aclu.org/press-releases/court-rules-warrantless-section-702-searches-violated-the-fourth-amendment. The judgement in U.S. v. Hasbajrami (11-cr-00623-LDH) (January 21 2025) is available online: https://www.aclu.org/documents/section-702-memorandum-and-order-u-s-v-hasbajrami-11-cr-00623-ldh.

435 U.S. v. Hasbajrami (11-cr-00623-LDH) (January 21 2025) at p 52, online: https://www.aclu.org/documents/section-702-memorandum-and-order-u-s-v-hasbajrami-11-cr-00623-ldh.

436 See *R. v. Bykovets* (2024 SCC 6); *R. v. Spencer* (2014 SCC 43).

437 *Privacy Act* (RSC, 1985, c P-21) at s 4.

438 Office of the Privacy Commissioner of Canada, *Police use of Facial Recognition Technology in Canada and the way forward* (10 June 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/. Office of the Privacy Commissioner of Canada, *Police use of Facial Recognition Technology in Canada and the way forward* (10 June 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/.

439 Office of the Privacy Commissioner of Canada, "Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta" (2 February 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/.

440 Office of the Privacy Commissioner of Canada, "Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta" (2 February 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/ at "Overview."

441 Office of the Privacy Commissioner of Canada, "Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta" (2 February 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/ at "Overview."

442 Office of the Privacy Commissioner of Canada, "Report of findings: Investigation into the RCMP's collection of personal information from Clearview AI (involving facial recognition technology)," *Police use of Facial Recognition Technology in Canada and the way forward* (10 June 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/ at para 4.

443 Office of the Privacy Commissioner of Canada, "Report of findings: Investigation into the RCMP's collection of personal information from Clearview AI (involving facial recognition technology)," *Police use of Facial Recognition Technology in Canada and the way forward* (10 June 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/ at para 42.

444 Office of the Privacy Commissioner of Canada, *Police use of Facial Recognition Technology in Canada and the way forward* (10 June 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/ at "Commissioner's Message."

445 Royal Canadian Mounted Police, "Response to the Report by the Office of the Privacy Commissioner into the RCMP's use of Clearview AI" (10 June 2021), online: https://www.rcmp-grc.gc.ca/en/news/2021/response-the-report-the-office-the-privacy-commissioner-the-rcmps-use-clearview-ai.

446 See Office of the Privacy Commissioner of Canada, "Investigation of the RCMP's collection of open-source information under Project Wide Awake" (15 February 2024), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202324/sr_pa_20240215_rcmp-pwa/.

447 Office of the Privacy Commissioner of Canada, "Report of findings: Investigation into the RCMP's collection of personal information from Clearview AI (involving facial recognition technology)," *Police use of Facial Recognition Technology in Canada and the way forward* (10 June 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/ at para 42.

448 *Hunter et al v Southam Inc* ([1984] 2 SCR 145) at 161.

449 See *R. v. Tessling* (2004 SSC 67) at para 32.

450 See *R. v. Kang-Brown* (2008 SCC 18) at para 175.

451 See David TS Fraser, "Law enforcement requests for customer information- Come Back With A Warrant," *Canadian Privacy Law Blog* (16 May 2022), online: https://blog.privacylawyer.ca/2022/05/video-law-enforcement-requests-for.html. See also Kristen Robinson, "Battle between police and Coquitlam, B.C. Cactus Club over surveillance video," *Global News* (28 February 2024), online: https://globalnews.ca/news/10322811/battle-police-coquitlam-cactus-club-surveillance-video/.

452 See 404Media.co, "The Powerful AI Tool That Cops (or Stalkers) Can Use to Geolocate Photos in Seconds" (January 20, 2025), online: https://www.404media.co/the-powerful-ai-tool-that-cops-or-stalkers-can-use-to-geolocate-photos-in-seconds/.

453 The Citizen Lab, *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada* (Toronto: The Citizen Lab, 2020) at 75.

454 Joe Bongiorno, "As police increasingly use facial recognition technology, calls grow for regulations," *Toronto Star* (30 June 2024), online: https://www.thestar.com/news/canada/quebec/as-police-increasingly-use-facial-recognition-technology-calls-grow-for-regulations/article_60d524fa-4beb-5731-8a05-d9e4844da4e5.html.

455 Joe Bongiorno, "As police increasingly use facial recognition technology, calls grow for regulations," Toronto Star (30 June 2024), online: https://www.thestar.com/news/canada/quebec/as-police-increasingly-use-facial-recognition-technology-calls-grow-for-regulations/article_60d524fa-4beb-5731-8a05-d9e4844da4e5.html.

456 *R. v. Rahi* (2023 ONSC 190), online: https://canlii.ca/t/jttlg.

457 *R. v. Rahi* (2023 ONSC 190) at paras 18-19, online: https://canlii.ca/t/jttlg.

458 *R. v Hughes* (2023 ONSC 109), online: https://canlii.ca/t/jxfks.

459 Office of the Privacy Commissioner of Canada, "Investigation of the RCMP's collection of open-source information under Project Wide Awake" (15 February 2024), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202324/sr_pa_20240215_rcmp-pwa/ at para 32.

460 *R. v. Tessling* (2004 SSC 67) at para 19.

461 *R. v. Tessling* (2004 SSC 67) at para 19.

462 See The Citizen Lab, *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada* (Toronto: The Citizen Lab, 2020) at 75.

463 See for example: *R. v. Bagri* (2004) 184 C.C.C. (3d) 449 (S.C.C.); *R. v. Regan* (2002), 161 C.C.C. (3d) 97 (S.C.C.); *R. v. Shirose and Campbell* (1999), 133 C.C.C. (3d) 257 (S.C.C.); Report of the Ipperwash Inquiry; Martin Report; Code-Lesage Report.

464 See Ontario, "Crown Prosecution Manual" (updated January 31, 2024), online: https://www.ontario.ca/document/crown-prosecution-manual.

465 See Canada, "Public Prosecution Service of Canada Deskbook" (March 1, 2014), online: https://www.ppsc-sppc.gc.ca/eng/pub/fpsd-sfpg/index.html.

466 *Smith v. Ontario (Attorney General)*, 2019 ONCA 651 at paras 76, 89.

467 See for example: R. v. Bagri (2004) 184 C.C.C. (3d) 449 (S.C.C.); R. v. Regan (2002), 161 C.C.C. (3d) 97 (S.C.C.); R. v. Shirose and Campbell (1999), 133 C.C.C. (3d) 257 (S.C.C.); Report of the Ipperwash Inquiry; Martin Report; Code-Lesage Report.

468 *R. v. Vu* (2013 SCC 60); *R. v. Fearon* (2014 SCC 77).

469 *R. v. Stinchcombe* [1991] 3 SCR 326.

470 *R. v. McNeil*, 2009 SCC 3, para 17.

471 *R. v. Gubbins*, 2018 SCC 44 at para19.

472 *R. v. Gubbins*, 2018 SCC 44 at para 19.

473 *R. v. McNeil*, 2009 SCC 3 at para 24.

474 *R. v. McNeil*, 2009 SCC 3 at para 54.

475 *R. v. Gubbins*, 2018 SCC 44, at para 23.

476 *R. v. O'Connor*, [1995] 4 SCR 411; R. v. McNeil, 2009 SCC 3.

477 *R. v. McNeill*, 2009 SCC 3 at para 46.

478 *R. v. Hughes*, 2022 ONSC 2164 at para 136.

479 *R. v. Amer*, 2017 ABQB 651 at para 33.

480 *R. v. Richards*, [1997] OJ No 2086 (Ont. CA) at para 11.

481 *R. v. Hughes*, 2022 ONSC 2164 at para 148.

482 *R. v. Hughes*, 2022 ONSC 2164 at para 148.

483 *R. v. Hughes*, 2022 ONSC 2164.

484 On a *Garofoli* application the reviewing judge will consider whether, based on the record and as amplified on review, whether the authorizing justice could have issued the warrant. R. v. Garofoli, [1990] 2 SCR 1421.

485 *R. c. Mirarchi*, 2015 QCCS 6629.

486 *R. c. Mirarchi*, 2015 QCCS 6629.

487 *Parent c. R.*, 2018 QCCA 555.

488 Aaron Shapiro, "Predictive Policing for Reform? Indeterminacy and Intervention in Big Data Policing," (2019) 27 Surveillance and Society.

489 "Algorithms as Discrimination Detectors" (2020), 117:8 PNAS 30096.

490 Jon Kleinberg et al, "Discrimination in the Age of Algorithms" (2019), 2018:10 J Leg Analysis 114 at 114.

491 See Jon Kleinberg et al, "Algorithms as Discrimination Detectors" (2020), 117:8 PNAS 30096 at 30099.

492 See Jon Kleinberg et al, "Algorithms as Discrimination Detectors" (2020), 117:8 PNAS 30096 at 30100; Daniel Konikoff, *Automating the Thin Blue Line: Controversy, Knowledge, and the Governance of Police Technology in Canada* (PhD Dissertation, University of Toronto, 2024) [unpublished], ch 2-3.

493 See Tzu-Wei Hung & Chun-Ping Yen, "Predictive Policing and Algorithmic Fairness" (2023) 201:206 Synthese; Yen and Hung, "Achieving Equality with Predictive Policing Algorithms: A Social Safety Net Perspective" (2021) 27:36 Science and Engineering Ethics.

494 "Achieving Equality with Predictive Policing Algorithms: A Social Safety Net Perspective" (2021) 27:36 Science and Engineering Ethics at 11.

495 See The Citizen Lab, To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada (Toronto: The Citizen Lab, 2020) at 51-52.

496 See Tzu-Wei Hung & Chun-Ping Yen, "Predictive Policing and Algorithmic Fairness" (2023) 201:206 Synthese at 21.

497 The use of AI to enhance EIS systems was pioneered by a 2015 collaboration between University of Chicago researchers and the Charlotte-Mecklenburg Police Department and is now employed in commercial software such as Benchmark Analytics' First Sign. See Samuel Carton et al, "Identifying Police Officers at Risk of Adverse Events" (Paper delivered at the 22nd ACM SIGKDD International Conference, August 2016), DOI: <https://dl.acm.org/doi/10.1145/2939672.2939698>; Benchmark Analytics, "First Sign Early Intervention," online: https://www.benchmarkanalytics.com/first-sign-early-intervention-system/.

498 See John McCormick, "Police Departments Turn to AI-Based Intervention System for Officer Misconduct," *The Wall Street Journal* (21 September 2020), online: https://www.wsj.com/articles/police-departments-turn-to-ai-based-intervention-system-for-officer-misconduct-11600693200

499 See Ted Gregory, "U. of C. Researchers Use Data to Predict Police Misconduct," *Chicago Tribune* (18 August 2016), online: https://www.chicagotribune.com/2016/08/18/u-of-c-researchers-use-data-to-predict-police-misconduct/.

500 See Samuel Carton et al, "Identifying Police Officers at Risk of Adverse Events" (Paper delivered at the 22nd ACM SIGKDD International Conference, August 2016), DOI: https://dl.acm.org/doi/10.1145/2939672.2939698.

501 See "Profiling Accountability Solution System," US Patent No 2022156671A1 (16 November 2020). PASS was developed specifically to facilitate police departments' adherence to California's *Racial and Identity Profiling Act*; see LEFTA Systems, "LEFTA Systems Offers Solution to Satisfy California's Racial and Identity Profiling Act" (2 December 2020), online: https://leftasystems.org/lefta-systems-offers-solution-to-satisfy-californias-racial-and-identity-profiling-act/.

502 See Umar Farooq, "Police Departments Are Turning to AI to Sift Through Millions of Hours of Unreviewed Body-Cam Footage," *Propublica* (2 February 2024), online: https://www.propublica.org/article/police-body-cameras-video-ai-law-enforcement; Jonathan Serrie & Samantha Daigle, "Police Departments Across America Using AI to Analyze Officers' Bodycam Video," *FOX News* (18 July 2023), online: https://www.foxnews.com/us/police-departments-america-using-ai-analyze-officers-bodycam-video. These programs are not without controversy: In Seattle, police stopped using AI to analyze body cam footage following criticisms from civil liberties groups and the police union. See Mike Carter, "Decision to Halt Program Analyzing Seattle Police Bodycam Video Under Scrutiny," *Seattle Times* (27 September 2023), online: https://www.seattletimes.com/seattle-news/law-justice/decision-to-halt-program-analyzing-seattle-police-bodycam-video-under-scrutiny/.

503 See Jordyn Pair, "Ann Arbor Police to Use AI to Review Body Camera Footage," *MLive.com* (7 August 2023), online: https://www.mlive.com/news/ann-arbor/2023/08/ann-arbor-police-to-use-ai-to-review-body-camera-footage.html; Libor Jany, "LAPD to Use AI to Analyze Body Cam Videos for Officers' Language Use," *Los Angeles Times* (22 August 2023), online: https://www.latimes.com/california/story/2023-08-22/lapd-to-use-ai-to-analyze-body-cam-videos-for-officers-language-use.

504 See Umar Farooq, "Police Departments Are Turning to AI to Sift Through Millions of Hours of Unreviewed Body-Cam Footage," *Propublica* (2 February 2024), online: https://www.propublica.org/article/police-body-cameras-video-ai-law-enforcement.

505 See Russell Contreras, "AI Helps Defense Attorneys Sift Through Police Body Cam Videos," *Axios* (16 November 2023), online: https://www.axios.com/2023/11/16/ai-defense-attorneys-police-bodycam-videos; Matt Reynolds, "Locked in: Criminal Justice Startups Tap into Generative AI's Early Promise," *ABA Journal* (1 February 2024), online: https://www.abajournal.com/legalrebels/article/locked-in-criminal-justice-startups-tap-into-generative-ais-early-promise.

506 See National Institute of Justice, "Attitudes of Reporting Officers Extracted From Incident Reports Can Affect Rape Case Outcomes," *NIJ* (1 March 2024), online: https://nij.ojp.gov/topics/articles/attitudes-reporting-officers-extracted-incident-reports-can-affect-rape-case.

507 See National Institute of Justice, "Attitudes of Reporting Officers Extracted From Incident Reports Can Affect Rape Case Outcomes," *NIJ* (1 March 2024), online: https://nij.ojp.gov/topics/articles/attitudes-reporting-officers-extracted-incident-reports-can-affect-rape-case.

508 See National Institute of Justice, "Research Rooted in Machine Learning Challenges Conventional Thinking About the Pathways to Violent Extremism," *NIJ* (24 July 2023), online: https://nij.ojp.gov/topics/articles/research-rooted-machine-learning-challenges-conventional-thinking-about-pathways.

509 "Detecting Racial Inequalities in Criminal Justice: Towards an Equitable Deep Learning Approach for Generating and Interpreting Racial Categories Using Mugshots" (2023) 38 AI & Soc 897.

510 See CBS News Philadelphia, "Police Hope Artificial Intelligence Can Help Solve 1991 Cape May County Cold Case," *CBS News* (25 May 2023), online: https://www.cbsnews.com/philadelphia/news/mark-himebaugh-cold-case-ai-cape-may-county-crime/.

511 See Vivek Narayanan, "AI Image Raises Hope of Finding 2-year-old Girl Missing for 13 Years," *The Times of India* (20 May 2024), online: https://timesofindia.indiatimes.com/city/chennai/ai-image-raises-hope-of-finding-2-year-old-girl-missing-for-13-years/articleshow/110259361.cms.

512 See Mikaila Kimball, "Western Prof Michael Arntfield is Catching Serial Killers with AI," *The Gazette* (5 March 2024), online: https://westerngazette.ca/culture/profiles/western-prof-michael-arntfield-is-catching-serial-killers-with-ai/article_7b9aae78-db0b-11ee-a84b-9712c59f39de.html.

513 See Forensic Technology Centre of Excellence, *What FSSP Leaders Should Know About Artificial Intelligence and its Application to Forensic Science* (Research Triangle Park, NC: RTI International, 2023).

514 In one case in Pune, India, AI accident reconstruction helped to avoid retraumatizing a child witness by bringing them to the scene of the accident. See Times of India City Desk, "Pune Porsche Crash: Police to Digitally Recreate Accident Scene with AI Tools," *The Times of India* (30 May 2024), online: https://timesofindia.indiatimes.com/city/pune/pune-porsche-crash-police-to-digitally-recreate-accident-scene-with-ai-tools/articleshow/110549050.cms.

515 See Waad Barakat, "Dubai: Autopsy in 5 Minutes; How Police are Using AI to Solve Crimes Faster," *Khaleej Times* (5 March 2024), online: https://www.khaleejtimes.com/uae/dubai-autopsy-in-5-minutes-how-police-are-using-ai-to-solve-crimes-faster.

516 See University of Pennsylvania, "How AI Tools Can Help Assess Verbal Eyewitness Statements," *Phys.org* (4 March 2024), online: https://phys.org/news/2024-03-ai-tools-eyewitness-statements.html.

517 See Kyodo News, "Japan Police to Stamp Out Online Criminal Activity with Help of AI," *Kyodo News* (28 September 2023), online: https://english.kyodonews.net/news/2023/09/f23065f0cc1a-japan-police-to-stamp-out-online-criminal-activity-with-help-of-ai.html.

518 See Kim Hyun-Soo, "Police Develop Deepfake Detection Tool to Stamp Out AI-driven Crimes," *Yonhap News Agency* (5 March 2024), online: https://en.yna.co.kr/view/AEN20240305003100315.

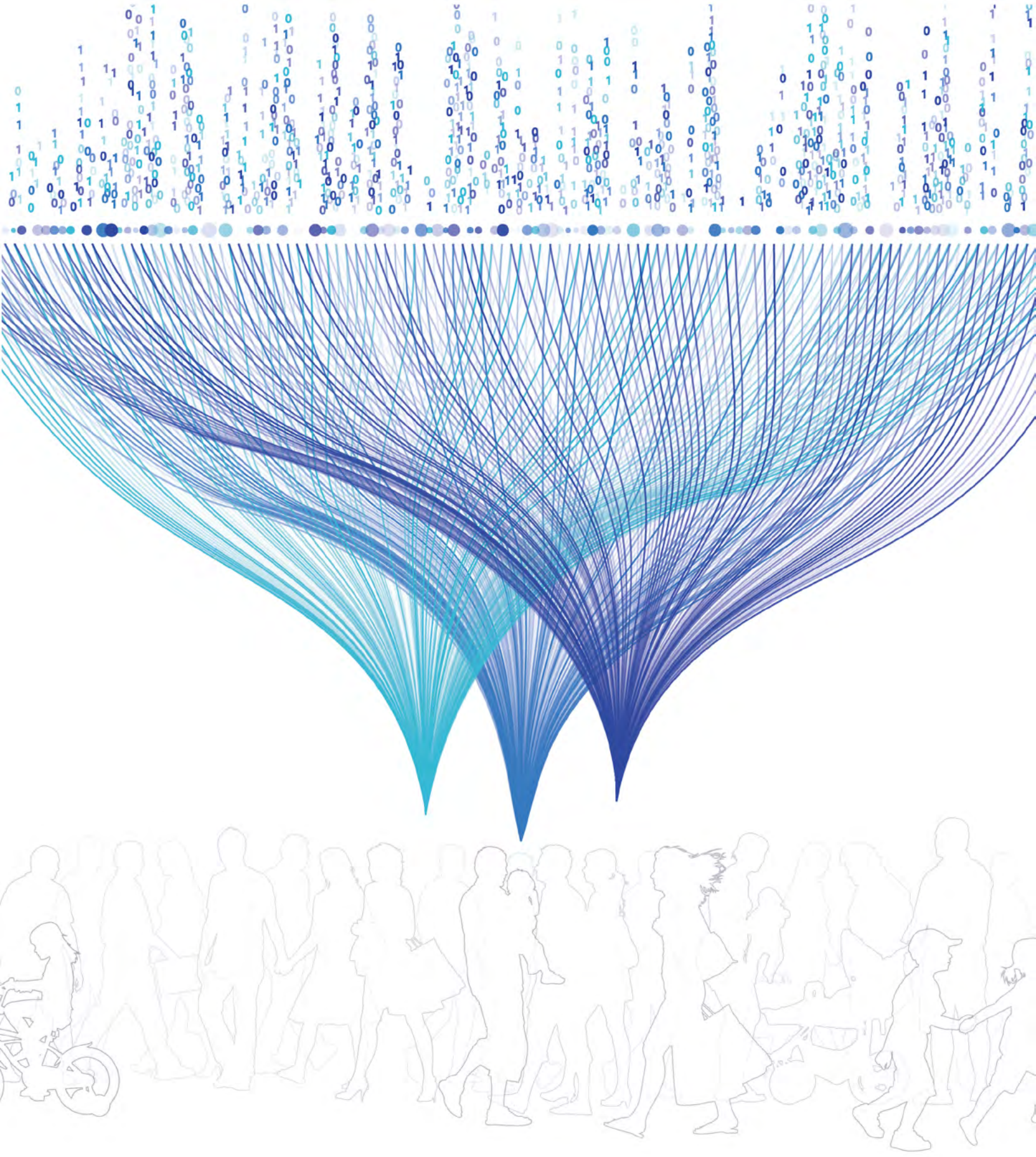
519 See Kate Park, "StealthMole Raises $7M Series A for its AI-powered Dark Web Intelligence Platform," *TechCrunch* (27 March 2024), online: https://techcrunch.com/2024/03/27/stealthmole-raises-7m-series-a-for-its-ai-powered-dark-web-intelligence-platform/.

520 See Paul John & Ashish Chauhan, "Facebook AI Helps Police to Prevent Livestreamed Suicides," *The Times of India* (15 June 2023), online: https://timesofindia.indiatimes.com/city/ahmedabad/facebook-ai-helps-police-to-prevent-livestreamed-suicides/articleshow/101007958.cms.

521 See Anthony Cuthbertson, "Indian Police Trace 3,000 Missing Children in Just Four Days Using Facial Recognition Technology," *Independent* (24 April 2018), online: https://www.independent.co.uk/tech/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html.

522 See Jared Rondeau et al, "A Deep Learning Framework for Finding Illicit Images/Videos of Children" (2022) 33:66 Machine Vision and Applications.

523 See AI for Good, "How AI is Helping Uncover Modern Slavery," *AI for Good Blog* (11 March 2021), online: https://aiforgood.itu.int/how-ai-is-helping-uncover-modern-slavery/.



LCO CDO
LAW COMMISSION OF ONTARIO
COMMISSION DU DROIT DE L'ONTARIO

2032 Ignat Kaneff Building
Osgoode Hall Law School, York University
4700 Keele Street, Toronto, Ontario, Canada M3J 1P3