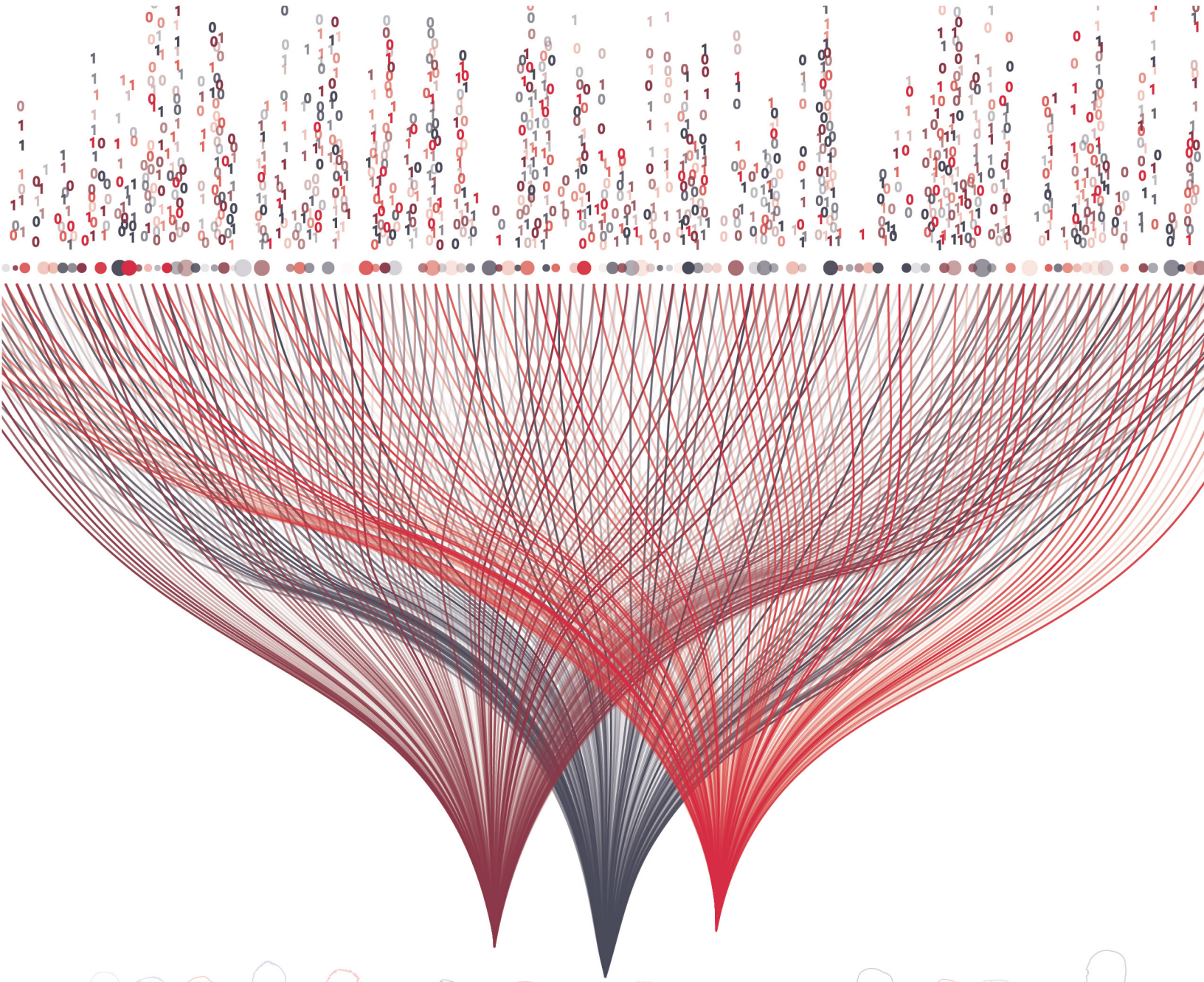


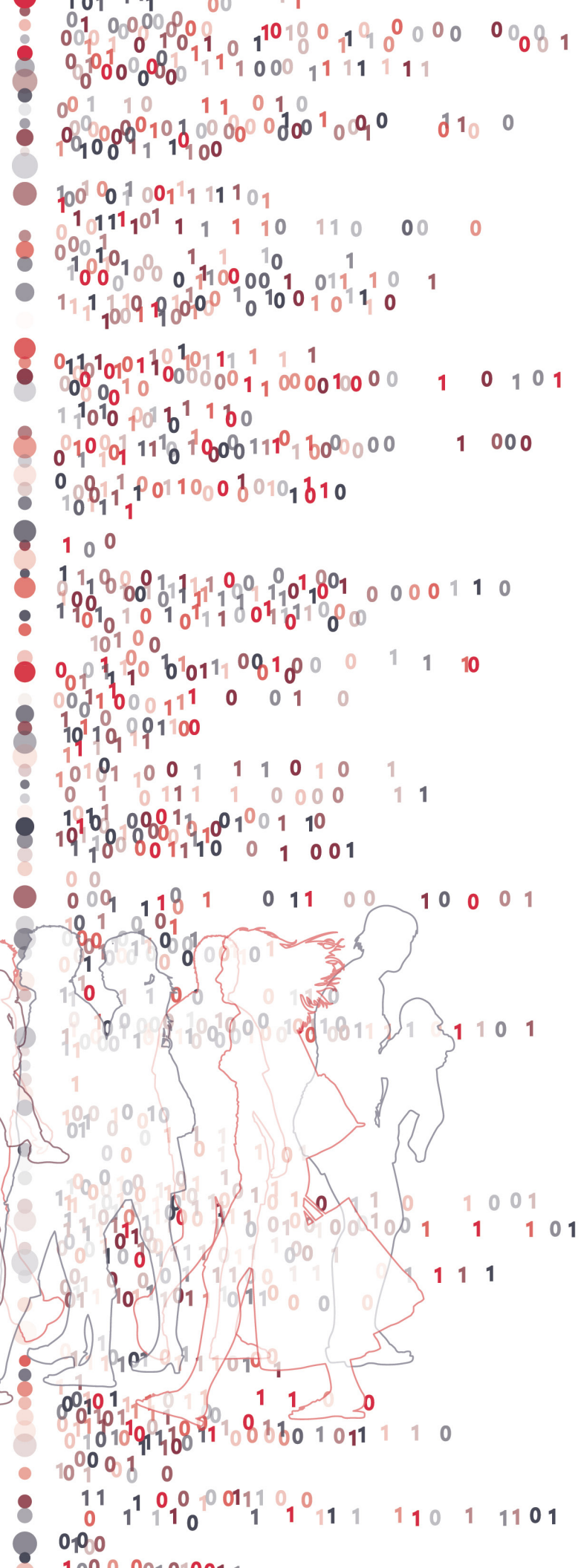
Law Commission of Ontario

AI IN CRIMINAL JUSTICE PROJECT | PAPER 5

# AI and Systemic Oversight Mechanisms in Criminal Justice

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.

## Authors

**Brenda McPhail**, Senior Technology and Policy Advisor, Information and Privacy Commissioner of Ontario
**Marcus Pratt**, Senior Policy Advisor, Legal Aid Ontario
**Jagtaran Singh**, Counsel, Ontario Human Rights Commission

## 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<br>Nye Thomas, Executive Director, LCO<br>Ryan Fritsch, Counsel, LCO |
| Paper 2 | Use of AI by Law Enforcement<br>Ryan Fritsch, Counsel, LCO |
| Paper 3 | AI and the Assessment of Risk in Bail, Sentencing, and Recidivism<br>Armando D'Andrea, Staff Lawyer, Provincial Office, Legal Aid Ontario<br>Gideon Christian, Professor of Law, Faculty of Law, University of Calgary |
| Paper 4 | AI at Trial and on Appeal<br>Paula Thompson, Strategic Initiatives, Ministry of the Attorney General<br>Eric Neubauer, Defense Counsel, Neubauer Law, and Co-Chair, Criminal Lawyers Association Technology Committee |
| Paper 5 | AI and Systemic Oversight Mechanisms in Criminal Justice.<br>Brenda McPhail, Senior Technology & Policy Advisor, Information and Privacy Commissioner of Ontario<br>Marcus Pratt, Senior Advisor, Policy Department, Legal Aid Ontario, and Chair of the LAO Test Case Committee<br>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, ***AI and Systemic Oversight Mechanisms in Criminal Justice: Paper 5 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
Twitter: @LCO_CDO
YouTube: @lawcommissionofontario8724

## Funders

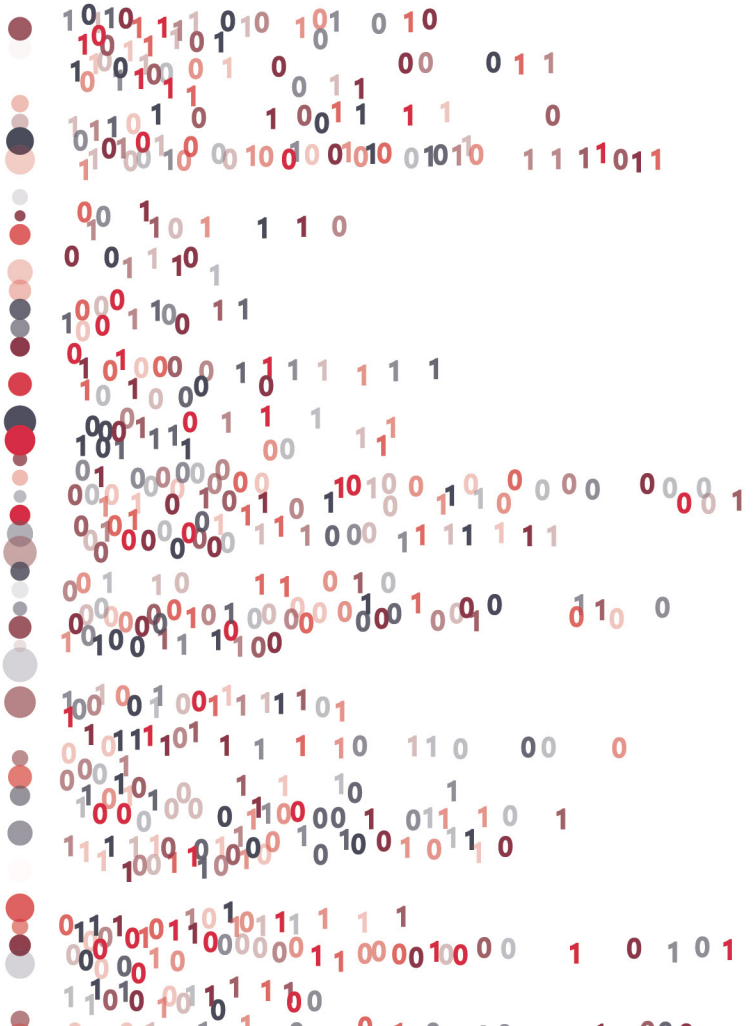
Financial support is provided by the Law Foundation of Ontario, the Law Society of Ontario, and Osgoode Hall Law School. The LCO is located at Osgoode Hall Law School in Toronto.

The Law Foundation of Ontario
*Advancing access to justice*

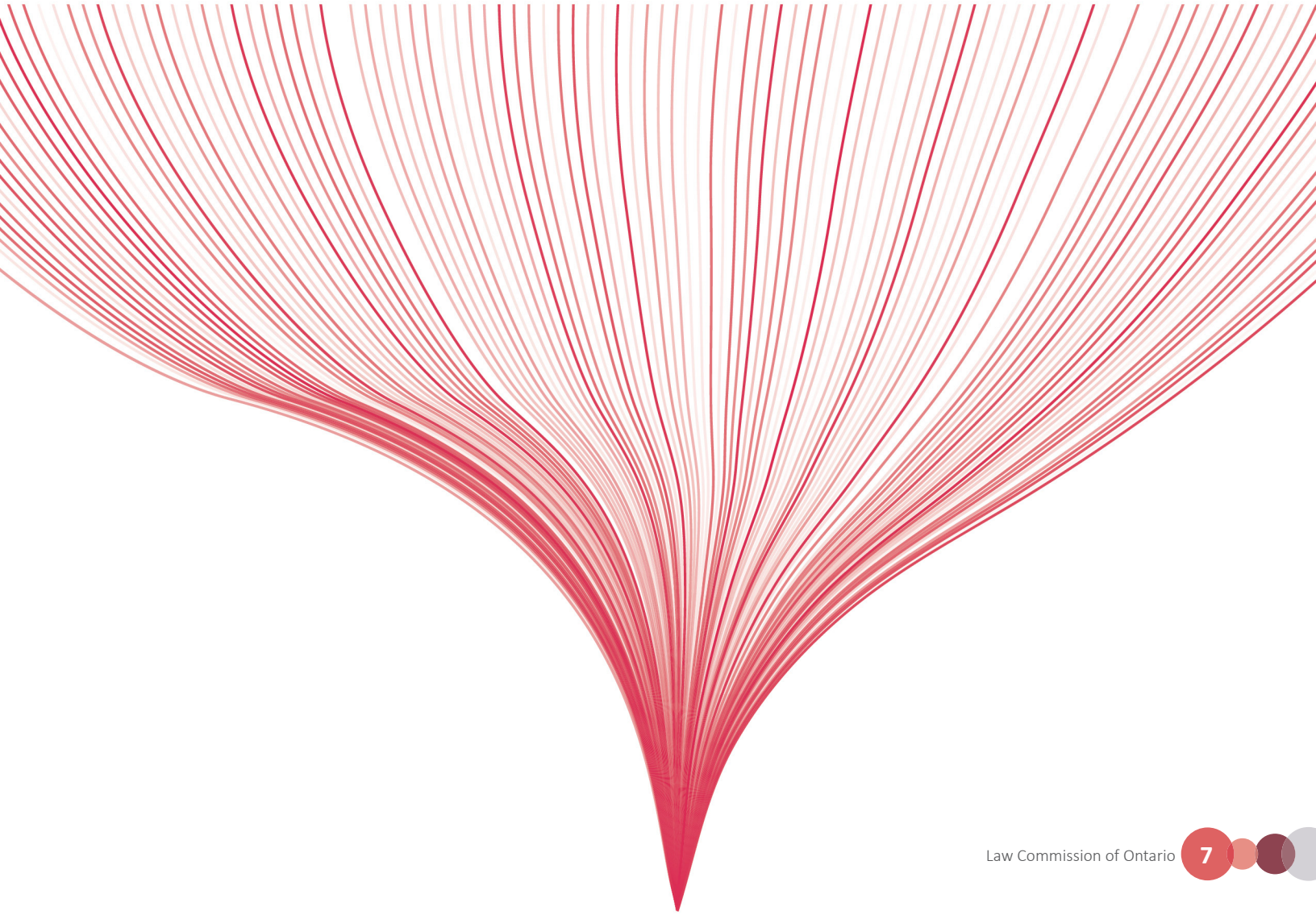
Law Society of Ontario | Barreau de l'Ontario

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 fifth of a series of five Issue Papers that comprise the project. 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 through a law and policy reform lens.

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.

### AI in Criminal Justice Case Studies.

See the LCO AI in Criminal Justice Project ***Annex B, Project Case Studies*** for a discussion based on several scenarios highlighting legislative, regulatory and practical issues with AI technology in criminal justice.

## 1.2 Executive Summary: Oversight of Artificial Intelligence in Criminal Law Proceedings

This paper assesses the institutions, processes and remedies that provide an oversight function to criminal justice proceedings. The central question in this paper is the extent to which existing oversight mechanisms are likely able to respond effectively to the foreseeable challenges of AI in a criminal justice proceeding. It is particularly relevant given a key theme of the LCO AI in Criminal Justice Project is to explore the necessity and benefit of avoiding a disconnected mess of diverging and inconsistent approaches that might govern AI across multiple criminal justice institutions and participants. This consideration is particularly critical given the inherent reticence and limitations on criminal courts to set systemic policies, the narrowness of many precedents, the expense of litigation, and the considerable lag between the introduction of a technology and a court decision about it many years later.

The discussion in this paper instead aims at a coherent, complimentary and proactive approach to governing readily foreseeable challenges with the use of AI across these institutions. It identifies and discusses ideas for additional necessary avenues for enhanced systemic oversight functions and processes, placing them in the context of leading or pending legislation and policy within and outside of Canada.

The analysis in this paper builds on the insights provided by the other papers that have identified in some detail the real dangers posed by the increasing use artificial intelligence in all aspects of the criminal law life cycle. It supplements these analyses by articulating different ways, both doctrinally and institutionally, in which there might be reason for both optimism and concern in the oversight capacity that can be provided from within criminal proceedings themselves.

An effort is made to provide some ideas on how to reform the criminal litigation model so that it can increase its capacity for oversight. Ultimately, however, the conclusion is that, as seems to be the case for jurisdictions around the globe, meaningful oversight of the use of AI cannot be left to criminal courts and criminal process alone. To ensure the meaningful, effective, efficient, and reliable ability to hold AI systems to the standards of the Canadian *Charter of Rights and Freedoms* (the *Charter*),[1] procedural fairness, evidentiary law, and criminal common law, this paper highlights how AI oversight can and must be addressed through changes to the legal, regulatory and policy frameworks that direct the operation of the criminal justice system as a whole.

The paper is structured as follows.

Section 2 discusses Canadian and global approaches to AI law and governance in relation to systemic oversight. The section begins with an analysis of AI oversight law and policy that has been introduced or adopted in Canada. This includes lessons learned from federal bill C-27, which includes the proposed *Artificial Intelligence and Data Act*; Ontario's recently enacted Bill 194, *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*; and municipal police policies including the Toronto Police Services Board "Use of AI Technology Policy."[2] Section 2 then shifts to a comparative analysis of AI oversight law and policy introduced or adopted in other leading jurisdictions. This includes the European Union *Artificial Intelligence Act* and legislation proposed in the United States, including the *Justice in Forensic Algorithms Act* and the *Public Oversight of Surveillance Technology (POST) Act*.[3]

Section 3 discusses a wide range of ways in which existing mechanisms within Ontario's criminal justice system might provide (or inform the development of) effective oversight of the use of AI tools. The issues explored here consider how existing evidentiary and procedural law established in the *Charter*, *Criminal Code* of Canada (*Criminal Code*), the *Canada Evidence Act* (CEA)[4] and common law should inform the establishment of legal, regulatory and policy standards addressing some of the most challenging aspects of AI, including:

- freedom from identification and surveillance (such as mass facial recognition);
- protection against arbitrary detention and arrest (such as predictive policing or risk assessment instruments in bail and sentencing);
- disclosure rules based on full answer and defence (such as contending with AI transparency, explainability and intellectual property assertions); and
- gatekeeping against unreliable scientific, technical opinion evidence (such as untested recommendations from AI systems).

Section 3 further considers how existing evidentiary, procedural, Criminal Code, and *Charter* law are limited in their ability to set standards in other use cases for AI, such as:

- the limits of privacy law and common law to govern the diverse uses of AI and its technological components, as well as ensuring adequate notice and disclosure of these uses;
- legal uncertainty about establishing reasonable suspicion by means of AI profiling and prediction;
- the inherent limits of criminal court litigation as a means to address unreliable scientific evidence;
- the available resources that support criminal defence bar;
- the limited impact of *Charter* remedies on systemic reforms; and
- the limits on judicial protection of constitutional rights without legislative oversight.

Section 4 engages in a comparative analysis of the role for AI oversight regulators proposed or implemented in the US, EU and private sector. This sections suggests the potential efficacy of system-wide governance through mechanisms including privacy and data controls; reflecting growing international consensus around regulatory and policy approaches including presumptive prohibition of the highest-risk uses of AI and broad transparency and disclosure obligations; the importance of an active and ongoing role for the public to participate in the consideration and review of AI technologies before they are adopted; and the efficacy and reasonable expectations associated with self-regulation and accountability.

Section 5 summarizes next steps the project will take after publication of this series of papers, and consolidates the questions raised in this paper for public consultation.

Overall, the paper makes several key findings and poses several questions for consideration as law reform proposals, including:

- Proactively developing a coherent and coordinated mix of legislative, regulatory and policy standards to effectively, consistently and predictably manage foreseeable risks with AI across the criminal justice system.
- Ensuring the high standards of fairness in criminal proceedings under the *Charter*, procedural fairness, evidence law, and criminal common law are reflected in any legislative, regulatory or policy standards for deploying AI anywhere in the criminal justice system.
- Clarifying which uses of AI technology carry sufficient risk to adopt a presumptive prohibition on their use, and determining criteria for assessment.
- Ensuring necessary supports are available within the justice system to keep state power on the use of AI in check, such as adequate support for defense counsel; test case support; and creation of an office that can assist with centralized research and expertise (perhaps similar to Legal Aid Ontario's research department for legal aid clinics).
- Reviewing the capacity and mandate of existing court oversight and order-making abilities – such as judicial authorizations for investigations – to scale-up to increased requests (and the complexity of these requests) related to AI tools, and whether this can play greater role in public transparency through, for example, annual public reporting on the number and kind of such requests and authorizations.
- Managing the risks of AI technologies through mitigation measures such as third-party independent audits of data validity, source code, and unintended outcomes; explainability requirements; metrics testing; de-biasing techniques; public and expert consultations; and public participation and reporting requirements on pre-acquisition evaluations and post-acquisition performance review.
- Ensuring oversight institutions have the needed mandate to effectively investigate misuses of AI in criminal justice, including coroner's investigations, civilian police oversight institutions, human rights mechanisms, judicial oversight systems, etc.
- Exploring the utility of an independent office of AI technology assessment to oversee the assessment and certification of AI tools; validate their efficacy and operational requirements on an ongoing basis; and facilitate system-wide transparency and reporting on the use of AI in criminal justice.
- Establishing clear legislative guidance to govern how assertions on trade secrets and intellectual property are handled in the criminal justice sector;
- Establishing clear legislative or regulatory guidance to clarify and streamline instances where law enforcement or other entities seek to procure or rely on commercially sourced data sources or third-party data sources.
- Ensuring lessons learned from the Goudge, Motherisk and other inquiries are acted on by ensuring adequate guidance or regulation on expert evidence and testimonial standards related to AI evidence and recommendations.
- Establishing mechanisms and building capacity for the public to participate meaningfully in AI assessment and consultations.

## 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 the final report.

### 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

Telephone: (416) 650-8406
Email: LawCommission@lco-cdo.org
Web page: https://www.lco-cdo.org
X/Twitter: @LCO_CDO
LinkedIn: https://linkedin.com/company/lco-cdo

### Author and Project Editors

This series of papers is edited by Nye Thomas (Executive Director) and Ryan Fritsch (Counsel) with the LCO.

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, Information & Technology Command, 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
- Associate Professor Daniel Konikoff, Department of Sociology, University of Alberta
- Rosemarie Juginovic, Office of the Chief Justice, Ontario Superior Court of Justice
- Michelina Longo, Director, External Relations, Ministry of the Solicitor General
- Jessica Mahon, 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, Ministry of the Solicitor General
- Marcus Pratt, Senior Policy Advisor, Legal Aid Ontario
- 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. AI Oversight in Canada and Elsewhere: An Applied Comparison

This section examines how different Canadian jurisdictions (federal, provincial, and municipal) have begun to regulate AI tools. It also provides examples of prominent, relevant attempts in foreign jurisdictions including the European and the United States.

The rationales for regulating AI are extensively documented in the LCO report *Regulating AI: Critical Issues and Choices*. As they note, AI systems "raise significant, novel and systemic legal risks that have not—and cannot—be comprehensively addressed through individual litigation, best practices, existing or piecemeal legislation."[5] Their position is one widely shared internationally, as demonstrated by global activity in AI governance. As several professors note in a recent article examining AI governance initiatives in Canada, "the governance of artificial intelligence (AI) systems has quickly become a strategic necessity for governments around the world, with more than 40 national governments having adopted AI strategies as of 2022," many of which include some form of regulation.[6]

These efforts reflect a mix of approaches. Some adopt laws of general application, such as Canada's proposed (and presently prorogued, at the time of writing) *Artificial Intelligence and Data Act*. Others adopt sector specific regulations, such as the proposed *Justice in Forensic Algorithms Act* in the United States. Still others aim to limit different types of AI-enabled technology, such as New York City's *Public Oversight of Surveillance Technology (POST) Ac*t. The scope potential forms of AI regulation may take perhaps mirrors the potential scope of the technology, itself. However, each raises useful questions that can help guide an exploration of the way in which AI relevant to how the criminal justice system might be regulated in Canada.

## 2.1 Canada: Bill C 27, the *Artificial Intelligence and Data Act*

Legislative oversight of AI in Canada is currently being considered before parliament in the form of Bill C-27. The Bill, originally tabled in June 2022, is among the many pieces of legislation caught in a prorogued parliament at the time of writing.[7] Although not enacted, Bill C-27 is nevertheless indicative of approaches and issues government may contend with in future AI legislation and presents a helpful case study for discussion.

As introduced, Bill C-27 is indicative of the manifold complexity in regulating AI technology of broad and general application. In fact, Bill C-27 is a tripartite bill with three distinct pieces of legislation:

- Part 1 is the *Consumer Privacy Protection Act* (CPPA), an "Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in the course of commercial activities."
- Part 2 is the *Personal Information and Data Protection Tribunal Act* (PIDPTA), an "An Act to establish the Personal Information and Data Protection Tribunal."
- Part 3 is the *Artificial Intelligence and Data Act* (AIDA), the first Canadian federal legislation "respecting artificial intelligence systems and data used in artificial intelligence systems."

As stated in its preamble, Bill C-27 is meant to "modernize Canada's legislative framework so that it is suited to the digital age."[8]

Unfortunately, for those concerned with the implications of artificial intelligence for criminal law, the Act would appear to have limited application. Understanding AIDA's deficiencies is instructive, not least because at least some of the specific criticisms that have been leveled against AIDA as an oversight model for the use of AI would also apply to the oversight offered by the criminal law process alone.

From the access to justice community, a rough consensus has emerged on the deficiencies of C-27 generally and AIDA specifically. In broad strokes, the criticism can be grouped under the following headings.

### A. No Oversight of Government and Law Enforcement Use of AI

AIDA intends to establish common requirements for the design, development, and use of "high impact" AI systems and to prohibit conduct that might result in serious harm to individuals. But it primarily governs private entities who develop AI systems, not government. Furthermore, AIDA specifically excludes government institutions, products, services or activities which fall 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, or other heads of federal or provincial agencies that might be prescribed by regulation (and yet undefined).[9]

AIDA, however, is of (speculative) relevance to the use of AI by law enforcement. In response to criticism that AIDA fails to define what "high impact systems" are, the responsible Minister of Innovation, Science and Economic Development proposed a series of amendments to identify such systems. Among others, the amendments define:

- "the use of artificial intelligence systems by a court or administrative body in making a determination in respect of an individual who is a party to proceedings before the court or administrative body;" and
- "the use of artificial intelligence systems 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."[10]

If enacted, these proposed amendments would seem to bring some AI tools that might be procured from private sector vendors and used in the criminal justice system into scope of the bill. However, as noted in the submission of the Canadian Bar Association to the legislative committee reviewing C-27, the general exclusion of public bodies from the jurisdiction of the Bill creates a real risk that human rights violations resulting from the state use of AI – such as in refugee determinations for example – will go "unchecked" due to the difficulties in seeking oversight of these rights violations by way of judicial review.[11]

Critics have pointed out that by creating a private-public distinction for oversight, AIDA underestimates the overlap between private bodies that produce and develop AI systems and the government bodies (and police) who make use of them.

The BC Civil Liberties Association (BCCLA) notes the boundary between commercial and state surveillance is now simply too "porous" to separate the legal regulation of the private and the public sphere.[12] While proposed amendments to C-27 would seem to bring various public sector uses within scope of AIDA – including ones of key concern to the criminal justice community – absent such amendment, this separation of the private from the public would means that the legislation will be unable address the rising use of, "commercially sourced data and technologies by law enforcement."[13]

## B. Ease of disclosure of private information to law enforcement

AI systems require data for training, and as system inputs. As noted by Kate Robertson in her comprehensive submission to the INDU Committee on Bill C-27, the CPPA holds the potential to significantly enhance the ability of private sector companies to collect personal information.[14] This happens in two ways. The CPPA, in section 44, includes text largely taken from s. 7.3 of PIPEDA that allows disclosure without knowledge or consent for law enforcement purposes once "lawful authority" is identified, a provision that both pre-and post-*Spencer* has been a source of concern and contestation.[15] As Robertson points out, these "permissive" controls, "drafted at a time when more traditional policing activities were contemplated…could, troublingly, now be repurposed to exempt contemporary APTs [algorithmic policing technologies] from much needed privacy controls, including clear limits defined by necessity and proportionality."[16]

Secondly, new consent exceptions for "legitimate interests" of businesses in the CPPA (s. 18.3) allow for private sector vendors to collect personal information, again, without knowledge or consent, so long as the organisation has a legitimate interest in the information and its collection will not have an adverse effect, seemingly opening a door for use of such information in training AI tools, including tools for sale to law enforcement bodies.[17] Robertson's assessment is that the bill "appears to operate as a green or yellow light at best, to all forms of commercially-developed APTs" without the needed privacy controls.[18]

## C. Oversight Provisions in C-27 Do Not Provide Effective Access to Remedies

The CPPA is the bill that turns on the tap for data to flow to AI applications, with its deliberate exceptions raising the risk that the Privacy Commissioner will have no effective means to make findings or recommend administrative monetary penalties (AMPs) against companies that inappropriately use personal information for creating or training commercial AI tools, despite the addition of much-needed binding order powers for the Commissioner in the CPPA. A brief consideration of the nature and scope of information that would be required to train a tool to assess pretrial release or recidivism risks, for example, in tools for use in the court system, highlights the real need to access to remedies if such tools were to inappropriately collect or use sensitive personal information.

Of particular relevance in the context of AI tools, section 18, the legitimate interest exception, and section 39, which facilitates sharing of de-identified information with public bodies for socially beneficial purposes, are excluded from those sections whose violation can give rise to AMPs. There is also a concern that the bill anticipates that findings of the OPC can be appealed to a new Data Protection Tribunal, created in part 2 of Bill C-27, the *Personal Information and Data Protection Tribunal Act*.[19] The tribunal also has jurisdiction in respect of the imposition of penalties under section 95 of the CPPA. Many organizations have criticized the tribunals' lack of independence because it will be appointed by the Minister, rather than serving as "an independent, arms-length public tribunal with full investigatory and enforcement powers."[20]

## D. Bill C-27 is based on a limited view of privacy rights

A number of non-governmental institutions have decried the limited view of rights protection that is provided in Bill C-27, including AIDA which itself does not contain an unencumbered statement recognizing the fundamental right to privacy, despite its role in regulating a data-driven set of technologies. The Office of the Privacy Commissioner points out that while a right to privacy often work to support commercial innovation, the legislation fails to clearly state that in those "rare circumstances where the two are in an unavoidable conflict, privacy rights should prevail."[21]

A different kind of criticism has pointed to the exclusively individualistic view of harm that the legislation seeks to regulate. AIDA focuses on biased outputs, and defines harms as individual and quantifiable, relating to physical or psychological harm, property damage or economic loss. However, there are other larger "group" or "societal" harms that are at risk with artificial intelligence that seem to be beyond the purview of this legislative regime. These harms include loss of collective privacy, violations of principles of Indigenous data sovereignty, and the reproduction of pre-existing biases and other forms of discrimination.[22] As pointed out by Amnesty International in its submissions, these broader forms of harm are "now widely recognized but ignored under this Act."[23]

Assuming the amended definition of a "high impact" system will include AI tools used in courts or policing contexts, AIDA does place accountability, monitoring, and transparency requirements on persons responsible for, or persons making available, a high-impact system, which is a positive step.

## E. AIDA does not include independent oversight

Oversight in AIDA vests not in an independent, arms-length body but in a senior official of ISED, a new Artificial Intelligence and Data Commissioner, who will "assist" the Minister in the administration and enforcement of the Act (AIDA s. 33.1). Placing oversight in the same Ministry and under the same Minister responsible for promoting economic development and fostering AI innovation raises questions about how rigorous or effective it might ultimately be in enforcing those requirements.

In addition to the gaps created by these failings in the bill, there is a larger question raised by AIDA as currently drafted, reading in the Minister's amendments. It seems unlikely that any significant debate will arise as to whether uses of AI by courts or administrative bodies to make determinations regarding individuals should be presumptively high impact AI systems. Given the significant personal and social consequences of such systems, and the controversies surrounding many of them in other jurisdictions, it seems clear that such systems should never be used without appropriate safeguards in law and policy (if they are deemed fit for use at all, a larger question).[24] The question remains however, as to whether other uses of AI in the criminal justice system such as those enumerated in the introductory paper of this series (including 'helping' self-represented litigants, testing testimony, or even drafting pleadings) might in some cases or some ways rise to the level of high risk? Errors that have the potential to influence judges, adjudicators, or juries in legal proceedings all carry human consequences. If such systems are judged not to rise to the level of high risk, then are lower levels of risk in a criminal proceeding acceptable if the trade-off is convenience or efficiency?

### F. Consultation Questions

1) Does Canada's approach to a risk-based framework that only captures and mitigates risks considered 'high' meet the needs of the justice system?

2) AIDA does not introduce prohibitions on technologies that are so high risk as to be unjustifiable for use in a democracy or under our *Charter*. Should it do so, and what might those technologies be in relation to the criminal justice system writ large?

## 2.2 Ontario: Bill 194, the *Strengthening Cyber Security and Building Trust in the Public Sector Act*

Ontario introduced Bill 194, the *Strengthening Cyber Security and Building Trust in the Public Sector Act*, 2024, on May 13th 2024 and was granted Royal Assent on November 25th 2024.

The first schedule of the Act creates requirements for cyber security measures and introduces provisions to govern the use of artificial intelligence systems for public sector entities in Ontario. The second schedule amends the Ontario *Freedom of Information and Protection of Privacy Act* to provide for privacy impact assessment, mandatory breach reporting and stronger enforcement. The focus of this report is on the provisions relating to AI.

There is no doubt that Ontario and Ontarians can benefit from comprehensive public sector AI legislation and regulations. However, many critics including the LCO have noted in written consultation submissions that Bill 194 falls short of public expectations and fails to integrate internationally emerging benchmarks for such legislation.[25]

Section 4.1 and 4.2 below go into greater detail about limitations with Bill 194, particularly in relation to fostering systemic oversight of criminal justice.

For introductory purposes, however, there are three specific areas where the AI provisions in Bill 194 fall short in relation to the criminal justice system.

### A. The bill fails to enshrine core principles in the legislation

Bill 194 is a skeleton on which to hang regulations, rather than a well-fleshed out approach to AI governance. There is no specificity or detail, lacking even basic provisions to ensure that public sector AI use is, as the LCO notes in their submission regarding the bill, "beneficial, lawful, and accountable."[26] The standard argument for this "put it all in the regs" approach is the fast pace of change in the AI landscape, but other jurisdictions, including the EU, the US, and the Canadian federal government (post amendments) have all passed or proposed more substantive legislation classifying risk, centering human rights, and mandating procedural fairness.

As Linder, McPhail and Chatwin argue in their submission on this bill, leaving everything to regulation is problematic because regulation, by definition, provides the rules and procedures to ensure the law is implemented and enforced as intended.[27] If the specific intention of the legislature, our democratically elected representatives, is vague or subject to debate, then the regulations may fail to uphold the legislation's intent.

Further, the regulatory process is far more unpredictable and unaccountable than the legislative process for members of the public, leaving consultation and public transparency to be included at the will of the responsible Ministry. Clear, democratically debatable law is better than law via regulatory frameworks from the perspective of public accountability.

Even as a guiding framework for regulations, the bill arguably misses the mark. The absence of required ethical and operational principles is particularly notable considering the good work that Ontario has done in developing its own Trustworthy AI Framework, which could have reasonably informed the principled core of an Ontario AI law. Human rights protections, procedural fairness, and explainability are all principles at the core of the criminal justice system, and the court and tribunal system, that must be part of any law that governs the tools used in that system and the absence of such principles risks undermining public trust. Core principles of validity and reliability, safety, privacy protection, transparency, accountability are similarly foundational and necessary.

## B. The bill fails to mention the need to protect human rights, beyond privacy

The Ontario Human Rights Commission highlights in their submission on the bill the need to recognize the overarching importance of upholding human rights in Bill 194. It is widely accepted that one reason that AI governance initiatives around the world are proliferating is the risk that AI tools, badly conceived, trained, or implemented, have the potential to introduce, embed or exacerbate discrimination into tools and the practices that use them. This risk is particularly important to mitigate in the context of public services, including all elements of the justice system. Recognizing in the text of the bill that the full suite of human rights, beyond privacy, must form the core of a governance framework for AI is necessary if the bill is to provide appropriate protections for Ontarians. Whether in policing, courts, law offices or other loci of the justice system, constitutionally protected human rights are necessarily a core consideration and AI tools for those systems should be reviewed through a rights lens.

## C. The bill leaves it unclear as to the extent to which police and policing, courts and tribunals will be or can be included in proposed regulations

Bill 194 specifies in s. 5 (1) that the AI regulations will apply **"**to such public sector entities as may be prescribed for the purposes of this section if they use or intend to use an artificial intelligence system in prescribed circumstances." Public service entities are defined as institutions within the meaning of subsection 2 (1) of either Ontario's *Freedom of Information and Protection of Privacy Act* (FIPPA) or the Municipal *Freedom of Information and Protection of Privacy Act* (MFIPPA). While it is clear that police service boards are defined as institutions under section 2(1) of MFIPPA, it is less clear as to whether police services themselves might additionally be prescribed. Similarly, courts or tribunals are not listed entities.

This is a significant omission, given the impact of these bodies on Ontarians. Police forces across the province are increasingly adopting AI tools, or tools that include or carry AI analytics, including drones, facial recognition and predictive analytical programs, and some have explicitly referenced a lack of provincial guidance when doing so.[28]

This concern is shared by regulators. With regards to facial recognition for example, the federal Privacy Commissioner and his provincial and territorial counterparts have issued joint guidance for police that explicitly highlights the inadequacy of current laws, stating explicitly at the outset of their joint guidance document that they "are of the opinion that the current legislative context for police use of FR is insufficient" and that "In the absence of a comprehensive legal framework, there remains significant uncertainty about the circumstances in which FR use by police is lawful."[29]

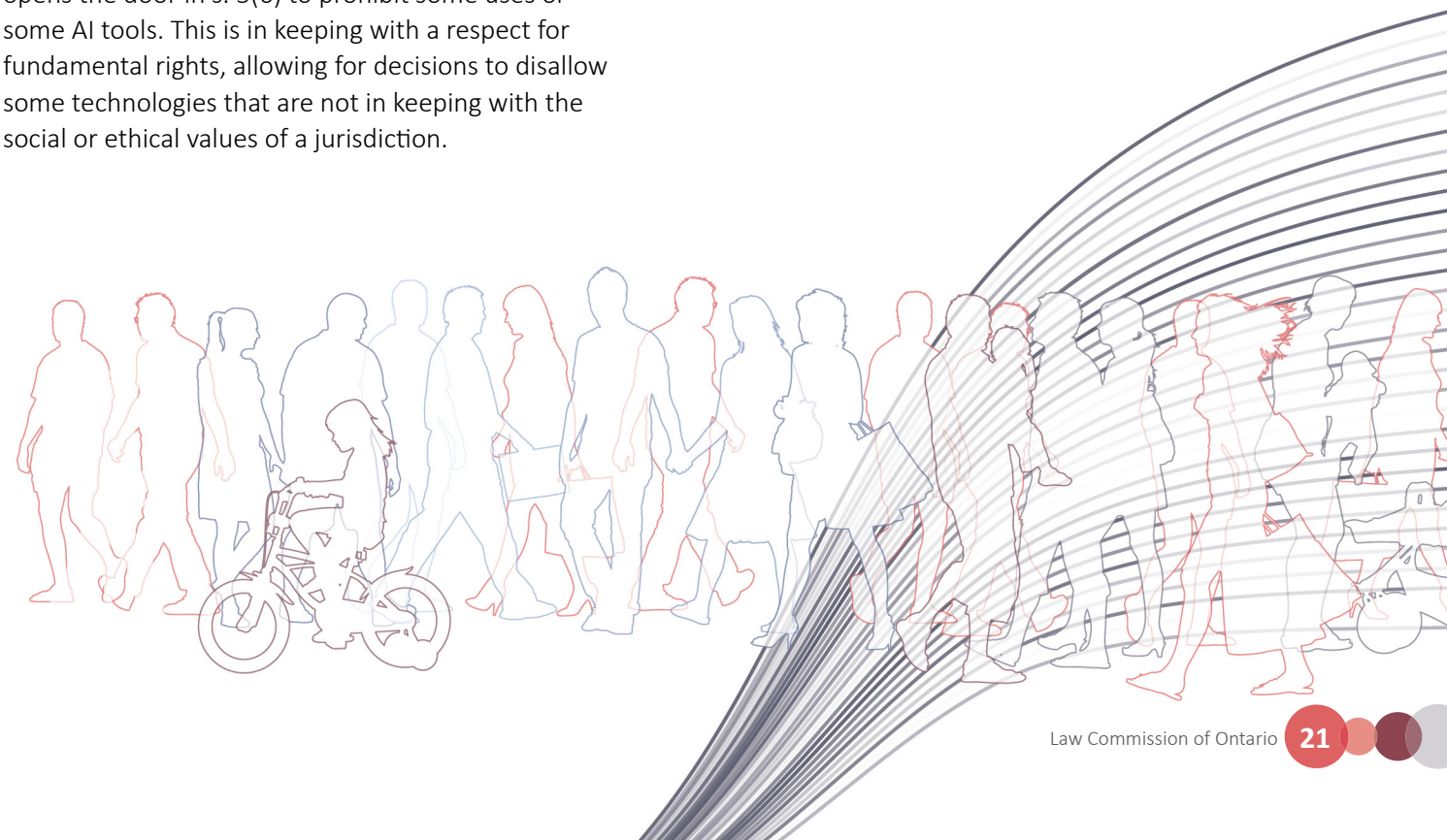
There are clear reasons for including police in a law governing public sector use of AI. When it comes to the courts, many, including the Federal Court, and Courts in Alberta, Newfoundland and Labrador, Manitoba, Quebec and the Yukon have issued practice directions regarding the use of generative artificial intelligence tools, Ontario has not.[30] Courts in other jurisdictions are, and have been, using AI tools for bail eligibility determinations, recidivism calculations, and other processes, and there is active interest in such tools in Canada.[31]

There are good reasons for ensuring that operational policing procedure is independent of political bodies — it is for this reason that police service boards' remit is confined to policy, while daily operational procedure is the domain of police services. However, this demarcation is neither unambiguous or undisputed.[32] There are precedents for direct regulation that legislate operational aspects of policing in publicly significant and narrowly targeted areas such as data collection and use of force where the 'paper wall' between state and law enforcement is permeable, and it is worth public debate regarding whether AI policy is another such area where not just police boards, but also police forces, should be subject to reasonable legislated limits set by democratically elected MPPs. This is particularly the case in that Bill 194 specifically opens the door in s. 5(6) to prohibit some uses or some AI tools. This is in keeping with a respect for fundamental rights, allowing for decisions to disallow some technologies that are not in keeping with the social or ethical values of a jurisdiction.

The EU AI Act also takes this approach, with Article 5 codifying a list of prohibited AI practices, including subliminal techniques for behavioural manipulation, social credit systems, AI systems that create or expand facial recognition databases through untargeted scraping of images, and systems that assess the likelihood of persons committing a criminal offense based solely on profiling or personality assessments, as being too high risk for legitimate use. The latter two are of direct relevance to criminal justice.

### D. The bill talks about risk but does not explicitly require a risk-based approach to AI assessment

Many AI regulatory regimes, existing or in progress, take a risk-based approach, with rules and requirements for organisations creating or implementing an AI system becoming more stringent as the risk of harms to individuals or groups increases. The federal AIDA takes this approach, as does the Toronto Police Service Board AI policy; internationally, the EU *Artificial Intelligence Act* and the NIST "AI Risk Management Framework" are prominent examples of the approach.[33] Harmonizing Ontario's approach with other jurisdictions would be a reasonable approach.



### E. Consultation Questions

**3)** It is clear that Ontario Bill 194 should identify policing, courts, corrections, and other criminal justice sector entities as prescribed "public sector entities" in Bill 194 that use AI. In that case:

- Should this include related tribunals, for example, Criminal Injuries Compensation Board? Victims / Witness Assistance Programs?
- Should this include court support programs, such as Community Diversion programs?
- Are there exceptions that should be considered? What criteria should be developed or specific institutions / functions identified for exceptions? (ex: national security? Others?)

**4)** To achieve "accountability frameworks" under Bill 194 in criminal justice, should Bill 194 include a **provincially mandated impact assessment** that addresses privacy, human rights, and procedural fairness and provides assurances about how an AI system will comply with other legal obligations?

- Should assessment along these lines be mandated?
- What are the kinds of risks that should be included to develop a comprehensive and consistent criteria for assessments?
- What mechanisms are necessary to ensure that this is being used consistently, and reported consistently?

**5)** Bill 194 provides for the possibility that some uses of AI may be prohibited by regulation. What technologies relevant to the criminal justice system might carry sufficient risk to make a prohibition on their use appropriate?

## 2.3 Toronto Police Service Board "Use of Artificial Intelligence Technology" Policy

The Toronto Police Services Board (TPSB) approved their policy entitled "Use of Artificial Intelligence Technology" on February 28, 2022 following a period of extensive public consultation. The policy "establishes governance for the use of new and/or enhanced Artificial Intelligence (AI) technology, and for previously approved AI technology that will be used for novel purposes or circumstances" and further "establishes an assessment and accountability framework regarding the acquisition and use of AI technology."[34]

TPSB was a pioneer in Canada with this policy; as they noted in the background notes provided with their consultation, it was the first time a Canadian Police Board or Commission had created such a policy.[35] It is also an experiment in self-regulation, one that deserves scrutiny not just in terms of its content, but even more in terms of its effectiveness given that codes of conduct and internally-established risk mitigation measures and self-written plans and system descriptions form a core part of the compliance environment created by AIDA.[36]

The policy establishes a series of core principles to guide the acquisition and use of AI technology by the Toronto police service: legality, fairness, reliability, justifiability, personal accountability, organisational accountability, transparency, privacy and meaningful engagement. It takes a risk-based approach, identifying five risk levels from Extreme risk technologies, which may not be considered for adoption, through high, moderate, low and minimal risk. Mitigation levels vary for each risk category.

Examples of high-risk technologies include:

- where training data is known or thought to be of poor quality or carry bias
- applications which link biometrics to personal information, or
- where the proposed system could be used to assist in the identification of individuals for the purpose of their arrest, detention or questioning.[37]

The policy requires assessments to be undertaken prior to the acquisition of new AI technologies, establishes reporting obligations to the Board, provides for a public complaint mechanism and establishes a process of continuous review of high risk (every two years) and moderate risk (every five years) to assess its effectiveness, ongoing utility, and to ensure its use remains in the scope of its original approved purpose.

In January 2024, an "Update on the Implementation of the Board's Policy on Use of Artificial Intelligence Technology" was presented to the Board and discussed. The report, and a pointed published response to it by the Information and Privacy Commissioner of Ontario, provide an interesting illustration of the promise and pitfalls of AI governance through self-developed policy instruments.

The report identified five AI systems used by the Toronto Police Service since the adoption of the policy. One, a facial recognition program that is used on the internal mugshot database, was identified as high-risk. Four other systems were classified as low-risk:

- an automated fingerprint identification system
- two automated license plate recognition systems, and
- the BriefCam system which is a tool for rapid video review and search which can include face recognition.[38]

In her letter to the TPS, Commissioner Kosseim disputed the classification of the low-risk systems. The Commissioner correctly pointed out that all four of these tools might be used to assist in identifying individuals for purposes of arrest, detention or questioning, one of the criteria used in the policy to define a high impact system, and that the fingerprint recognition system further linked a biometric to personal information. Either could result in an individual being detained, questioned, or jailed, all significantly impactful events.

It is unclear to an external observer what impact the Commissioner's intervention had in the TPSB process. What is clearer, however, is the gap the exchange highlights, between mechanisms for transparency provided in the policy, and mechanisms for public accountability for adherence to the policy. While the transparency provisions of the policy did serve to allow the public, and Ontario's privacy regulator, to question the operation of the policy and the accuracy of the assessments it required, the ability of the public to challenge such assessments that carry real consequences for individuals in contact with police appears limited. This shortcoming is one to consider with regards to self-regulation and 'soft law' approaches to AI use, especially in sensitive sectors such as the criminal justice system.

### A. Consultation Questions

**6)** Under what circumstances in the criminal justice system might oversight be adequately achieved through self-directed and self-enforced policy? Is it possible to embed sufficiently meaningful accountability measures into such instruments for use in sensitive sectors?

**7)** In light of the questions about the effectiveness of the TPSB self-regulation, how might Ontario's Bill 194 address police use of AI technologies?

- Should regulations under Bill 194 provide for oversight, an independent complaints process, or take other measures?
- Might the risk categories and criteria that define them, as identified in the TPSB policy be enshrined in regulation and given the force of law?
- Are those systems identified as extreme risk in the TPSB policy appropriate candidates for prohibitions under Bill 194?

## 2.4 International Approaches to AI Oversight

### A. The EU: *AI Act* and Related Directives

In the face of the oversight deficiencies of the current Canadian legislative landscape, it is worth looking elsewhere to ascertain whether other jurisdictions have made more complete efforts to provide oversight of AI in criminal law.

Note: sections 4.1 and 4.2 below provide additional detail about the EU AIA, and specifically in relation to systemic oversight of criminal justice.

The European Union's efforts in AI regulation provide a good example of what has been called, the "Brussels effect" whereby the EU initiatives became a model for other jurisdictions.[39] There is certainly some of that effect in the oversight of AI in criminal law. At the same time, a closer analysis suggests limitations to its approach similar to those articulated with respect to Bill C-27.[40]

The leading piece of AI legislation in the EU is the *Artificial Intelligence Act* (EU AIA).[41] It began phasing into force in August 2024, with operative sections coming into force through 2027.[42] It is a substantial piece of legislation, running to several hundred pages when reading both the articles and explanatory recitals.

The LCO AI in Criminal Justice Project *Paper 1: Introduction and Summary* provides a helpful overview of the EU AIA.

Briefly, for the purposes of understanding the approach of the EU AIA model for systemic oversight of criminal justice, the following two points are emphasized.

First: the EU AIA creates a comprehensive regulatory scheme that mandates a role for several independent investigatory, oversight, auditing, reporting, and assessment and certification bodies, with various of these functions and authorities either centralized in the European Commission or delegated to member states.[43]

Second: the EU AIA aims to manage AI use by imposing various oversight conditions based on assessment of risk, with AI technologies occupying a spectrum from low risk to high risk. The centrepiece of the EU AIA risk spectrum includes a presumptive ban on AI systems categorised as "prohibited," these being the highest risk systems. These systems are defined as including:

- systems to assess and predict the risk of individuals committing criminal offenses based solely on profiling;
- the use of systems for social scoring, a process of assigning people "scores" based on observations of behaviours considered positive or negative (for instance, lowering scores for littering or jaywalking);
- compiling facial recognition databases by scraping images from online or from CCTV footage;
- real time remote biometric identification; and
- biometric categorisation systems that infer sensitive attributes such as race or sexual orientation.

However, there are exceptions for law enforcement for some use of real-time systems in serious cases, and some use of FRT for "post" remote biometric identification systems after court approval. In some of these circumstances, additional procedural and transparency requirements must be met, such as obtaining a judicial warrant for use and compiling both requests and orders into published databases.[44]

In addition to the recently passed EU AI Act, there have for some years been measures in place to provide some degree of AI oversight relevant to criminal law matters. The EU's General Data Protection Regulation (GDPR 2018) and the Law Enforcement Directive (LED 2016) jointly prohibit decisions arising "solely" from automated processing where such decisions produce "adverse legal effects on an individual.[45]

In the case of "special categories" of personal data, automated decision-making is prohibited unless "suitable measures to safeguard the data subject's rights and freedoms and legitimate interests" are in place. Article 9 of the GPRD describes these special categories as:

> "Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex."[46]

Most specifically, the use of these special categories for profiling is prohibited if it results in discrimination against natural individuals.

## B. Oversight limited to use of AI technology, not its development

Both the GDPR and the LED are limited to prohibiting the sole use of automated processing for decision-making with significant adverse effects on individuals. In this way, as noted by Fair Trials, the laws regulate the "impact of decisions made through automated processing, but not the AI systems themselves."[47] This separation of AI development from its use in the criminal process is similar to the private/public split identified with respect to the limited scope of Bill C-27. The proposed oversight mechanism fails to deal with the "main human rights challenges of AI", which are found in the design, training and technology used in AI systems.[48]

Moreover, a focus on the end-use of AI by considering whether a decision was solely based on an automated process at the expense of human decision-making, underestimates the impact of AI technology on any decision-making processes. As various studies show, the introduction of AI as even just a way to augment decision-making creates an immediate risk that human decision makers will simply follow the information that AI provides in place of their own reasoning.[49] In the absence of further regulatory guidance of how to limit the use of automated processing information, the drift to "de facto" over-reliance on automated processes may be impossible to resist. [50]

## C. Absence of specific criminal oversight safeguards

In terms of its application, EU nations may effectively opt out of these directives, and lawfully provide for automated decision-making so long as there are appropriate safeguards for the rights and freedoms of the data subject, at least the right to obtain human intervention.[51] At the same time, an absolute prohibition appears to be in place against discriminatory profiling/social scoring under the EU AIA as described above.

In addition, the EU's recognition of privacy rights (or the rights of "individual data" subjects) within the Law Enforcement Directive is limited by the need to "avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties," as well as the need to "protect the rights and freedoms of others."[52]

The apparent breadth of exceptions available to nations to, for example, establish that safeguards are in place, or that privacy rights must give way to law enforcement needs, suggests further work is required before a definitive statement can be made about the level of oversight governed by these Directives.

A recent analysis the impact of the EU Directives on criminal law questions "the missed (?) and eagerly awaited opportunities for the EU regulator."[53] The conclusion was that "data protection rules in place do not compensate for the lack of specific criminal procedural safeguards."[54]

The discussion paper provided by *Fair Trials* made much the same point:

> It is significant that EU laws emphasise the need for human rights safeguards, and the need to ensure the possibility of human interventions, but neither of these concepts have yet been adequately defined and there is currently no authoritative guidance on the practical safeguards that need to be in place.[55]

## D. United States: Proposed *Justice in Forensic Algorithms Act*

### The problem of trade secrets and disclosure in US law

The *Justice in Forensic Algorithms Act* has been tabled on at least two separate occasions before the United States Congress without being passed into law. It is now before the Congress again.[56] In many ways, the proposed legislation responds to a particular gap in the due process rights of defendants in the United States. Under American law, it is at least an open question, where the prosecution is relying artificial intelligence, or other forms of machine-generated evidence, as to whether the defendant can obtain the details of the workings of the underling technology where private companies hold that information. In these circumstances, U.S. courts have held that the intellectual property rights of the private company in that technology may supersede the due process rights of defendant to that information.[57]

The importance of propriety, or trade secret, rights of private companies over the rights of accused persons has played itself out in a number of different criminal law contexts. The examples include:

- refusing access to a defendant of an algorithm risk testing technique on sentencing;[58]
- denying to a "death penalty" defendant the source code for a cybernetics software program that identified his DNA found in a critical piece of evidence;[59] and
- precluding a defendant from challenging a search warrant by information about the reliability of the software program that identified him as being in possession of child pornography.[60]

There are no equivalent trade secrets rights for third parties under the governing rules of disclosure in Canadian criminal law proceedings.[61] At the same time, these results speak to a real risk by which the increasing private development of techniques of artificial intelligence that are being relied on by law enforcement may, without further legislative initiatives, undermine the due process rights of accused persons. It is not a risk that Canada is immune from and, as noted above, Bill C-27 does not engage with this risk, and instead arguably exacerbates it.

To its credit, the *Justice in Forensic Algorithms Act* addresses that risk directly through three central provisions by which the *Act*:

- Prohibits the use of trade secrets privileges to prevent the defense from accessing source code and "other information about software used to process, analyze, and interpret evidence in criminal proceedings;"
- Directs the National Institute of Standards of Technology (NIST) to establish both "Computational Forensic Algorithm Testing Standards" and a "Computational Forensic Algorithm Testing Program,"[62] and
- Requires federal law enforcement to comply with these standards and testing requirements when using forensic algorithms.[63]

By way of background, the NIST is an independent public agency founded in 1901 as part of the US Department of Commerce. It provides "technology, measures and standards" for a range of products and services from smart electric power grids to computer chips. Importantly, the NIST mandate also engages with privacy rights and the risks and benefits associated with AI in the private and public sphere.

As part of this mandate the NIST established a Privacy Engineering Program which "supports the development of trustworthy information systems … that protect privacy and, by extension, civil liberties."[64] In its discussion of its AI portfolio, NIST followed the 2023 US federal executive directive established under the Biden administration to achieve "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" (and recently rescinded under the Trump administration).[65] The NIST notes that issues of bias, explainability and security are fundamental questions that must be addressed in developing any system of artificial intelligence.[66]

The *Justice in Forensic Algorithms Act* goes beyond just referring the question of algorithm testing to NIST, although as an agency which appears to have a public record of industry independence, this is an important component of the protections the Act envisions. The Act goes on to set out in some detail how the NIST is to develop and implement testing standards to ensure the fair use of "computational forensic evidence" in criminal case. The standards must among other features:

- Assess the "potential for disparate impact" including race, gender and other demographic features.
- Address the requirements for testing the software that can show its "system performance statistics" including accuracy, precision and reproducibility, as well provide for ongoing testing to address any "material change" in the software and
- Consult a "range of outside experts", including from the fields of forensic science, bioethics, algorithmic discrimination, data privacy, racial justice, criminal justice reform, exonerations, and other areas "that may be identified through public input."[67]

In terms of the criminal process, the Act states that the results or reports resulting from an analysis of computational forensic software, including the source code, must be provided to the defendant. In fact, "evidence that is the result of analysis by computational forensic software" is inadmissible unless it has been admitted for testing by the NIST and the owners and users of the software waive all claims against the defence for the purpose of analyzing and testing the software.[68]

## A model for Canadian Legislation?

On its face, the Act provides a model for the oversight of AI systems involved in criminal proceedings. It provides for a mandatory, transparent and independent process for the ongoing testing of evidence resulting from the use of computational forensic software in any criminal case. It requires that this testing consider the risks of racial bias and privacy breaches. It also aligns with calls over the last 15 years in the United States for a new forensic oversight body and a greater role to NIST in that oversight.[69] More specifically, it responds to the need that "A.I. tools used in the criminal legal system must be subject to peer review, and that peer review includes making the tools available for auditing by research groups with no stake in the outcome."[70]

It is unclear whether the *Justice in Forensic Algorithms Act* will ever become law in the United States. It may well remain only aspirational. However, it is a model worth returning to in considering it as an oversight option for the use of artificial intelligence in Canadian criminal proceedings.

## E. New York: *The Public Oversight of Surveillance Technology Act (POST)*

The POST act, passed by the New York City Council on June 18, 2020, requires "comprehensive reporting and oversight of New York City Police Department surveillance technologies, which includes but is not limited to AI technologies."[71]

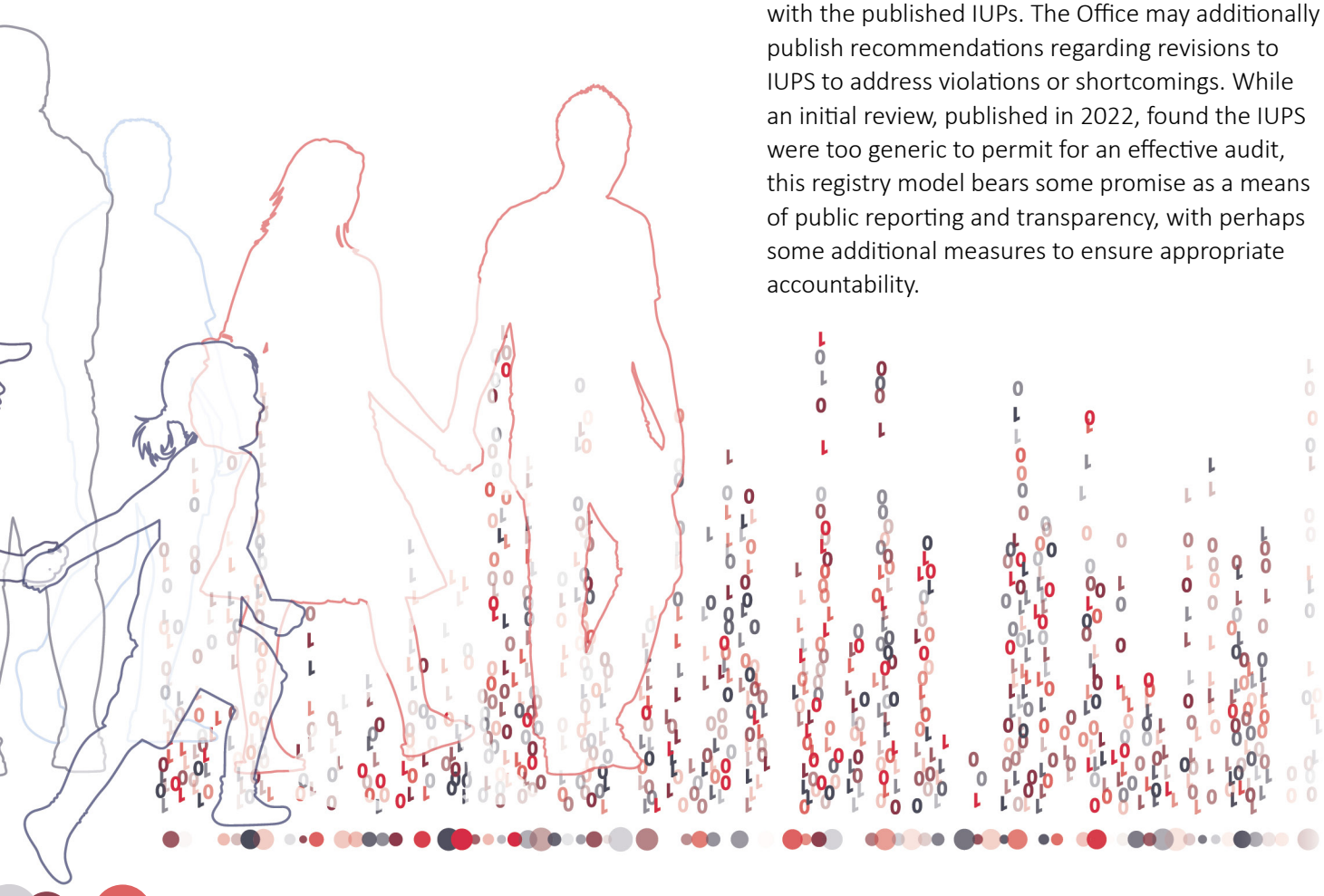
The Act seeks to provide transparency and accountability mechanisms to allow New Yorkers to scrutinize surveillance technology acquisitions and uses by the New York Police Department (NYPD). The Act was introduced as a response to concerns expressed by civil society and advocacy groups about the proliferation of sophisticated surveillance technologies with the potential to impact civil liberties in the name of public safety.

POST has several notable features.

First: Impact and Use Policies (IUPs) must be published for all qualifying technologies. These reports must include descriptions of the capabilities of the AI system and the rules or processes that the NYPD has in place to ensure:

- General safeguards;
- data retention policies;
- public access to surveillance data;
- training information;
- internal audit and oversight mechanisms;
- health and safety reporting; and
- analysis of potential disparate impacts on identifiable communities or groups.[72]

Second: compliance and oversight of POST vests with the Office of the Inspector General for the NYPD. That office prepares annual audits to assess whether uses of surveillance technologies align with the published IUPs. The Office may additionally publish recommendations regarding revisions to IUPS to address violations or shortcomings. While an initial review, published in 2022, found the IUPS were too generic to permit for an effective audit, this registry model bears some promise as a means of public reporting and transparency, with perhaps some additional measures to ensure appropriate accountability.



## F. Consultation Questions

**8)** If Ontario follows emerging best practice and incorporates a risk-based model and criteria (like EU AIA , AIDA, Federal AIA levels) and further establishes that prescribed entities are not allowed to determine their own risk:

- **a)** Will a binary model like the AIDA provide accountability in criminal justice? Or should there be more levels like the TPSB Use of AI Policy, or the EU or Federal AIA?
- **b)** What, if any AI tools should be prohibited for use because the risks they pose to *Charter* rights and civil liberties are simply too high:
  - biometric surveillance, and if so, under what conditions?
  - predictive policing tools?
  - other?
- **c)** Should this model specifically account for human rights, *Charter* rights, and procedural fairness, privacy analysis when considering the deployment of AI in criminal justice contexts?

**9)** With specific reference to the criminal justice system, Ontario should incorporate measures to mitigate risks of technologies used in all stages of the criminal justice lifecycle from investigations to court and corrections.

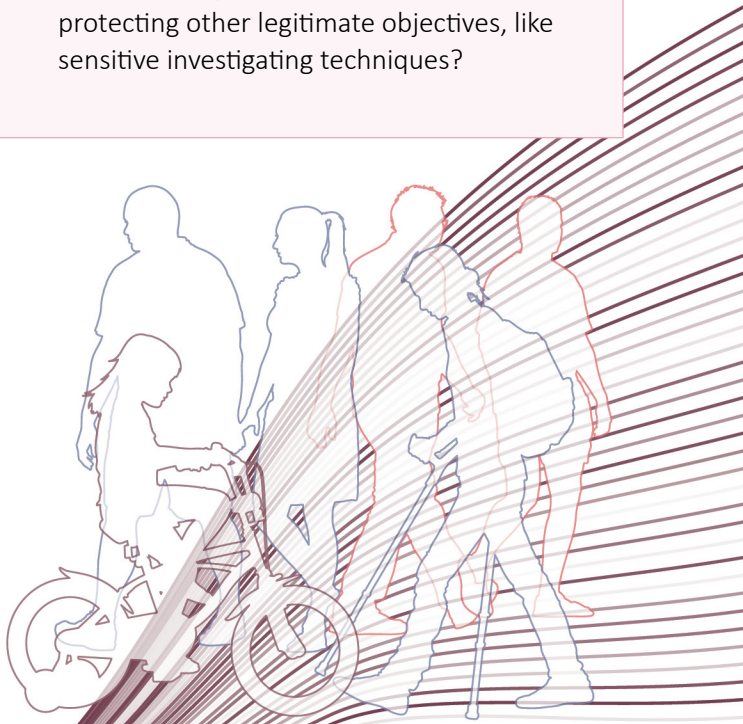
- **a)** What mitigation measures should be considered and included? For example:
  - Third party independent audits of data validity, reliability and relevancy; design/ source code; and unintended outcomes.
  - iExplainability requirements.
  - Metrics testing
  - De-biasing techniques
  - Public and expert consultations.
  - Public reporting requirements on pre-acquisition evaluations and post-acquisition performance review
  - Others?
- **b)** To what degree should court oversight and orders for certain AI uses be required? (compare to the EU AIA which requires court orders for various exceptional uses. EU also requires all these law enforcement applications AND any subsequent court orders to be disclosed to a public registry)

**10)** Should there be a prohibition on criminal justice sector provincial entities procuring, developing or deploying high-risk systems prior to Bill 194 and accompanying regulations being developed?

- **a)** How should the grandfathering of existing AI systems be handled?

**11)** How and to what extent should the use of AI in criminal justice require a mandatory AI registry and disclosure of key elements of public sector AI systems?

- **a)** Disclosure of the training data and transparency
- **b)** Disclosure of the output data for independent auditing and independent oversight, performance monitoring
- **c)** What are the resourcing needs to facilitate reporting to a mandatory AI registry?
- **d)** How can a registry like this be effective while protecting other legitimate objectives, like sensitive investigating techniques?



# 3. Internal Oversight: Criminal Law Oversight Mechanisms

In addition to existing or emerging models for oversight of AI in the justice system external to that system itself, there are aspects of the criminal law process that lend themselves to an active and robust role in overseeing the use of artificial intelligence. In particular, the legal rights set out in the *Charter*, the procedural provisions of the *Criminal Code*, the rules of evidence in the *Canada Evidence Act* (CEA), along with the common law, all inform the rigorousness of governance, lawfulness, and oversight in the use and interpretation of AI by law enforcement, the Crown and courts.[73]

From the accompanying papers in the LCO AI in Criminal Justice series – as well as recent path-breaking reports by legal scholars, lawyers and activists – there are numerous examples of how criminal law litigation, particularly related to *Charter* rights and the law of evidence, might serve as bulwarks against the risks and dangers of AI in the criminal process.

At the same time, there are limitations, as discussed below, to these potential oversight mechanisms from a doctrinal, institutional, and access to justice perspective. Setting out these limitations does not diminish their importance, but it does suggest that these kinds of internal oversights must be accompanied by other reforms from both within and outside the criminal legal system if there is to be full and proper oversight of artificial intelligence.

## 3.1 *Charter*, Evidentiary and Criminal Code Oversight Mechanisms

The information that follows is offered in summary format to better grasp the scope and applicability of existing constitutional law. Readers are alerted to more detailed discussion of the law that follows in the LCO's 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*; and Paper 4, *AI at Trial and on Appeal*.

All papers are available online at https://www.lco-cdo.org/CrimAI.

## A. Freedom from identification and surveillance (s.8)

The surveillance of individuals through the techniques of AI may be found to violate the right against unreasonable search and seizure. The Supreme Court has recognized that the right to privacy in s.8 of the *Charter* includes anonymity, and allowing persons "to act in public places but to preserve freedom from identification and surveillance."[74] The Ontario Court of Appeal has noted that personal privacy "protects an individual's ability to function on a day-to-day basis within society while enjoying a degree of anonymity."[75] Thus, for example, the monitoring of a vehicle's whereabouts on public highways constitutes a warrantless search as it interferes with the right of persons to move around in public.[76]

## B. Protection against Arbitrary Detention and Arrest (s.9)

The police use of algorithms that re-produce racially biased assumptions about criminal activity to detain individuals may be challenged under s.9 as a form of arbitrary detention. The police authority to detain requires a reasonable suspicion that the person is connected to a particular crime, and the grounds must be shown to be objective, "amenable to an exacting review" and not reliant on "peremptory assertions of suspicion."[77] The key question is whether reasonable suspicion can be established in the "totality of the circumstances, including the specific characteristics of the suspect, the contextual factors, and the offence suspected."[78]

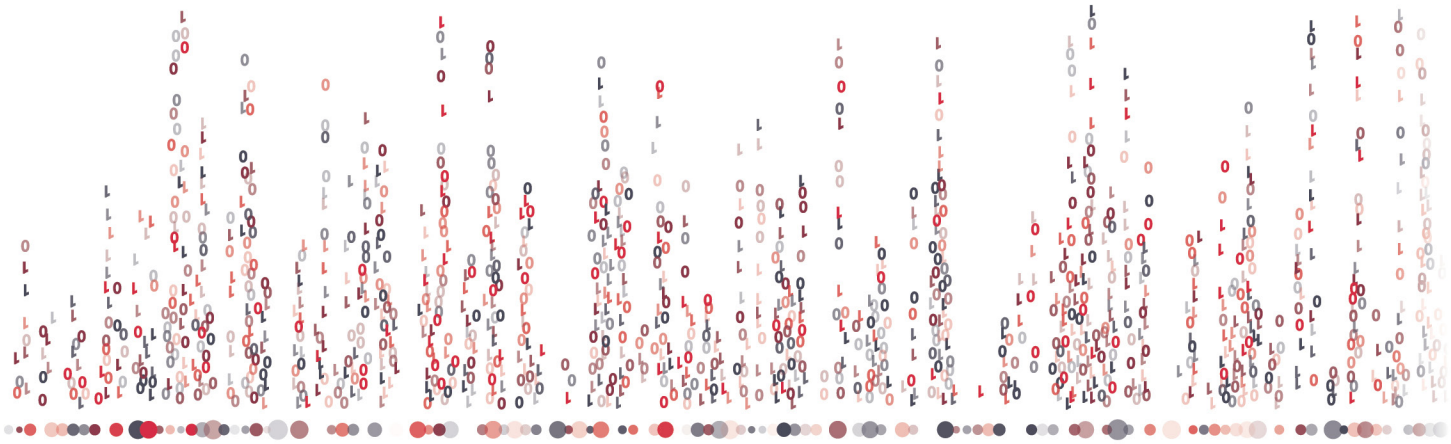
## C. Substantive Equality (s.15)

The use in the criminal law proceedings of facially neutral algorithms that produce unequal and racially biased outcomes may violate the right to "substantive equality" under s.15 of the *Charter*. Substantive equality addresses adverse impacts from facially neutral government action. It is the "animating norm" underlying s.15 protections. It requires that the state not create or contribute to a distinction based on a protected ground *and* that the distinction cannot impose burdens or deny benefits that reinforce or perpetuate or exacerbate a protected group's disadvantage.[79]

## D. Disclosure Rules Based on Full Answer and Defence (s.7)

The prosecution cannot refuse to disclose forensic algorithmic information simply because it represents a legally protected trade secret.[80] Rather, the Crown is required to disclose all relevant, non-privileged information in its possession, or control. In turn, the police are required to disclose to the Crown all material pertaining to their investigation of the accused.[81]

Records not in the possession or control of the Crown or the police will be considered third party records. These records must be produced if a trial judge is satisfied, on having reviewed them, that they are likely relevant. With few exceptions, if found to be likely relevant, the accused person's right to the information will outweigh any competing privacy interests in the records.[82]



### E. Individualized Decision-Making Requirements in Bail and Sentencing Decision-Making

In bail proceedings, the use of AI-generated risk assessments that reproduce existing anti-Indigenous, and racial bias, may be limited by *Criminal Code* requirements that in bail decisions a justice is required to give "particular attention to circumstances of an Aboriginal accused and an accused who belong to a vulnerable population that is overrepresented in the criminal justice system."[83] In fact, as a result of recent 2023 *Criminal Code* amendments, before ordering the pre-trial detention of an accused from those vulnerable communities, justice is required to include in the record of proceedings a statement … "indicating how they considered their particular circumstances."[84]

Similarly, at sentencing, the use of AI to generate risk assessment reports may be limited by the requirement that the court must consider the impact of colonialization and anti-Black racism on individual Indigenous and Black offenders.[85]

### F. Gate Keeping Against Unreliable Scientific, Technical Opinion Evidence

Finally, the common law, and the *Canada Evidence Act*, provide a number of ways to preclude the admission of evidence based on artificial intelligence. These mechanisms center on the requirements of authentication, the best evidence rule, and the admission of expert opinion evidence.[86] Notably, a trial judge has the authority to act as a gatekeeper to preclude the admission of unreliable opinion evidence that "may distort and prejudice the fact-finding process."[87] In particular, expert evidence that advances a novel scientific theory, or technique should be subject to "special scrutiny" particularly where that evidence speaks to an ultimate issue to be determined at trial.[88]

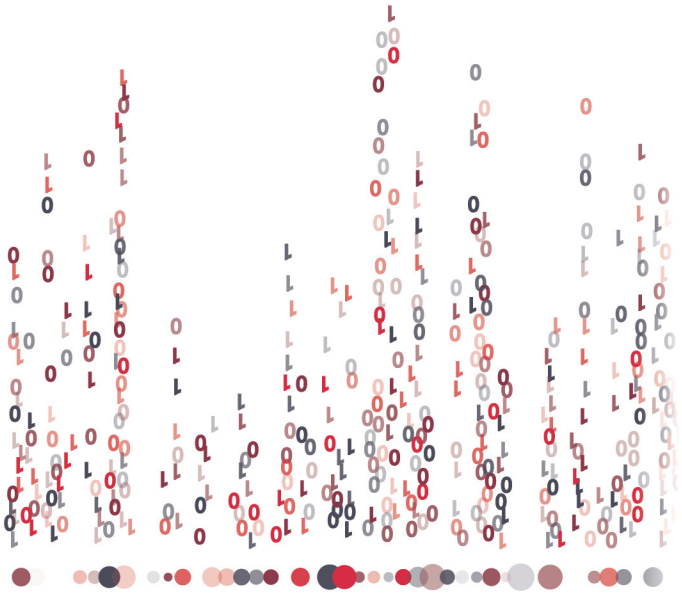
## 3.2 Challenges with Criminal Law Oversight Mechanisms

Each of these legal challenges to the use of artificial intelligence in criminal law proceedings, and there are others, have much to commend them as ways to provide oversight to the admission and use of AI. Certainly, as will be addressed in the final section, any oversight model must contain within its mechanisms support for their use and effectiveness in criminal proceedings.

At the same time, it is important to recognize the potential limitations of these approaches to provide, on their own, sufficient oversight on the use of artificial intelligence. An understanding of these limitations does not detract from their importance in criminal law matters but leads to a better appreciation of how they can, and must, be supported by other reforms.

### A. Section 8 Privacy rights are limited in Application

Under s.8 of the *Charter*, there is no unqualified right to privacy. Instead, the right against unreasonable search and seizure applies only where the state has interfered with a "reasonable expectation of privacy." It is settled law that a s.8 violation can only be established by a state action that violates the accused's reasonable expectation of privacy, rather than the privacy rights of third parties.[89]



## B. Limited notice requirements to protect privacy rights

As a practical matter, a right to a privacy that encompasses anonymity can only work as an oversight mechanism if there is a corresponding duty on law enforcement to notify persons that their "right to be left alone" may have been violated.

As others have pointed out, "notice is thus a vehicle for facilitating meaningful access to remedies for *Charter* and human rights violations that are occasioned by a given law enforcement agency."[90] Other than *Criminal Code* provisions dealing with wiretapping, there is no legislative requirement for law enforcement to notify people when they are under surveillance. In particular, there are no legislative requirements that require law enforcement to provide notice to persons that their right to privacy may have been infringed by being the subject of surveillance techniques.

It is unrealistic to expect that this "notice gap" for citizens in the oversight of AI could be filled by the criminal trial process alone. In a criminal prosecution, an accused would seemingly have notice of the surveillance of others if that surveillance resulted in inculpatory evidence that the Crown was seeking to use as part of its case. However, it is at least an open question whether that surveillance would be seen to have impinged on the accused's "reasonable expectation of privacy", as protected under s.8 of the *Charter*. More fundamentally, however, that mechanism is only triggered by a criminal prosecution. It would simply not apply to the ongoing surveillance of persons, and privacy violations, that do not result in criminal charges.[91]

In addition, as discussed below with respect to the limited impact of *Charter* remedies, it does not seem that a finding of a *Charter* violation in any particular case will necessarily result in a change in the police conduct or surveillance technique that resulted in the *Charter* violation.

## C. Privacy rights are normative and should be set out in legislation

The question of when state action will interfere with a constitutionally protected "reasonable expectation of privacy", which would trigger the protection of s.8, has been described as a "normative inquiry" which requires a judicial consideration of the "aspirations and values" of society as whole."[92] More broadly, if the protection of privacy rights in the criminal law process requires an assessment and articulation of the underlying goals and beliefs of society as a whole it is preferable that the assessment be conducted by a democratic process rather than developed through the particular prism of the criminal trial and the viewpoint of the judiciary. What is at stake, as courts themselves have recognized, is the question of what kind of society individuals want to live in, and what degree of state surveillance they want or are willing to tolerate in exchange for public safety, versus what degree of privacy they desire, even if it comes with a level of safety risk. In other words, what is the correct balance between privacy, anonymity, and public safety in a free democratic state? This is not a question to be answered on a case-by-case basis but rather a larger one for the justice system as a whole.

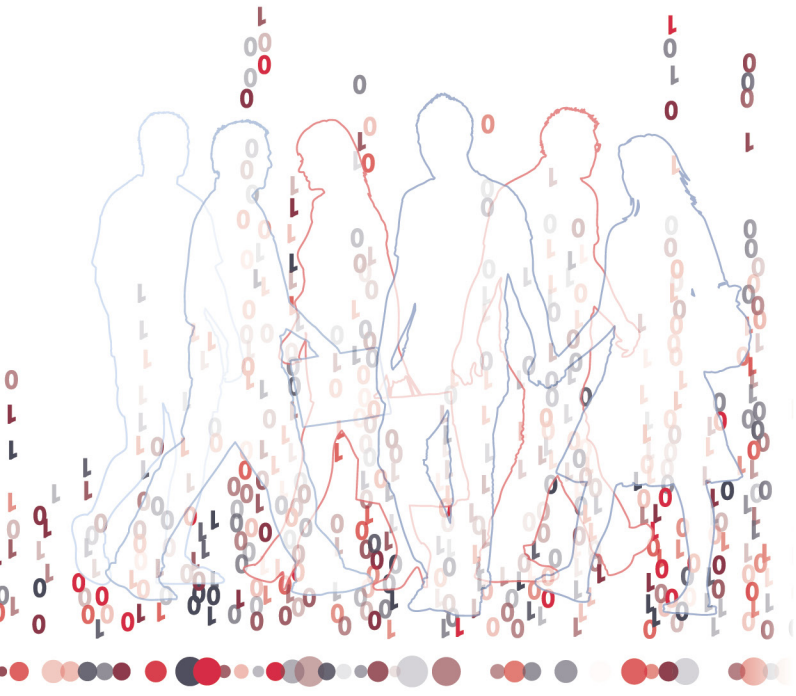
## D. Bad facts can result in bad law

In addition, criminal law prosecution is by definition fact-based and may not provide the best record for a court to understand the impact of any particular technique of artificial intelligence. Certainly, the benefits of AI may be before the court by the evidence put forward by the Crown, but the risks attached to it may be viewed as more hypothetical and difficult for the trial court to appreciate. Leaving oversight to the courts, risks the spectre of bad facts resulting in bad law.[93]

## E. Uncertainty about algorithmic profiling to determine reasonable suspicion

Some of the general concerns outlined above with respect to the right against unreasonable search and seizure, apply to s.9 as well. At the same time, there is good reason to think the protection against arbitrary detention under s.9 of the *Charter* should provide an effective mechanism for the oversight of the police use of "algorithms trained on past crime data" to predict criminal activity.[94] Even here, as a matter of law, the scope of s.9's protection against the use of algorithmic policing, still may depend on the facts of the case, or at least on the defence's ability to challenge the prosecution's understanding of those facts.

It was established in *R. v. Chehil* that "[c]haracteristics identified by a police profile can be considered when evaluating reasonable suspicion."[95] However, the use of police profiles should be "approached with caution" to ensure that they do not undermine the requirement of a "careful individualized assessment of the totality of the circumstances."[96] This ambiguity in the jurisprudence has led to the conclusion that "reasonable people can disagree about how to incorporate this new policing technology into reasonable suspicion determinations."[97]



## F. Limits on Judicial Protection of Constitutional Rights without Legislative Oversight

At the most general level, relying on court oversight through the criminal process to assess the legality of law enforcement use of AI tools, without legislation to set some basic guardrails, risks expanding and not limiting those police powers. In the area of police powers of detention, search and arrest, courts, in the absence of legislation to address the scope of police powers, have expanded that authority under the common law and in supposed compliance with the *Charter*. The lessons from the rise of the common law police ancillary powers are particularly apt for a larger consideration of the use of criminal process as an oversight mechanism for the use of AI.

In this area of law, and in the absence of legislation to guide the oversight of police conduct, courts have viewed the question as being whether the conduct is authorized under the common law, rather than whether the conduct infringes on the *Charter*.[98]

There is an important and impactful distinction between the two approaches. Although this common law analysis is informed by the values of the *Charter*, it does not proceed by the two-stage approach mandated by the *Charter* review of legislation. That approach requires an identification of the rights violation and then a consideration as to whether the violation is reasonably justified under s.1 of the *Charter*.

In contrast, the approach taken by courts in determining whether police action is authorized under the common law has been characterized as an "end run" around the *Charter.*[99] The impact of this end run is to diminish the importance of a rights-based approach to assessing the legality, and constitutionality, of police conduct. The result is common law police powers that are not "anchored in a theory of rights as limits on police powers" as mandated by the *Charter* but is a doctrine "anchored in a theory of police powers as limits on rights."[100]

### "Almost Irresistible pressure" to expand police power on an incremental basis

There are practical implications to that doctrinal shift. For criminal courts facing factually guilty persons, this approach results in an "almost irresistible pressure to continually expand police power."[101] Moreover, because of the restrictions of a case-by-case approach to the oversight of police conduct, courts, "are ill suited to the task of creating the sort of clear, comprehensive and prospective rules" necessary for meaningful oversight.[102] The common law rules may lack nuance and detail and are always subject to redefinition through litigation as new fact scenarios arise.[103]

### No accountabilities beyond criminal process

Most tellingly, from an institutional perspective, is that criminal court oversight excludes from its purview the vast majority of cases and individuals who may have been impacted by law enforcement's use of AI but who were not the subject of criminal law charges. Without a framework of accountabilities that extends beyond the criminal court, those actions and their impact on persons' rights remain unaddressed.

There is an argument that the required degree of accountability can be provided by the remedies that are available in criminal court proceedings, which have an impact beyond the particular facts of the criminal case. Certainly, the availabilities of remedies as discussed with respect to the proposed Bill C-27, must be a critical part of any oversight model. It is suggested below that the impact of *Charter* remedies on ongoing police conduct may be dramatically less than what would be expected if those remedies can provide a meaningful mechanism of oversight for the use of AI.

## G. Limited Impact of s.24(2) Remedies on Systemic Reforms

Following on the analysis of Professor Kent Roach, it is useful to assess the effectiveness of remedies by focusing on whether a given remedy advances one of two policy tracks. The first track is the compensation and protection of litigants whose *Charter* rights have been violated. The second track is geared to providing more systemic reforms to prevent similar *Charter* violations in the future.[104]

As the risk of generalization, there is some mixture in the use of both the first and second track approach in providing remedies in the area of criminal law. Ultimately, however, the remedies provided in criminal law proceedings show a focus on providing individual redress, rather than advancing institutional reform. Moreover, even where the question of remedy does assess factors beyond individual redress, it may well adopt an approach that allows for the continuation of the underlying conduct.

This emphasis on individual redress vs systemic reform in remedies has manifested itself in different ways. In criminal law litigation, the most common remedies under 24(2) for *Charter* violations are exclusion of evidence, and to a lesser extent stays of proceeding, and reductions of sentence.

### Exclusion, stays and reduction in sentence

In considering whether exclusion is an "appropriate and just" remedy under s.24(2), courts have moved away from only considering whether the evidence would not have been obtained "but for" the *Charter* violation, which reflects a focus on redressing the harm caused to the individual accused.[105] Instead, courts now adopt a balancing of factors approach, including the "but for" test, but also including an assessment of the seriousness of the *Charter* breach and its impact on others, and not simply the accused.[106]

Unfortunately, the question of the seriousness of the breach is often a subjective or political assessment that may minimize the seriousness of the breach by stressing the importance of police powers. The level of judicial subjectivity in assessing whether illegally obtained evidence means that the availability of the remedy can be characterized as a "legal lottery."[107] The uncertainty of obtaining a remedy for a *Charter* violation would seem to undermine the potential of the remedy to deter future misconduct.

The remedy of stay of proceedings has been viewed as a mechanism that incorporates both first track and second track approaches. However, there is a risk of "remedial deterrence" depending on the seriousness of the charge or charges that are stayed.[108] Courts may be reluctant, as one sees in the s.11(b) jurisprudence, to find an underlying *Charter* breach because of the bluntness of the remedy. It thus may not ultimately serve as an effective way to reform underlying state misconduct.

Finally, sentence reductions are only available to address an abuse of power related to the individual or the offence and thus are limited as second track mechanism of systemic change.[109]

Regardless of the doctrinal differences, the impact of *Charter* remedies in criminal law proceedings has been limited in terms of addressing ongoing state misconduct. The reality is that individual remedies of exclusion, and even stays of proceedings, "may simply place a heavier tax on the continued violation" as the remedy does not address the systemic basis for the violation.[110]

### A case in point

The limited impact of the decision of the Supreme Court in *R. v. Golden* is an instructive case in point.[111] In that case, the Supreme Court imposed common law limitations on the "inherently degrading and humiliating" practice of strip searches. It also noted the need for legislative guidance in this area. Notwithstanding this direction from the Court, it does not seem that the police have significantly changed their practices in this area. Instead, "there is evidence of chronic non-compliance by some police services."[112] The legality of strip searches continues to be litigated, and evidence excluded, and charges stayed. In the meantime, courts continue to find it "inexcusable" how little knowledge the police have of the restrictions set out in *R. v. Golden.*[113]

Outside of the criminal trial process, there are a variety other remedies that may be sought to challenge the state use and abuse of techniques supported by tools using artificial intelligence. The most obvious one would be seeking declaration of invalidity with respect to particular forms of government or legislative action. As noted, the unequal impact of AI on marginalized communities may provide opportunities to purse such a remedy under s.15 of the *Charter*.

## H. Limited Data to Demonstrate S.15 Disproportionate Impact

It is worth providing some realistic appraisal of the potential of s.15 to address the discriminatory aspects of the application of AI to the investigation and prosecution of criminal offences.

In *R. v. Sharma*, the Supreme Court addressed the potential for s.15 to challenge the unequal application of facially neutral legislation and state action in the area of criminal law.[114] At issue were sentencing provisions that limited the availability of conditional sentences for offences which, under s.742(1)(c) of the *Criminal Code*, carried a maximum prison sentence of 14 years or life imprisonment. In particular, the court considered the constitutionality of that facially neutral limitation in light of s.718 of the *Code* that required sentencing courts to address the overrepresentation of Indigenous persons in Canada's prisons.

The majority of the Supreme Court found that the limitation on non-custodial sentences in s.742(1)(c) did not violate either s.15 or s.7 of the *Charter*. Justice Rowe for the majority acknowledged that substantive equality was an "animating principle" of s.15, which was available to challenge the unequal impacts of facially neutral government action. At the same time, these kinds of equality challenges can only be sustained if the applicant, as a first step in a s.15 challenge, is able to demonstrate that the impugned law or state action creates or contributes to the disproportionate impact on a protected group. The majority agreed with the trial judge that there was no evidence, for example by expert opinion or statistical data, to show that Indigenous offenders were disproportionately impacted, relative to non-Indigenous offenders, by s. 742(1)(c) and the removal of non-custodial conditional sentences as a sentencing option.

Justice Karakatsanis, for the minority, found that the requisite disproportionate impact of s.742(1)(c) was demonstrated by the simple fact that it was only Indigenous offenders, and not non-Indigenous offenders, who would now be precluded from obtaining a non-custodial sentence which would otherwise have been available to them under s.718.

It is difficult to disagree with Justice Karakatsanis's view in *R. v. Sharma* that the majority is "effectively raising the evidentiary bar of the first step" in assessing s.15 equality claims.[115] It would have been possible, and taken "little imagination", given the general overrepresentation of Indigenous persons in prison, to conclude that any legislation that limits the availability of non-custodial sentences would disproportionally impact Indigenous persons.[116]

The majority, however, does not allow for that kind of logical reasoning to show disproportionate impact. Instead, it requires evidence of disproportionate impact specific to the legislative or government action at issue. The reality, however, as both the majority and the minority opinion may have been aware, is that the criminal justice system simply does not regularly collect data on the disproportionate impact of particular forms of legislation or government action. This lacuna of data moving forward is almost certain to include the use and impact of artificial intelligence at any stage of a criminal proceeding.

The same constraint on the use of s.15 to challenge the use of AI tools in the criminal justice system can be gleaned from the earlier decision of the SCC in *Ewert v. Canada*.[117] In *Ewert*, the court addressed the use of standardized assessment tools to predict the potential recidivism of Indigenous offenders even though the assessment tools were based only on data as to the behaviour and recidivism of non-Indigenous persons.

The court agreed with the trial judge and found that that there was a risk "that the impugned tools are less accurate when applied to Indigenous inmates than when they are applied to non-Indigenous inmates."[118] The court concluded, however, that this difference in the reliability of assessment tools when applied to Indigenous offenders did not establish a violation of s.15.[119] They found that what was missing and necessary to establish a violation of s.15 was evidence that "the impugned tools do in fact overestimate the risk posed by Indigenous inmates or lead to harsher conditions of incarceration or to the denial of rehabilitative opportunities because of such an overestimation."[120] Similar to *R. v. Sharma*, the court reasoned that it was not enough to argue that the overrepresentation of incarcerated Indigenous persons shows in and of itself the disproportionate impact of unreliable risk assessments on Indigenous offenders.

Taken together, the result and reasoning in both *R. v. Sharma* and *R. v. Ewert* shows that any potential for s.15 to act as an oversight mechanism for the use of AI in the criminal justice system may be dependent on the implementation of better mechanisms to collect and share data with respect to its impact on protected groups.

## I. *Ewert v. Canada* as a Model for AI Oversight?

The importance *of R. v. Ewert* to an understanding of the mechanisms needed for the oversight of AI is not limited to its s.15 consideration. It also provides some positive, but also cautionary, lessons on the litigation model to address the inequities in the use of AI in criminal law matters.

The challenge to the culturally biased risk assessment tools in *R. v. Ewert* was not based just on ss.15 and 7 of the *Charter*. It was also premised on the failure of correction officials to meet their statutory obligation under s.24 (1) the *Corrections and Conditional Release Act* (CCRA)[121] to "take all reasonable steps to ensure that any information about an offender that it uses is as accurate, up to date and complete as possible."[122] The majority of the court concluded that that because correctional officials did not take steps to ensure that risk assessments could be applied reliably to Indigenous offenders it had failed to meet its statutory obligation under the CCRA.

In the "exceptional circumstances" of the case, which involved almost 20 years of litigation, the majority refused to send the matter back for Mr. Ewert to seek a remedy and instead issued a declaration that the correctional officials had failed to meet their obligations under s.24(1) of the CCRA.

The result in *Ewert* shows the importance of imposing statutory obligations on state actors to ensure reliability and accuracy, including eliminating the risk of cultural bias, in its use AI techniques. *Ewert* shows that it may be insufficient to rely on just abstract *Charter* principles to challenge AI generated evidence. Instead, real statutory limitations and obligations should be imposed.

As evidenced by *Ewert* there are significant practical advantages in imposing statutory obligations to address the improper use of risk assessment tools, or AI tools more generally. From a litigation point of view, in these circumstances, the onus is now on the state to lead evidence that it has met those statutory obligation, rather than relying on individuals to demonstrate the impact of those tools on their *Charter* rights.

More generally, the decision in *Ewert* shows that these kinds of statutory obligations require officials to "advance substantive equality" and provide an "opportunity to consider solutions for the system as a whole."[123] Certainly, the insights provided by the court in *Ewert* on the limitations posed by risk assessment tools used in the correctional law context have been recognized and applied with respect to similar risk assessment tools used for Indigenous persons in dangerous offender proceedings.[124]

At the same time, it is difficult to assess the precise impact of *Ewert*. The court indicated that could not define "with precision what the Correctional Services of Canada (CSC) must do to meet the standard set out in s. 24(1)." Instead, it suggested that "at a minimum" further research should be conducted as to whether the assessment tools "are subject to cross-cultural variance when applied to Indigenous offenders."[125] The result of that research would determine if the CSC should discontinue their use or modify how they are used to eliminate prejudice to Indigenous offenders. [126]

The court also emphasized that it was not making any finding that correctional officials had improperly relied on the existing assessment tools in determining Mr. Ewert's recidivism risk. Instead, it left it to Correctional officials to make that determination through the usual CCRA grievance process, which could then be challenged by Mr. Ewert.

The uncertainty of both the systemic remedy and the result for Mr. Ewert provided by the Supreme Court is particularly noteworthy in light of the length and expense of the ligation to reach those results. The matter took 18 years to make its way through the CCRA's internal grievance process, and through both the Federal and the Federal Court of Appeal, before the Supreme Court released its decision. There is much to commend the result in *Ewert*. However, the efficiency and cost-effectiveness of the litigation process in reaching that result is not one of them.[127]

## J. Limits of Litigation to Address Unreliable Scientific Evidence

As indicated previously, in the criminal law context there are a number of mechanisms particularly available at the trial stage, to contest the admissibility and use of scientific evidence, including the use of evidence generated by artificial intelligence.

In brief, Canadian courts are instructed to apply a two-part "*Mohan*" test in determining the admissibility of expert opinion evidence.[128]

The first part of the *Mohan* test requires that the evidence be relevant, necessary, otherwise admissible, and it must be introduced through a properly qualified unbiased expert. The second part of the test speaks to the "gatekeeping" role of the trial judge to ensure that the benefit of the proposed evidence outweighs its potential risks. In this assessment, a trial judge considers factors such as legal relevance, necessity and the reliability of the evidence, and the absence of bias. Notably, it is settled law that a novel scientific theory or technique is subject to "special scrutiny" under *Mohan*, particularly where the evidence speaks to an ultimate issue to be determined at trial.[129]

As a matter of legal doctrine, these common law rules would seem to provide useful safeguards, and oversight mechanisms, for the use of evidence generated by the use of artificial intelligence. Certainly, the growth of these common law requirements, particularly the emphasis on a gatekeeper function for trial judges, is drawn from the findings and recommendations of several judicial inquires that have documented how the admission of unreliable and biased scientific evidence has led directly to wrongful convictions and miscarriages of justice.[130]

At the same time, without further reforms and expansions to institutional capacity in which these common law rules operate, the admissibility rules cannot provide sufficient oversight on the use and misuse of evidence generated by artificial intelligence.

Academic research has suggested, across a number of jurisdictions, that the threshold of requirements of admissibility, even those including assessments of reliability, are not effective in limiting the use of novel, biased or untested scientific evidence. As summarized by one commentator "the adversarial process has failed to identify the vulnerabilities of expert testimony or to prevent wrongful convictions."[131]

One comparative study analyzed the consequences of different admissibility standards used in four different countries for the use of forensic scientific evidence in legal proceedings. It summarized its findings as follows:

> Our basic conclusion-which may surprise many readers, particularly lawyers, and disappoint those contemplating law reform-is *that formal admissibility standards do not seem to make much difference.* Formal admissibility standards, particularly those incorporating reliability, are not enforced in ways that regulate the reception of expert opinion evidence that is of unknown reliability [emphasis in original.][132]

With respect to Canadian practices, the same study acknowledged that several high-profile inquiries have highlighted how unreliable scientific evidence can directly lead to wrongful convictions and miscarriages of justice. The study pointed out, however, that these findings, which have also been cited by Canadian appeal courts, had seemingly little impact on trial court practices where there was still only a "perfunctory admissibility enquiry" to assess the reliability of novel scientific evidence.[133]

It has been similarly suggested in the Canadian legal context that with the "high volume, under-resourced run of ordinary cases in the criminal legal system" it is simply too difficult for judges and lawyers to identify the factors that may show the unreliability of any proposed new piece of scientific evidence.[134]

Fortunately, these same inquiries, which have identified the dangerous impact of unreliable scientific evidence, have also recommended a number of institutional reforms to address the use and misuse of that kind of evidence. These recommendations are not limited to simply emphasizing the role of the trial judge as gatekeeper for the admission of unreliable evidence. Instead, these recommendations encompass a number of larger institutional reforms. These reforms may be the most relevant to developing ideas to provide oversight to the use and admission of evidence produced by artificial intelligence.

## 3.3 Proposed Institutional Reforms to Address Unreliable Scientific Evidence

In Ontario, there are two significant inquiries on the use and misuse of forensic scientific evidence that may be useful in assessing how to ensure the proper use of evidence generated by artificial intelligence. The first is the 2008 *Inquiry into Pediatric Forensic Pathology in Ontario* (the "Goudge Inquiry"), dealing with the use of pediatric forensic pathology evidence in wrongful death criminal prosecutions.[135] The second, occurring about a decade later, is "*Harmful Impacts: The Reliance on Hair Testing in Child Protection, the Report of the Motherisk Commission* (the "Motherisk Commission" or "Motherisk Report"), which addressed the improper use of hair analysis to identify drug use by parents in child protection matters.[136] These inquiries were ordered after the admission of unreliable scientific evidence through the usual criminal trial adversarial process resulted in persons being wrongfully convicted in the death of their children, or wrongfully losing the custody and care of their children.

### A. The Goudge Inquiry

oudge inquiry resulted in 169 recommendations with respect to "the organization, practice and presentation" of forensic pathology evidence in Ontario.[137] It is difficult to do justice to all of them regarding whether they might also apply to the oversight and organization, practice and presentation of AI evidence in Ontario. However, a number of themes seem relevant to both forms of scientific evidence. This includes:

- More attention to scientific research, enhanced communications, greater transparency and improved documentation by the expert witness.
- Better training, certification and accreditation for the expert.
- Introduction of a code of practice that would include "principles that should guide them as they write their reports and the information that should be contained in them, including the need for clarity, identifying the limits of their own expertise, and alternative explanations."
- Requirement that experts should not formulate or articulate their opinions in terms of "proof beyond a reasonable doubt" and should not change their level of confidence "depending on the forum in which the opinions are expressed."
- Code of Conduct for Expert Witnesses emphasizing their duty to assist the court which overrides any obligation to the person from who they received instruction or payment
- More pre-trial meetings between experts, and between experts and lawyers.
- Consideration of the use of concurrent evidentiary procedures in which experts with different views are presented and testify as part of a panel and are questioned concurrently.
- Better supports for the trial judge in meeting its "heavy burden" as gatekeeper from the admission of unreliable evidence, including programs from the National Judicial Institute "on threshold reliability and the scientific method in the context of determining the admissibility of expert scientific evidence."

- Enhanced supports for legally aided defence services to critically evaluate and even challenge the admission of unreliable forensic scientific evidence.[138]

It is beyond the scope of this paper to assess the impact of the Goudge recommendations on the subsequent oversight of forensic evidence in criminal proceedings. However, one author, who testified as an expert at the Goudge Inquiry, and is a registered forensic psychologist, has written that result of the inquiry was a "transformative" and has led to the establishment of the Ontario Forensic Pathology Service, the training of forensic pathologists in accredited programs, and "the development of robust and quality driven service."[139]

## B. The Motherisk Commission

The Motherisk Commission addressed the impact of unreliable testing and results for drug and alcohol consumption and exposure in child protection proceedings, and in a much smaller number of criminal proceedings.

The Report made a number of recommendations to child protection law and the need for more rigorous standards for the admission of scientific evidence, including a better understanding by judges in that area of law of their gatekeeping function. The Report also include some specific recommendations for enhanced legal aid funding and support for counsel to challenge the use and misuse of scientific opinion evidence in child protection proceedings.

The Report also recommended changes to the Family Law Rules that would require parties when adducing medical or scientific test results to accompany those results, similar to the requirement in criminal proceedings, with an expert report "explaining the meaning of the test results and the underlying science behind the testing."[140]

### Impact Assessment

More importantly, the Report went on to recommend that expert reports should "include any known possible impacts of gender, socio-economic status, culture, race or other factors in the testing or assessment of the tests and what, if any, steps the expert took to address them."[141] This requirement to attach an impact assessment to any expert report seems particularly relevant to the use of AI given the acknowledged potential for socio-economic and racial biases to be present, particularly in tools created using legacy policing data, in evidence produced by artificial intelligence.

## C. A Justice and Science Commission

The Motherisk Report also discussed the potential introduction of a Canadian "Justice and Science Commission" to study the reliability of forensic tests and techniques. This body would be comprised of scientific experts who, with the assistance of advisory committee, would "evaluate the reliability of existing and novel forensic scientific methods and issue these methods in legal cases."[142]

A critical component of the proposal for a Justice and Science Commission is the recognition that it could serve to bridge the gap in resources between the state's use of scientific evidence and the ability by the defence to challenge the reliability of that evidence in court.[143] The Commission could act as an objective source of information that could be relied on by courts to assess the reliability of proposed scientific evidence. In fact, it is suggested that the reports prepared by the Commission would be directly admissible without the need to call expert testimony or witness.[144]

The Motherisk Report additionally noted that while there was some approval for such as Commission among those it consulted, there were also concerns that this state-funded institution would not have sufficient independence to assess the use of forensic evidence by other state actors in child protection proceedings.

Importantly, to Professors Cunliffe and Edmond, who the Motherisk Report acknowledges have been the strongest advocate for such a proposal, a Justice and Science Commission could work along side but separate from a formal Criminal Conviction Review Commission or Miscarriage of Justice Commission. The latter would be concerned with addressing individual injustices. A Justice and Science Commission would provide more systemic reports on the reliability of proposed forensic scientific techniques which could then by used by courts in assessing the reliability of scientific evidence and avoiding miscarriage of justices in individual cases.[145]

It is unclear at this early stage how a Justice and Science Commission might work with the recently proposed federal Miscarriage of Justice Commission. Legislation establishing the Miscarriage of Justice Review Commission largely focuses on addressing individual wrongs. It is silent on whether the Commission could take on larger more systemic research focused, for example, on the reliability of new scientific evidence, such as the use of AI generated evidence. Outside of addressing individual cases, the legislation does seem to only "authorize the Commission …to provide the public… with information about its mandate and miscarriages of justice" and to "require the Commission to make and publish policies and to present and publish annual reports that include demographic and performance measurement data."[146]

The original report by Justices LaForme and Westmoreland-Traoré, which led to the federal proposal for a Miscarriage of Justice Commission, very much envisions that the Commission would be proactive, and would address larger systemic research issues. In this way, the Commission would not simply be reactive by addressing only individual injustices. In addition, the report recommended that a Miscarriage of Justice Commission include experts in forensic sciences given the documented history of how unreliable forensic science has contributed to wrongful convictions and miscarriages of justice in this country.[147]

At the same time, the Report was aware that too much a commitment to systemic reform by a Miscarriage of Justice Commission could act as a drain on its limited resources that should be focussed on repairing individual injustices. The report noted that there might be other organizations that are in a better position to advocate for systemic reform.

In any event, regardless of the precise division of labour in the proposed Miscarriage of Justice Commission between individual assessments of harm and the systemic causes of harm, it is easy to see how a Justice and Science Commission could positively impact and support the work of a Miscarriage of Justice Commission. This positive impact by a Justice and Science Commission could be quite apparent if it could be used to assess the reliability of new kinds of evidence produced by the use of artificial intelligence.

The need for institutional resources in the area of Legal Aid supports to address this access to justice gap in the oversight of AI in criminal proceedings merits its own discussion.

## 3.4 Legal Aid Supports for the Oversight of AI in Criminal Proceedings

### A. An Overview of Supports in Ontario

The LCO AI in Criminal Justice Project papers consistently express concern for the inequitable resources available between the state's prosecution of criminal offences and the resources available to the defense of the accused. This is identified as a significant impediment to the capacity of criminal law proceedings to provide fair and effective oversight of AI systems. Certainly the issue is elevated to critical status if issues of AI oversight are largely left to courts to sort out on a case-by-case basis.

This inequity in resources has also been the subject of several commentaries that have reviewed the impact of AI on criminal proceedings.[148]

The challenges and opportunities in addressing this inequality of resources by way of services provided or funded by Legal Aid Ontario is discussed below.

#### Legal Supports at Bail Hearings

Legal Aid Ontario (LAO) estimates that approximately 80% of accused persons in bail court are represented either by duty counsel, or by the private bar who are acting on legal aid certificates.[149] Duty counsel represents the majority of these legal aid clients at bail hearings (between 60%-70%).[150]

As a legal matter, there are inherent constraints in mounting a full challenge at a bail hearing to the admissibility and the use of AI generated evidence. A justice presiding at a bail hearing is not a "court of competent jurisdiction" capable of providing *Charter* remedies under s.24(1).[151] In addition, the *Criminal Code* provisions dealing with bail provide a "certain level of informality," which relaxes the rules of evidence and introduces an expansive approach to relevance.[152] Finally, any such challenge may well require an adjournment resulting in a significant delay that would not be in the client's interests.

To better appreciate the complexity and practicality of raising issues with AI for the purposes of bail, sentencing and other forms of risk assessment, see the extended discussion in LCO AI in Criminal Justice Project Paper 3, *AI and the Assessment of Risk in Bail, Sentencing, and Recidivism*, available online: https://www.lco-cdo.org/CrimAI.

Moreover, as carefully documented in the LCO paper addressing the use of AI in risk assessments, duty counsel is already overtasked with providing basic representation to clients, and thus, without additional supports, will be challenged to address the admissibility of AI tools or AI-driven assessments, predictions, or conclusions in those proceedings. In 2022-23, LAO provided legal advice and/or representation to 630,062 accused persons through its criminal duty counsel program.[153] This represented about an 11% increase from the numbers served in 2021-22.

Similarly, it is reasonable to conclude that, as a general matter, the resources provided to privately retained counsel on certificate matters for bail representation provides similar obstacles to defence counsel to mount a full challenge to the admissibility and use of AI generated evidence those proceedings.

LAO has over the past several years expanded its funding of bail services for the private bar acting on certificates. At the same time, for certificates that are billed by hourly billing, LAO caps coverage at four or five hours, depending on whether it is a first or second bail hearing. For matters that are billed by way of block fees, the compensation ranges from approximately $780 to $880.[154]

Private bar lawyers may be authorized to bring a bail review that can provide an additional 10 hours of coverage to the certificate or a block payment of about $1,000, depending on how the matter is billed.[155] In 2024, LAO introduced a new pilot authorization for habeas corpus applications to expedite bail proceedings that provide an additional 16 hours of coverage, other than attendance on the application.[156]

### Legal Aid Supports After the Bail Stage: Block Fee and Hourly Tariff Services

If a matter proceeds to trial, the kind of legal aid support that may be required to contest the admissibility of evidence generated by AI, or even for defence counsel to review and understand the AI evidence, is more expansive.

To better appreciate the complexity and practicality of raising issues with AI at trial, see the extended discussion in LCO AI in Criminal Justice Project Paper 4, *AI at Trial and On Appeal*, available online: https://www.lco-cdo.org/CrimAI.

Notably, however, the eligibility for full legal services that are provided by certificates is more restrictive than for duty counsel services. Eligibility for certificate services that can contest charges at trial is limited to those charges where the accused is likely to receive a jail sentence in the event of a conviction, and where the accused meets LAO's financial eligibility requirements.

In addition, most LAO criminal law certificates involve matters that are not set down for trial but instead are resolved by way of a guilty plea. These matters, unless they involve the most serious of charges, or the prosecution of a young person, are not billed by the hour but instead are paid by way of pre-determined block fees. These fees are defined in the *Legal Aid Services Act Rules* and generally fall within $250-$1500.[157]

In exceptional circumstances, LAO may allow a block fee service to be billed by the way of the hourly tariff. Even so, any such block fee exemptions are ineligible for expanded coverage that hourly tariffs might otherwise be able to access, such as an expanded pre-determined litigation budget and discretionary payment after the matter is resolved and in excess of the tariff.

For the most serious charges, as well as charges under the *Youth Criminal Justice Act,* and any charge that has been set down for trial, lawyers bill at a set hourly rate for the hours spent on the case, subject to a maximum number of hours.

As of April 1, 2025, the LAO hourly rate ranges from $126.35 to $186.44 depending on the experience of the lawyer, and the case's complexity, although the rates are somewhat higher for matters in the Northern regions of the province.[158]

The maximum hours that can be billed will depend on a certificate is dependent on a number of factors:[159]

- the seriousness of the type of matter (LAO categorizes offences by Indictable Offence 1, Indictable Offences 2, and two different levels of summary conviction offences[160]);
- how the matter is resolved (guilty plea, withdrawal or contested trial);
- the length of the proceedings, and
- whether there were "ancillary" criminal proceedings (ie *Charter* applications, bail proceedings, and the use of a *Gladue* or a Impact of Race and Cultural Assessment [IRCA Report]).

In general, the hours that may be billed will increase proportionate to the seriousness and complexity of the charge(s) and whether the charge(s) are contested at trial.[161]

As discussed below, both the block fee and tariff payment mechanisms include the potential for additional compensation for defence counsel to better address the particular challenges posed in dealing with the state's use of AI evidence.

## B. Enhanced Supports

### LAO Budget Setting Programs

In addition, under the *Legal Aid Service Rules*, LAO has the authority to issue a budget where the proceeding is "exceptionally complex", and "the amount of the fees and disbursements for the proceeding is likely to exceed the available tariff."[162] The budget will determine what defence counsel is paid irrespective of the hours that would normally be paid for that matter under the tariff. Lawyers are still however limited by the applicable hourly rate.

Two other budget setting programs could be used to obtain to additional funding to challenge the use of AI generated evidence, for the defence of accused persons charged with the most serious and complex charges:

- "Big Case Management (BCM)" budgets may be issued if the total amount of the fees and disbursements for the criminal proceeding is likely to exceed $20,000, or if the criminal proceeding involves more than one accused person and the total amount of the fees and disbursements is likely to exceed $50,000 for all accused persons, or the preliminary hearing is likely to take more than 10 days.
- "Mid Case Management" budgets may be issued if the total amount of fees and disbursement for the proceedings is likely to be between $8,000 and $20,000 and the matter has been set down for trial or a preliminary inquiry. The availability of mid case budgets is limited to only certain kinds of offences. Recently, LAO significantly expanded the number of offences that may be eligible for mid case budgets in excess of what is provided under the tariff.[163]

In the past, BCM certificate funding was used to overturn the wrongful convictions of persons based on the use of unreliable pediatric forensic evidence as identified by the Goudge inquiry.

More generally, both BCM and MCM budget setting programs have proved successful in addressing the requirements that are often required in defending clients charged with the most serious and complex charges. LAO reports spending in 2022-2024 approximately $23.5 million on BCM certificates, as compared to $73.5 million on non-BCM certificates.[164]

Notably, however, while the expenditures of LAO funds on BCM matters is significant, it still represents very much the exception in terms of number of certificates, and clients impacted. LAO reports that in 2022-2023 it issued 56,207 certificates with an average cost of $1,674 per certificate,[165] much less than the threshold requirement for a BCM budget.

### Discretionary Payments

Counsel may also seek after the fact discretionary payments in excess of the maximum hours that can be billed under the tariff for matters for which they did not receive a case budget. These discretionary payments are only authorized in "exceptional circumstances" and if a properly informed reasonable private, paying client of modest means would have authorized the payment.[166]

In ascertaining whether the circumstances are sufficiently exceptional to authorize a discretionary payment above the regular tariff, LAO will look at the "result, complexity, contributions of the applicant and others, amount time set aside for a lengthy trial, and any other relevant factor."[167]

### Complex Case Rate and Panel

LAO introduced in 2011 a higher complex case rate (CCR) for the defence of persons charged with first or second-degree murder, and other kinds of serious and complex chargers. The CCR is only available for lawyers who have been qualified and admitted to LAO's CCR panel, and for cases that have been admitted to the Big Case Management program.[168] The complex case rate is $186.44 an hour.

The introduction of the CCR and the CCR panel flowed in part from a recommendation made by the Goudge Inquiry. The Inquiry recommended that LAO and the Province work to ensure that serious cases involving the use of forensic pediatric science are represented by lawyers with "necessary skill and expertise" to defend them. The recommendation was made so that in these kinds of serious cases the state's use of "complex medical evidence" could be "critically evaluated and potential challenged."[169]

The availability of the CCR is a way for LAO to ensure that in the most serious cases, involving the use of AI generated evidence, clients will have access to lawyers with the skill and expertise to "critically evaluate" that kind of evidence and "potentially challenge" its admission.

### Second Chair - Mentorship

In 2015, to support the quality of representation provided in certificate matters, including criminal law, LAO introduced a "second chair program." The program provides paid mentorship, or second chair authorizations, for both senior and less experienced lawyers on certificate cases.[170] These authorizations are in addition to what typically would be paid under LAO's governing tariff. While funds are limited for this program, it could certainly be accessed to improve the "hands on training" for defence counsel in reviewing, critically evaluating and even challenging the use of AI generated evidence.

### Test Case Program

As has been noted elsewhere,[171] LAO's test case program has the potential to provide additional funding to lawyers seeking to challenge the use of AI in criminal proceedings. Through its test case program, LAO is able to provide funding beyond what may be authorized under the tariff for meritorious cases that advance not only the interests of the individual client but also have a positive impact on a larger group of low-income Ontarians and Legal Aid clients.[172]

The Test Case Committee focuses its funding on litigation that will support particularly disadvantaged communities, who might not otherwise have been in a position to advance their case without that funding. The Committee has funded, often with in-kind support from other justice partners, successful litigation at all levels of court, including the Supreme Court of Canada, at various administrative tribunals, and in related proceedings. The budget for this program is limited. In 2022-2023, LAO funded 31 test cases with budgets totaling $459,732.[173]

The test case program works separate and apart from the federal government's Court Challenges Program, which has a similar focus in supporting *Charter* and human rights challenges to legislation.[174] The ability of counsel to access funds from the Court Challenges Program may, however, be a relevant consideration in determining whether a case may be admitted to LAO's Test Case Program.

Notably, while the Test Case Program may fund litigants who are involved in larger public interest litigation, under the terms of *the Legal Aid Services Act* (2020), eligibility for test case certificates, and funding, is limited to individual applicants and not to organizations.

### Continuing Legal Education and Distribution of Information

Over the last several years, LAO has grown its capacity to provide ongoing continuing legal education to both staff lawyers, including duty counsel, and LAO's private bar roster lawyers. These webinars often address issues relevant to all justice system participants, and may include presentations from Crowns and Judges, and non-legal experts. A proposal may be made to use "lunch and learns" as a platform to improve the scientific literacy of both staff lawyers, and the private bar, with respect to the new reality of artificial intelligence and the challenges it poses for LAO clients.

Finally, in the past, LAO has responded to the particular concerns of the Goudge Inquiry and the Motherisk Commission, by making available to roster lawyers, who are authorized to represent clients in legal aid matters, a list of experts who may provide assistance in understanding and potentially challenging unreliable forensic scientific evidence. A proposal may be made to expand this list to include experts who can provide similar assistance in understanding and potentially challenging the admission of AI evidence.

## C. Consultation Questions

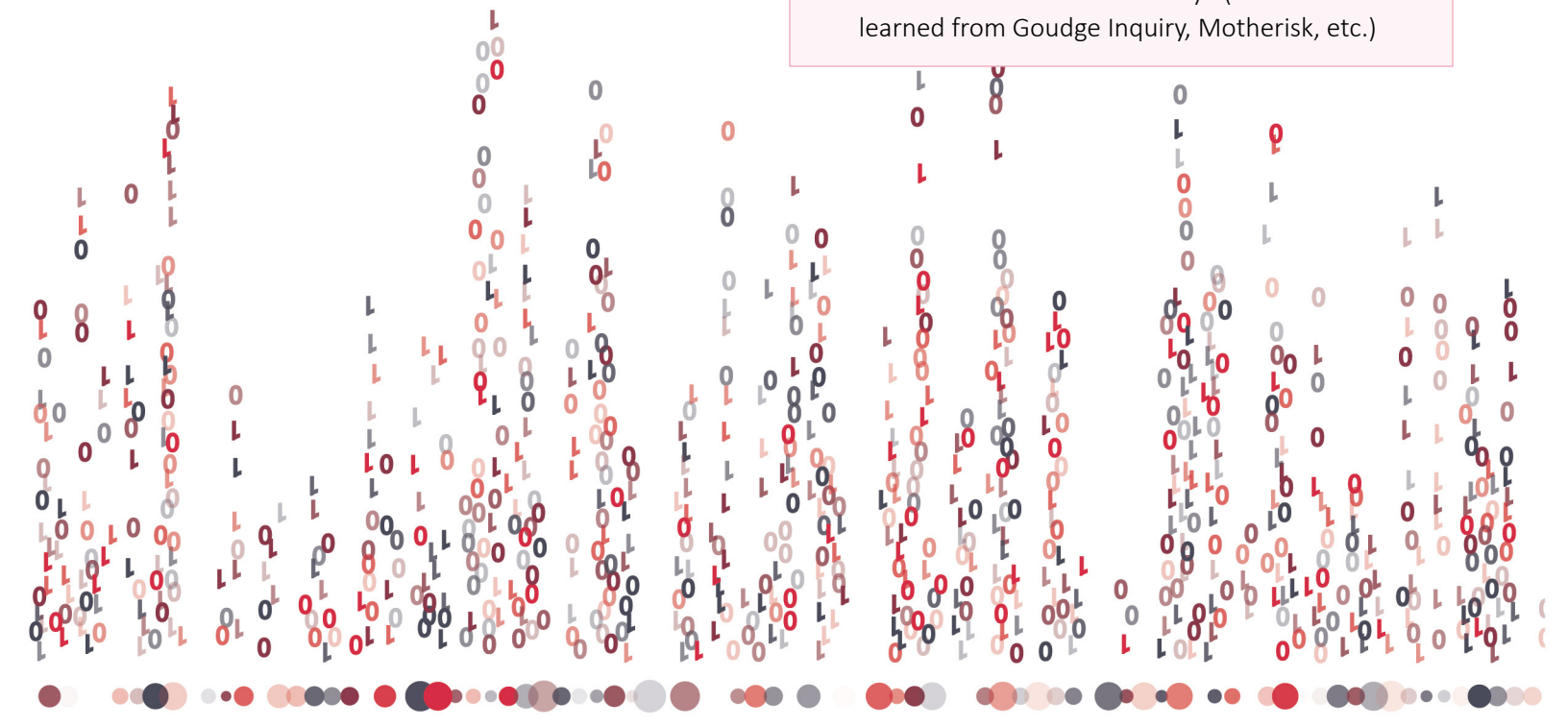
**12)** What remedies should be available outside of criminal justice alone where AI has been misused?

**13)** What supports are needed within the justice system to ensure state power on the use of AI is held in check?

- **a)** Assistance to defense counsel
- **b)** test case support
- **c)** office that can assist with centralized expertise – research, witnesses, etc – perhaps similar to LAO's research department for legal aid clinics
- **d)** accountability beyond criminal process – police oversight, judicial oversight, other independent authorities, complaints mechanisms, etc

**14)** What options exist to clarify how assertions on trade secrets are handled in the criminal justice sector? (CCC amendments? Courts develop a common rule or policy? It's an issue that crosses criminal and civil litigation)

**15)** Is there adequate guidance on expert evidence and standards for AI testimony? (See lessons learned from Goudge Inquiry, Motherisk, etc.)



# 4. Overarching and Interlocking Oversight Mechanisms

The previous section considered the oversight mechanisms within criminal law, including through trials and the application or extension of principles applied in comparable contexts of scientific or expert evidence. It also engaged in a thorough examination of the ways that individual cases might be funded through established legal aid mechanisms and programs to help interrogate the use of AI tools. The discussion suggests existing litigation systems possess the potential to effectively respond to challenges introduced by AI. The broad and purposive application of litigation principles and procedures – if properly resourced – suggest a framework capable of testing AI generated evidence, AI-enabled investigative tools, and other AI-enabled systems that may be deployed.

However, there are some fundamental differences between AI and other existing evidentiary and investigative tools. These differences suggest the need for a broader discussion about the role for general oversight and accountability of AI throughout the criminal justice system, above and beyond litigation as a singular check and balance.

First: "AI" refers to a rapidly growing and diversifying range of technologies and uses, not a single tool or even suite of tools. These applications may be technologically very different in terms of the way they work, they way they are trained, the way they are deployed, and the degree of transparency in their use, calibration, and explainability. The sheer diversity of AI-enabled systems and the rapid pace of development and adoption suggest an iterative, systemic, and enduring pressure on criminal litigation well beyond the historical impact of more occasional and discrete technologies.

Second: AI tools will not simply enter the justice system directly through investigative processes likely to be interrogated in court. As the other papers in this series discuss, AI tools may be used at all stages of the criminal justice lifecycle and by institutions both directly and indirectly involved in criminal justice. This points to the need to consider a an over-arching system, or interlocking systems, to oversee and track AI use system wide.

Third: A wide, diverse, and decentralized provincial network of institutions and actors play a role in developing, operating, overseeing, litigating, and adjudicating AI issues in Ontario's criminal justice system, potentially including:

- All 56 police services in Ontario.
- Police service boards, municipalities, and regional governments.
- The provincial Ministry of the Solicitor General (the Policing Division and Corrections).
- The provincial Ministry of the Attorney General.
- Crown Attorneys.
- Criminal judges sitting on both the Ontario Court of Justice and Superior Court.
- Criminal defence counsel.
- Criminal duty counsel.
- Legal Aid Ontario.
- Justices of the Peace.
- Other social supports, such as children's aid, family, immigration, and health care systems.
- Victim support services.
- Provincial oversight agencies (including the Ontario Human Rights Commission, Ontario Information and Privacy Commissioner, Law Enforcement Complaints Agency and the Inspectorate of Policing).

The coordination, access to justice and AI legal accountability challenges across this network are likely to be pervasive and difficult.

The final section of this paper explores a range of potential responses to the need for consistent, coherent, and systematic oversight of AI across this range of technologies, uses, institutions and impacts with the larger discussion of general oversight and accountability of AI. This looks both at the suitability and capacity of existing systemic oversight mechanisms and refers to innovations enacted and under development elsewhere.

## 4.1 Ontario's Commitments to Trustworthy AI and Criminal Justice Institutions and Oversight

It is fair to conclude from a groundswell of support that there is a growing consensus on the need for comprehensive AI regulation. Numerous organizations have made calls for robust regulation of both the public and private use of AI technologies, including:

- UN General Assembly and agencies;[175]
- Federal and provincial privacy commissioners;[176]
- Ontario's Human Rights Commission;[177]
- Public interest and academic institutions including the Law Commission of Ontario,[178] University of Toronto's *Citizenlab*[179] the *Canadian Civil Liberties Association*[180] and the Organization for Economic Cooperation and Development (OECD).[181]

Evidence of this consensus became more urgent in May 2023 when Ontario's Information and Privacy Commissioner (IPC) and the Ontario Human Rights Commission (OHRC) issued a joint statement on the use of AI technologies in Ontario. They noted how:

> …[I]t is urgent for the government to establish a binding set of robust and granular rules for public sector use of AI technologies. Such rules are necessary for Ontario to fully reap the benefits of AI technologies in a manner that is ethically responsible, accountable, sustainable, and supported by public trust. […][182]

The Commissions further emphasize that Ai guardrails must effectively address safety, privacy, accountability, transparency (including access to information), and human rights.[183]

"Trustworthy AI" is widely recognized as the flagship term that encompasses recommendations from these and other proponents. It has also been adopted by the province of Ontario in both its Trustworthy AI Framework and earlier published Principles for Ethical Use of AI.[184]

These policies emphasize that "trustworthy AI" is:

- Transparent and explainable, including "no AI in secret"
- Safe, with clearly defined risks and a proactive and preventative approach to mitigating those risks
- Accountable and responsible, including guarantees and processes to challenge AI decisions and a right to meaningful explanations
- Good, fair and rights respecting, including with reference to the rule of law, human rights, civil liberties, and democratic values. These include dignity, autonomy, privacy, data protection, non-discrimination, equality, and fairness.
- Human centric, sensible and appropriate.[185]

Subsequent to these commitments, Ontario introduced and shortly thereafter enacted Bill 194, the *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*.[186]

Unfortunately, Bill 194 appears unlikely meet commitments and expectations set by the provincial trustworthy AI policy frameworks. As summarized in submissions by the LCO, Bill 194 as drafted:

> "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. Simply stated, the problem is that the AI sections of Bill 194 are too brief (three sections, 1 ½ pages) and lack provisions that would ensure public sector AI use is beneficial, lawful, and accountable. More specifically, the Bill does not address the following widely acknowledged trustworthy AI priorities:
>
> - Human rights and procedural fairness.
> - AI systems in the criminal justice system.
> - AI systems used in courts and tribunals.
> - Public AI registries.
> - Impact assessments.
> - Risk categories and mitigation strategies.
> - Explainability requirements.
> - Governance requirements."[187]

Furthermore, the LCO notes the failure of Bill 194 to "address AI systems used by police or in the criminal justice system, which are widely acknowledged to be the highest risk public sector AI systems."[188]

This approach is likely to contribute to several foreseeable problems.

First: the criminal prosecution process must rely on the highest standards of trustworthy AI – yet Bill 194 is silent on the application of its framework to criminal justice, including police, the courts, and other entities. In the United States, this approach has resulted in "an extraordinary backlash to the use of AI and related tools in American criminal justice and courts... [an] experience [that] can teach Canadian policymakers many lessons."[189]

Second: the lack of legislative guidance means the multitude of criminal justice and criminal oversight institutions will not share a set of common standards to achieving "trustworthy AI" or in practices like:

- setting risk thresholds and criteria
- establishing presumptive prohibitions on highest-risk AI technologies and uses
- certification and testing standards
- mitigation standards
- and the like. Conflicting standards and inconsistent approaches are sure to introduce gaps likely to endanger rights and public confidence in the system.

Third: There are no standards proposed in Bill 194 for:

- any form of public AI registry to promote transparency.
- disclosure requirements, such as the mandatory disclosures required under Canada ADM Directive describing how components of an AI system work, the results of any reviews or audits, and a description of training data, among other criteria.
- notice to individuals who may be subject to AI systems or decisions.
- is currently systemic oversight mechanisms envisioned that would pull all these threads together. [190]

Collectively, the limits of Bill 194 suggest the need to explore law, policy and programmatic reforms responsive to the systemic need for oversight of AI in criminal justice. Examples can be drawn from jurisdictions including the European Union, United States, and an emerging private-sector tech assessment, validation and certification industry.

## 4.2 The Role of AI Oversight Regulators – Models in the US, EU and the Private Sector

Both the United States and EU envision a role for systemic oversight of AI systems across the multiple sectors that interact with criminal justice. Both jurisdictions have already begun enacting this oversight infrastructure, leaving Ontario (and Canada) lagging – but with a model to consider for possible adaptation and adoption here. Simultaneously, market-based solutions have also appeared, including private-sector entities offering AI system assessment, auditing, calibration, certification and reporting services.

### European Union AI Office

EU's *AI Act*, among other things, establishes a new EU level regulator, the European AI Office. Among other things, the AI office will

- monitor, supervise, and enforce the AI Act requirements;
- lead the EU in international cooperation on AI and strengthen bonds between the European Commission and the scientific community, including a forthcoming scientific panel of independent experts;
- help the 27 Member States cooperate on enforcement, including on joint investigations;
- act as the Secretariat of the AI Board, the intergovernmental forum for coordination between national regulators;
- support the creation of regulatory sandboxes where companies can test AI systems in a controlled environment;
- provide information and resources to small and medium businesses (SMEs) to aid in their compliance with rules.[191]

It would not be difficult to envision a similar arms-length regulator in Ontario or Canada, similar to a privacy or human rights commission, which is dedicated to ensuring the goals of its enabling legislation – i.e. the safe use of AI technologies and a more consistent approach to managing risks throughout and across systems, including criminal justice.

A regulator with these capabilities could provide additional and ongoing support to our existing oversight regime and adjudicative bodies which would benefit from the assistance in understanding AI technologies and the continuously evolving implications of their use. Courts and tribunals, which function as the enforcement mechanism of accountability in the use of AI technologies, could benefit from independent expert support in the form of *amicus curiae* or even expert research and policies published by the regulator.[192]

A regulator would also ensure that it is aware of and monitoring any and all developments in the field of AI. The EU's Office of AI is tasked with fostering connections with scientists but will also have a panel of independent experts. By engaging with experts on a regular basis or even integrating them with specialized roles in the regulatory body, an AI office would ensure that it remains up to date, and able to provide continuous legal education to judges, adjudicators, prosecutors and defense counsel (among others). That said, the question of who identifies, qualifies, and funds these experts remains to be answered, though it may be sensible for this to be actioned by the regulator itself.

## Offices of Technology Assessment

AI regulators could also expand their mandate to cover various other technologies which may require oversight similar to the Office of Technology Assessment (OTA) in the United States. It is indeed telling that nearly 30 years after the OTA's defunding there have been sustained calls for its revival, particularly in light of the challenges of AI. This includes a serious proposal published this year in the MIT Technology Review.[193]

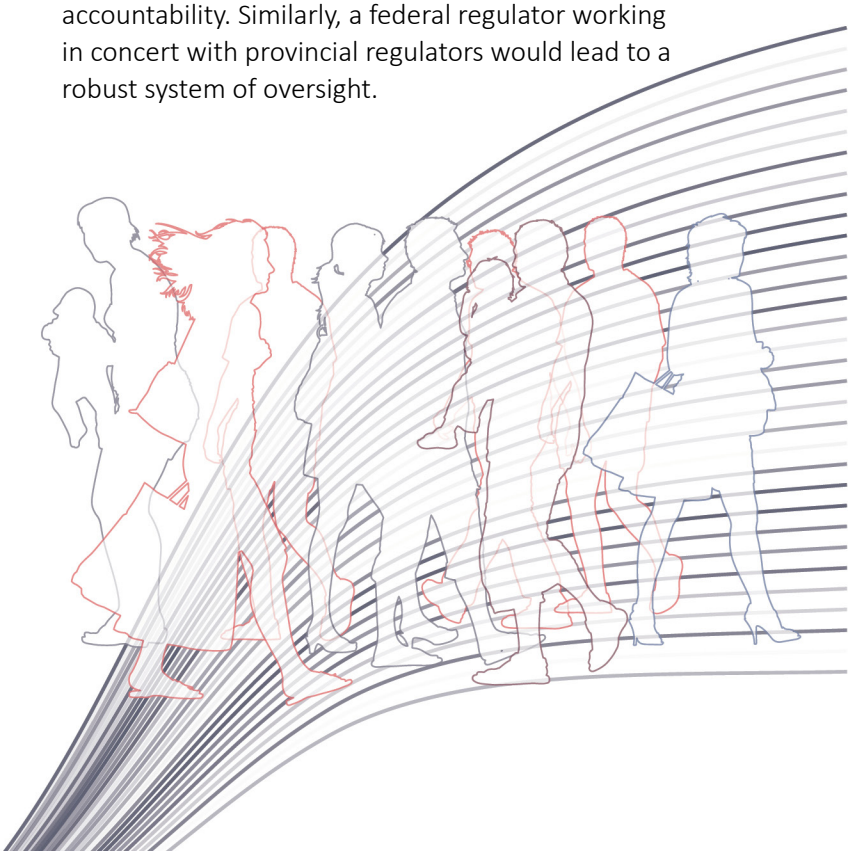
A similar mandate is established under the EU AIA. The EU AIA creates a comprehensive regulatory scheme that mandates a role for several independent investigatory, oversight, auditing, reporting, and assessment and certification bodies, with various of these functions and authorities either centralized in the European Commission or delegated to member states.[194] Several of these contribute to centralized technological assessment and standards settings to better ensure the validation, reliability, efficiency and certification of AI technologies. This network of offices include:

- **The Scientific Panel of Independent Exerts,** a panel that includes Commission-selected experts in the field of AI who contribute to evaluation schemes for AI; alerts the EU AI Office of possible systemic risks; and advises the AI Office on the classification of AI models including those with systemic risks.
- **The AI Advisory Forum,** an interdisciplinary Forum with a mandate to draw up opinions and recommendations including on harmonized AI standards across the EU, and which is made up of members with AI expertise that represent a balanced selection of stakeholders from industry, civil society and academia, as well as the Fundamental Rights Agency, the EU Agency for Cybersecurity and European standardization organizations.
- **The EU AI Board,** a committee that assists with the development of common criteria and shared understanding among competent authorities; assists with the creation and operation of, and cooperation between, AI regulatory sandboxes; and which issues opinions and recommendations related to the act's implementation, including on the development and application of codes of conduct, codes of practice, harmonized standards, and AI trends.[195]

## A Regulatory Marketplace for AI

Gillian Hadfield and Jack Clark have expressed the need for a regulatory marketplace, in which the government would regulate and promote many private regulators who would have the capacity to keep up with the dynamic nature of AI technologies.[196] While this is certainly one method which would allow for flexibility and growth, a centralized public regulator may be able to achieve the same result, so long as it remains focused on monitoring developments and reviewing oversight legislation on a regular basis. Alternatively, a public regulator could take the role of government in regulating private sub-regulators if it would lead to greater efficiency.

Ideally any legislative regulation would be harmonious in its federal and provincial application, in order to ensure comprehensive coverage of oversight and accountability. Similarly, a federal regulator working in concert with provincial regulators would lead to a robust system of oversight.



## 4.3 Oversight through privacy and data controls

Another key for the responsible and trustworthy use of AI in criminal justice relate to the kind and quality of data used to train AI systems.

It is now broadly recognized and accepted that biased data in means biased data out.[197]

Ensuring that AI systems trained for use in criminal justice control for biased data is one way to prevent discriminatory, unfair, or disparate results when using AI technologies.

This may take different forms. For instance, a requirement that all relevant AI systems used by actors in the justice system be trained on a central database of vetted or synthetic data sets.

Alternatively, the government could require that companies provide a full and detailed breakdown of the data used in the development of their technologies before allowing them to partake in any procurement process by criminal justice system entities as another way to ensure the quality of data.

Once again - this method is not without its issues. There is no such thing as a bias-free dataset, nor is the training data the only way in which bias can enter a decision system.[198] Synthetic data is also not perfect and can have quality issues of its own. While it may prove to be an improvement compared to real data in certain circumstances, it can suffer problems arising from being overly processed or not comprehensive enough. In addition, synthetic datasets may also accidentally retain some personally identifiable information from the sources from which it was created, which may lead to serious privacy concerns. In terms of procurement, companies may be hesitant or simply unwilling to delve into the details of their proprietary datasets. Finally, while quality data is important, it is only as good as the tool it is training or developing. Focusing on one element so heavily may lead to a lapse in scrutiny of the other.

As the authors of LCO AI in Criminal Justice Project Paper 4, *AI at Trial and On Appeal* note, the downstream effect of new technologies is foreseeable and, consequently, the need for a strong, effective, and comprehensive oversight regime for these technologies is similarly predictable.[199] It is critical that the government establish a robust and nimble oversight regime for the development, procurement and use of AI systems, that serves, as one goal, to provide appropriate safeguards and guardrails for the use of AI tools, to the extent they are determined to be fit for purpose, in the criminal justice system. Hopefully the discussion above will provide some inspiration to that end.

In light of the fact that public data is necessary to train AI,[200] but is also the output of AI, data privacy is a constant and ongoing concern. Has the data been sourced from reputable, legal sources? Was its collection consensual, or should it have been? Is the output of any AI technologies appropriately and securely stored? These questions among many others are critical to ensuring that privacy is central to the use of AI technologies.[201]

There are also larger questions that bridge the space between privacy and other *Charter* rights that privacy rights enable, including equality rights. While Canadian privacy legislation focuses primarily on the individual's right to assert control over personal information, AI technology raises significant questions of group and community privacy. As Bailey, Burkell and McPhail point out in their submission to the Standing Committee on Industry and Technology studying Bill C-27, in an algorithmically sorted society not just individual but also collective rights are jeopardised.[202] The privacy and equality implications of tools that take in information about individuals, process it, and use it to detect patterns that subsequently are used in decision making about groups are unlikely to be adequately captured by a focus on mitigating individual impacts of bias, yet that is Canada's current legislative approach in AIDA. Paper one in this series, which addresses the concept of predictive policing, and paper three which focuses on risk assessments each bring out these complications as they relate to tools with deeply consequential impacts on individuals interacting with the justice system.

## 4.4 AI Safety, Transparency, and Presumptive Prohibitions

The concept of safety as it relates to AI often refers to technical elements of a system: design, testing, data security and validation, but the principle of safety in the context of justice is one that requires a broader consideration. As already noted, AI technologies can make or lead to decisions or actions which can negatively affect the safety of those who are subject to those decisions or actions, many of whom belong to already marginalized communities. There are numerous examples of AI technologies being used in manner which has resulted in harm ranging from to the provision of government social services[203] to hiring practices,[204] policing[205] and more.

This is especially the case when AI technologies are relied on exclusively for decision making as opposed to informing human decision making. Across bodies as diverse as police and police service boards, forensics, and the SIU, there will be a tension between acquiring technically safe tools and making choices about tools that promote safety in the broader sense. It is useful to think carefully about which stages oversight can assist in promoting safety in both senses of the term, not just at during tool development but also at the point of procurement and subsequent monitoring requirements.

For instance, the transparency imperative extends from the creation of AI tools to their procurement and use in the criminal justice system. Two prominent examples are useful to consider when thinking the ways transparency principles should be applied to AI oversight in this sector. One is around transparency in procurement. There have been a series of 'reveals' by the media regarding police use of surveillance technologies in recent years, from Stingrays/IMSI Catchers[206] to spyware/ODITs[207] to Clearview AI facial recognition tools,[208] all procured and used for lengthy periods of time entirely without public awareness. The other obvious place where oversight will be critical relates to disclosure. A recent story in the Washington Post documents a study of police departments in 15 states, where facial recognition was used in more than 1000 criminal investigations, but was, records show, authorities "routinely failed to inform defendants about their use of the software—denying them the opportunity to contest the results of an emerging technology that is prone to error, especially when identifying people of color."[209]

Further, in order to ensure safety, an oversight regime or legislation must not shy away from placing prohibitions or moratoriums on the use of certain types of AI technologies, with as few exceptions as possible to those prohibitions.[210] As our brief review of relevant legislation and policies reveals, there are varying approaches to prohibitions or 'no go zones'. However, from an ethical perspective, it is precisely in those sectors where safety is most at risk that consideration should be given to the widest range of mitigation measures.

As mentioned above, Bill 194 lacks detail or guidance on prohibitions and restrictions on highest-risk AI technology and uses. These omissions heighten the foreseeable risks and harms of public sector AI systems, particularly in criminal law, and are likely to reduce public trust and accountability.

In contrast, many governments have enacted or proposed bans on certain technologies or their use in specific circumstances. Most notably, the EU AI Act creates a category of "unacceptable risk" in which AI systems are prohibited, including:

- Subliminal or Manipulative techniques: Using subliminal or manipulative techniques to distort decision-making leading to significant harm.
- Vulnerability Exploitation: Exploiting vulnerabilities due to age, disability, or social or economic situations, causing significant harm.
- Biometric Categorization: Inferring sensitive personal attributes such as race, political, religious or philosophical belief, trade union membership, through biometric systems, except for certain law enforcement purposes.
- Social Scoring: Evaluating or classifying individuals based on social behaviour or personal characteristics, leading to unfair or disproportionate treatment.

- Real-time Biometric Identification: 'Real-time' remote biometric identification in public spaces for law enforcement, with specific necessary exceptions
- Predictive Policing: Assessing the risk of criminal offences based solely on profiling or personality traits, except to support human assessments based on verifiable facts.
- Database Creation through scraping: Creating or expanding facial recognition databases through untargeted scraping from the internet or CCTV footage.
- Emotion Inference: Inferring emotions in workplaces or educational institutions, except for medical or safety reasons.[211]

The EU also pre-emptively identifies AI systems as high risk when deployed in one of these areas:

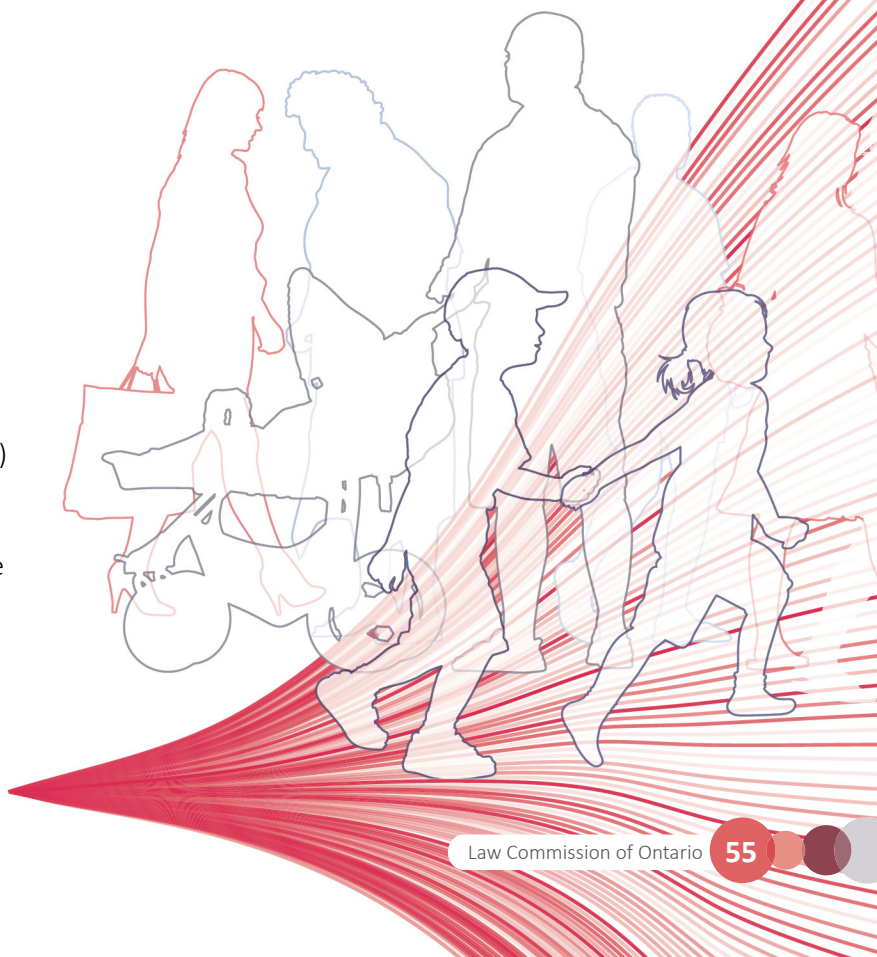
- Biometrics systems.
- Critical infrastructure management.
- Education and vocational training.
- Employment.
- Workers management and access to self-employment.
- Access to and enjoyment of essential services.
- Law enforcement.
- Migration.
- Asylum and border control management.
- Administration of justice and democratic processes.[212]

Furthermore, technologies increasingly used by law enforcement – including facial recognition and other biometric technologies – have probably been subject to the most (and most variable and complex) bans and restrictions. In the United States, for example, it appears more than 20 jurisdictions have enacted various types of bans and limitations on use of facial recognition technology, especially in law enforcement.[213]

## 4.5 Expert and community consultation

Experts, stakeholders, rights-holders and their advocates must be meaningfully included and involved in all phases of developing, implementing and evaluating AI technologies, including in exploring the risks and establishing the rationale, parameters and accountability associated with their use.[214]

Any such consultation will need to find effective ways and means to provide rights-holders, particularly those with involvement in the justice system who are vulnerable, with a voice. To some degree, the LCO is hoping to trigger some of the necessary public conversations through this discussion paper series. However, more broadly, consultation cannot be a 'one and done' exercise as the capacity, use cases, and implications of AI tools will change rapidly and repeatedly. Oversight mechanisms will need to consider ways to mandate ongoing consultation across the use lifecycle for high-risk tools, and iteratively as new tools emerge or are used in new ways in different parts of the justice system.



## 4.6 Human rights

Any oversight legislation should contain a recognition of human rights values and principles, and commitment to address systemic bias in AI that negatively affects or fails to appropriately account for the unique needs of marginalized communities.

Furthermore, the legislation should recognize that the use of AI technologies has the potential to facilitate discrimination (on both a systemic and individual level) as well as potentially infringe on human rights beyond discrimination. These series of papers have made this point abundantly clear.[215]

It is important to note that the ways rights might be infringed are as diverse as the AI-driven tools that present themselves for potential justice system use. Some are obvious, such as the potential chill on expressive and association rights if police bodycams were given live facial recognition capacity (although retroactive recognition from a stored data stream carries its own risks). Some are less clear; what, if any, would be the impact on an accused right to a fair trial if an AI tool used by their lawyer was faulty and failed to correctly include relevant precedents in a case scan prior to preparing a factum? Would it be useful for AI oversight to include human rights impacts assessments as a potential tool for ensuring the unique risks associated with any given technology implementation are adequately identified and addressed? How might such assessments be integrated into broader AI impact assessments? Should oversight or governance mechanisms require such tools be used?

## 4.7 Self-Regulation and Accountability

Though not currently mandated by any legislation or regulation, various organizations have taken it upon themselves to regulate their use of AI. Financial institutions, businesses, and some broader public service institutions have created policies or procedures in an attempt to self regulate the procurement and use of AI technologies. This paper discussed in section 2 the Toronto Police Services Board policy for the use and procurement of AI technologies by the Toronto Police Service. The policy was created following public consultation and consultation with various public and regulating bodies including the Ontario Human Rights Commission, the Information and Privacy Commissioner, and the Law Commission of Ontario. It covers a number of areas of importance, including a commitment to review the use of AI technologies which are already being used.

However, two years after the policy came into effect, concerns remain regarding its full implementation. The OHRC and IPC both set out these concerns in public letters, noting there to be confusion with regard to the process for reviewing AI technologies which were already being used by the TPS. While there was a process for grandfathering in these technologies, key elements of the process set out in the Board policy do not appear to have been followed.[216]

These concerns are emblematic of the fact that while there are benefits to self regulation- for example that parties turn their minds to potential issues with employing AI technologies and use internal resources to create policies to address those issues- there is ultimately little to no accountability ensuring that regulations are adhered to.

This lack of accountability in self-regulation relating to AI procurement and use, could pose a potential concern with regard to other actors in the criminal life cycle including courts, SIU, OIPRD/LECA and others.

Effective oversight requires accountability. As already noted, AIDA takes the approach of referring matters of non-compliance to a tribunal appointed by the Minister, while some have called for an independent arms-length public tribunal with full investigatory and enforcement power. The TPSB's AI policy allows complaints to be dealt with internally.

When considering the adequacy of accountability measures, the truism that justice must not only be done but be seen to be done is highly relevant, particularly in the context of AI technologies that suffer from high levels of hype coupled with a high degree of public distrust. The criminal justice system and its core constituent bodies rely to some extent on social license for legitimacy, particularly at a time of increasing political polarization coupled with an epidemic of mis and disinformation (fueled, ironically, by AI tools and business practices related tot heir use). Accountability as a consistent, visible, challengeable set of policies and processes is not just core to effective oversight, but critical to the ongoing reputation of the justice system as a whole.

This is one important reason to favour oversight measures of broader application than those built into the system itself. It has already been observed that the legal rights set out in the *Charter*, and the procedural provisions of the *Criminal Code* and the rules of evidence in the common law, and the *Canada Evidence Act*, can all be viewed as providing a level of oversight to law enforcement, the Crown and courts in their use and application of artificial intelligence. Such oversight is essential, but from a public accountability standpoint, arguably insufficient. Legal decisions hinge on careful consideration of complicated points of law within a specific factual situation. Larger social imperatives require larger scope for consideration and for public participation.

## 4.8 Consultation Questions

**16)** What are the appropriate mechanisms within the justice system for justice involved individuals to get prompt and full disclosure of data or AI analysis about that person as part of the proceeding?

**17)** How should justice sector institutions build capacity for the public to participate meaningfully in consultations? (Can point to other better examples in the public sector, like the Ministry of Health convening public citizen discussion panels they support with materials and get together several times a year for structured consultations.)

**18)** Ontario requires an entity or entities who are responsible 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 does AI oversight require some combination of capacity building within existing organizations as well as independent expertise?
- **b)** Does this require enabling legislation to facilitate collaboration across relevant criminal justice oversight bodies, incl investigations across those realms?
- **c)** Does this require an independent provincial commissioner or officer responsible for public oversight of public sector AI system, or building capacity among existing organizations?

**19)** What are the areas in criminal justice or shared or overlapping jurisdiction where Ontario should coordinate with the federal govt over the consideration or use of AI systems?

**20)** Does Bill 194 require clarity in governing "commercially-sourced data and technologies by law enforcement" and/or where law enforcement requests information held by commercial entities?

- **a)** Are current systems in criminal justice sufficiently robust to act as a check and balance on practices?
- **b)** How track and report on these kinds of requests?

# 5. Next Steps and Summary of Consultation Questions

## 5.1 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

## 5.2 Consultation Questions

1. Does Canada's approach to a risk-based framework that only captures and mitigates risks considered 'high' meet the needs of the justice system?

2. AIDA does not introduce prohibitions on technologies that are so high risk as to be unjustifiable for use in a democracy or under our *Charter*. Should it do so, and what might those technologies be in relation to the criminal justice system writ large?

3. It is clear that Ontario Bill 194 should identify policing, courts, corrections, and other criminal justice sector entities as prescribed "public sector entities" in Bill 194 that use AI. In that case:
   - Should this include related tribunals, for example, Criminal Injuries Compensation Board? Victims / Witness Assistance Programs?
   - Should this include court support programs, such as Community Diversion programs?
   - Are there exceptions that should be considered? What criteria should be developed or specific institutions / functions identified for exceptions? (ex: national security? Others?)

4. To achieve "accountability frameworks" under Bill 194 in criminal justice, should Bill 194 include a **provincially mandated impact assessment** that addresses privacy, human rights, and procedural fairness and provides assurances about how an AI system will comply with other legal obligations?
   - Should assessment along these lines be mandated?
   - What are the kinds of risks that should be included to develop a comprehensive and consistent criteria for assessments?
   - What mechanisms are necessary to ensure that this is being used consistently, and reported consistently?

5. Bill 194 provides for the possibility that some uses of AI may be prohibited by regulation. What technologies relevant to the criminal justice system might carry sufficient risk to make a prohibition on their use appropriate?

6. Under what circumstances in the criminal justice system might oversight be adequately achieved through self-directed and self-enforced policy? Is it possible to embed sufficiently meaningful accountability measures into such instruments for use in sensitive sectors?

7. In light of the questions about the effectiveness of the TPSB self-regulation, how might Ontario's Bill 194 address police use of AI technologies?
   - Should regulations under Bill 194 provide for oversight, an independent complaints process, or take other measures?
   - Might the risk categories and criteria that define them, as identified in the TPSB policy be enshrined in regulation and given the force of law?
   - Are those systems identified as extreme risk in the TPSB policy appropriate candidates for prohibitions under Bill 194?

8. If Ontario follows emerging best practice and incorporates a risk-based model and criteria (like EU AIA , AIDA, Federal AIA levels) and further establishes that prescribed entities are not allowed to determine their own risk:

   a) Will a binary model like the AIDA provide accountability in criminal justice? Or should there be more levels like the TPSB Use of AI Policy, or the EU or Federal AIA?

   b) What, if any AI tools should be prohibited for use because the risks they pose to *Charter* rights and civil liberties are simply too high:
      - biometric surveillance, and if so, under what conditions?
      - predictive policing tools?
      - other?

   c) Should this model specifically account for human rights, *Charter* rights, and procedural fairness, privacy analysis when considering the deployment of AI in criminal justice contexts?

**9.** With specific reference to the criminal justice system, Ontario should incorporate measures to mitigate risks of technologies used in all stages of the criminal justice lifecycle from investigations to court and corrections.

a) What mitigation measures should be considered and included? For example:
- Third party independent audits of data validity, reliability and relevancy; design/ source code; and unintended outcomes.
- Explainability requirements.
- Metrics testing
- De-biasing techniques
- Public and expert consultations.
- Public reporting requirements on pre-acquisition evaluations and post-acquisition performance review
- Others?

b) To what degree should court oversight and orders for certain AI uses be required? (compare to the EU AIA which requires court orders for various exceptional uses. EU also requires all these law enforcement applications AND any subsequent court orders to be disclosed to a public registry)

**10.** Should there be a prohibition on criminal justice sector provincial entities procuring, developing or deploying high-risk systems prior to Bill 194 and accompanying regulations being developed?

a) How should the grandfathering of existing AI systems be handled?

**11.** How and to what extent should the use of AI in criminal justice require a mandatory AI registry and disclosure of key elements of public sector AI systems?

a) Disclosure of the training data and transparency?

b) Disclosure of the output data for independent auditing and independent oversight, performance monitoring?

c) What are the resourcing needs to facilitate reporting to a mandatory AI registry?

d) How can a registry like this be effective while protecting other legitimate objectives, like sensitive investigating techniques?

**12.** What remedies should be available outside of criminal justice alone where AI has been misused?

**13.** What supports are needed within the justice system to ensure state power on the use of AI is held in check?

a) Assistance to defense counsel

b) test case support

c) office that can assist with centralized expertise – research, witnesses, etc – perhaps similar to LAO's research department for legal aid clinics

d) accountability beyond criminal process – police oversight, judicial oversight, other independent authorities, complaints mechanisms, etc

**14.** What options exist to clarify how assertions on trade secrets are handled in the criminal justice sector? (CCC amendments? Courts develop a common rule or policy? It's an issue that crosses criminal and civil litigation)

**15.** Is there adequate guidance on expert evidence and standards for AI testimony? (See lessons learned from Goudge Inquiry, Motherisk, etc.)

**16.** What are the appropriate mechanisms within the justice system for justice involved individuals to get prompt and full disclosure of data or AI analysis about that person as part of the proceeding?

**17.** How should justice sector institutions build capacity for the public to participate meaningfully in consultations? (Can point to other better examples in the public sector, like the Ministry of Health convening public citizen discussion panels they support with materials and get together several times a year for structured consultations.)

**18.** Ontario requires an entity or entities who are responsible 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 does AI oversight require some combination of capacity building within existing organizations as well as independent expertise?

b) Does this require enabling legislation to facilitate collaboration across relevant criminal justice oversight bodies, incl investigations across those realms?

c) Does this require an independent provincial commissioner or officer responsible for public oversight of public sector AI system, or building capacity among existing organizations?

**19.** What are the areas in criminal justice or shared or overlapping jurisdiction where Ontario should coordinate with the federal govt over the consideration or use of AI systems?

**20.** Does Bill 194 require clarity in governing "commercially sourced data and technologies by law enforcement" and/or where law enforcement requests information held by commercial entities?

a) Are current systems in criminal justice sufficiently robust to act as a check and balance on practices?

b) How track and report on these kinds of requests?

# Endnotes

1 *Canadian Charter of Rights and Freedoms*, being Part 1 of the *Constitution Act, 1982*, enacted as Schedule B to the *Canada Act 1982*, (1982, c. 11 (U.K.)) (in force April 17, 1982), online: https://laws-lois.justice.gc.ca/eng/const/page-12.html.

2 See: 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; 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), online: https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194; and 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.

3 See: 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; United States Congress, *Justice in Forensic Algorithms Act of 2024* (H.R.7394, 118th Congress (2023-2024)), online: https://www.congress.gov/bill/118th-congress/house-bill/7394/text; and New York City Council, *Public Oversight of Surveillance Technology Act* (Int. No. 487-A, enacted July 15, 2020), online: https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0.

4 See: *Canadian Charter of Rights and Freedoms*, being Part 1 of the *Constitution Act, 1982*, enacted as Schedule B to the *Canada Act 1982*, (1982, c. 11 (U.K.)) (in force April 17, 1982), online: https://laws-lois.justice.gc.ca/eng/const/page-12.html; *Criminal Code* (R.S.C., 1985, c. C-46), online: https://laws-lois.justice.gc.ca/eng/acts/C-46/; and *Canada Evidence Act* (R.S.C., 1985, c. C-5), online: https://laws-lois.justice.gc.ca/eng/acts/c-5/.

5 Law Commission of Ontario, *Regulating AI: Critical Issues and Choices* (April 2021),at p. 9, online: https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/regulating-ai-critical-issues-and-choices/.

6 Blair Attard-Frost, Ana Brandusescu and Kelly Lyons, "The governance of artificial intelligence in Canada: Findings and opportunities from a review of 84 governance initiatives" (Government Information Quarterly 41 (2), 2024).

7 Parliament of Canada, Bill C-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.

8 See preamble to Bill C-27.

9 AIDA s. 3 (1-2).

10 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), at 38, online: https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12751351/12751351/MinisterOfInnovationScienceAndIndustry-2023-11-28-Combined-e.pdf.

11 Canadian Bar Association, "Submission to the Standing Committee on Industry, Science and Technology re: Bill C-27, *Digital Charter Implementation Act, 2022*", online: https://cba.org/getmedia/12841d3c-2d91-4c91-88f7-50e543b812ea/24-12-eng-77bba701-fe68-44ee-ae56-041020676268.pdf.

12 BCCLA, "Submissions to the House of Commons Standing Committee on Industry and Technology regarding Bill C-27" (March 1, 2024), at p. 4, online: https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12951872/br-external/BritishColumbiaCivilLibertiesAssociation-e.pdf.

13 Kate Robertson, "Submission to the Standing Committee on Industry, Science and Technology re: Bill C-27, *Digital Charter Implementation Act, 2022*" online: https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12605754/br-external/RobertsonKate-Combined-e.pdf.

14 Kate Robertson, "Submission to the Standing Committee on Industry, Science and Technology re: Bill C-27, *Digital Charter Implementation Act, 2022*" online: https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12605754/br-external/RobertsonKate-Combined-e.pdf.

15 For a helpful legal summary see the Canadian Civil Liberties Association, "R. V. Spencer: Keeping Your Digital Identity Private " (April 13, 2017), online: https://ccla.org/get-informed/talk-rights/r-v-spencer-keeping-your-digital-identity-private/.

16 Kate Robertson, "Submission to the Standing Committee on Industry, Science and Technology re: Bill C-27, *Digital Charter Implementation Act, 2022*" at p. 9, online: https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12605754/br-external/RobertsonKate-Combined-e.pdf.

17 For a counterpoint argument that certain constraints will limit the collection of AI training data under this provision, see McCarthy Tetrault (Barry Sookman), "Legality of search engines and AI systems under PIPEDA and CPPA: Google v Privacy Commissioner" (October 9, 2023), online: https://www.mccarthy.ca/en/insights/blogs/techlex/legality-search-engines-and-ai-systems-under-pipeda-and-cppa-google-v-privacy-commissioner.

18 McCarthy Tetrault (Barry Sookman), "Legality of search engines and AI systems under PIPEDA and CPPA: Google v Privacy Commissioner" (October 9, 2023), online: https://www.mccarthy.ca/en/insights/blogs/techlex/legality-search-engines-and-ai-systems-under-pipeda-and-cppa-google-v-privacy-commissioner.

19 See Bill C-27 Part 2: *Personal Information and Data Protection Tribunal Act,* 2022.

20 See Canadian Civil Liberties Association, "Submission to the Standing Committee on Industry and Technology regarding Bill C-27" (September 12, 2023), online: https://ccla.org/wp-content/uploads/2023/09/Bill-C-27-Submission-to-INDU-CCLA.pdf.

21 The same point is made in Jane Bailey, Jacquelyn Burkell, and Brenda McPhail, "Submissions on Bill C-27 *The Digital Charter Implementation Act*", online: https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12605252/br-external/Jointly3-e.pdf.

22 See for example: Amnesty International Canada, "Study of BILL C-27, Submission to the Standing Committee on Industry and Technology" (March 1, 2024), online: https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12951650/br-external/Jointly12-067-240301-015-e.pdf; Women's Legal Education and Action Fund, "Submission to The Standing Committee on Industry and Technology on Bill C-27" (September 11, 2023), online: https://www.leaf.ca/wp-content/uploads/2023/09/2023-09-11-LEAF-Submission-re-AIDA-final.pdf.

23 Amnesty International Canada, "Study of BILL C-27, Submission to the Standing Committee on Industry and Technology" (March 1, 2024), online: https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12951650/br-external/Jointly12-067-240301-015-e.pdf.

24 Examples of such systems are OASYS (Offender Assessment System) used in the UK in the probation system to predict reoffending risk, or the COMPAS system in the US. For a helpful discussion of these systems, see The Conversation (Melissa Hamilton and Pamela Ugwidike), "A 'black box' AI system has been influencing criminal justice decisions for over two decades – it's time to open it up" (July 26, 2023), online: https://theconversation.com/a-black-box-ai-system-has-been-influencing-criminal-justice-decisions-for-over-two-decades-its-time-to-open-it-up-200594.

25 See for example, the Law Commission of Ontario, "Submission on *Bill 194: Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*" (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. Other similarly critical submissions include that of Prof. Teresa Scassa, "Submission to Consultation on Ontario's *Bill 194: Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*" (June 4, 2024), online: https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=383:submission-to-consultation-on-ontarios-bill-194-strengthening-cyber-security-and-building-trust-in-the-public-sector-act-2024&Itemid=80.

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

27 Thomas Linder, Brenda McPhail & Mervin Chatwin, "Submission on Bill 194: *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*" (unpublished, 2024).

28 For example, when the Toronto Police Service Board created their AI policy, they specifically highlighted a lack of provincial guidance, noting how "No current statutes or regulations fully govern the use of AI technologies in Ontario or Canada, and the province has not yet developed comprehensive guidelines for the use of such technologies in policing." See: Toronto Police Service Board, "Use of Artificial Intelligence Technology" (February 28, 2022), online: https://www.tpsb.ca/policies-by-laws/board-policies/195-use-of-artificial-intelligence-technology.

29 See Office of the Privacy Commissioner of Canada, "Privacy guidance on facial recognition for police agencies" (updated May 2, 2022), online: https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/.

30 Bennett Jones, "Unchartered territories: Canadian Courts and law societies grapple with the use of generative artificial intelligence tools" (May 23, 2024), online: https://www.bennettjones.com/Blogs-Section/Unchartered-Territories-Canadian-Courts-and-Law-Societies-Grapple-with-the-Use-of-Generative.

31 Bennett Jones, "Unchartered territories: Canadian Courts and law societies grapple with the use of generative artificial intelligence tools" (May 23, 2024), online: https://www.bennettjones.com/Blogs-Section/Unchartered-Territories-Canadian-Courts-and-Law-Societies-Grapple-with-the-Use-of-Generative.

32 For an analysis see Kent Roach, *Canadian Policing: Why and How It Should Change* (Toronto: Irwin Law, 2022), at p. 12.

33 See: European Parliament (2024). "Artificial Intelligence Act. Consolidated Text." Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html ; National Institute of Standards and Technology, "AI Risk Management Framework" (2023), online: https://www.nist.gov/itl/ai-risk-management-framework; Toronto Police Service Board, "Use of Artificial Intelligence Technology" (February 2022, updated January 2024), online: https://tpsb.ca/policies-by-laws/board-policies/195-use-of-artificial-intelligence-technology.

34 Toronto Police Service, "Artificial Intelligence" (undated), online: https://www.tps.ca/police-reform/artificial-intelligence/.

35 See Toronto Police Service, "Use of New artificial Intelligence Technology Policy – Public Consultation", online: https://tpsb.ca/ai.

36 See AIDA, ss. 6-12.

37 Toronto Police Service Board, "Use of Artificial Intelligence Technology" (February 2022, updated January 2024), at s. 1.iii, online: https://tpsb.ca/policies-by-laws/board-policies/195-use-of-artificial-intelligence-technology.

38 Information and Privacy Commissioner of Ontario, "Letter from Commissioner Patricia Kosseim to Ann Morgan, Chair, Toronto Police Services Board re: Update on the Implementation of the Board's Policy on Use of Artificial Intelligence Technology" (January 10, 2024), online: https://www.ipc.on.ca/sites/default/files/legacy/2024/01/2024-01-10-submission-to-the-january-11-2024-toronto-police-services-board-public-meeting-ai-policy-and-the-toronto-fr-mugshot-database-program-e.pdf.

39 See Brookings.edu, "The EU AI Act will have global impact, but a limited Brussels Effect" (June 8, 2022), online: https://www.brookings.edu/articles/the-eu-ai-act-will-have-global-impact-but-a-limited-brussels-effect/.

40 This analysis is taken from the policy paper prepared by Fair Trials, a global watchdog group studying and advocating for enhanced fairness in criminal trial. See Fair Trials, "Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU: Policy Paper" (2022), online: https://www.fairtrials.org/app/uploads/2022/01/Regulating-Artificial-Intelligence-for-Use-in-Criminal-Justice-Systems-Fair-Trials.pdf. Further discussion on the limitations on the Law Enforcement Directive can be found in Athina Sachoulidou, "Going beyond the 'common suspects:' to be presumed innocent in the era of algorithms, big data and artificial intelligence" (Artificial Intelligence and Law, February 2023), online: https://www.researchgate.net/publication/368716175_Going_beyond_the_common_suspects_to_be_presumed_innocent_in_the_era_of_algorithms_big_data_and_artificial_intelligence.

41 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.

42 For a timeline of how provisions of the EU AIA are phasing into force, see EU Artificial Intelligence Act, Implementation Timeline, online: https://artificialintelligenceact.eu/implementation-timeline/.

43 For a quick overview of these institutions and their intersecting roles, see IAPP.org, "EU AI Act Stakeholder Map" (May 2024), online: https://iapp.org/media/pdf/resource_center/eu_ai_act_stakeholder_map.pdf.

44 See EU Artificial Intelligence Act, Article 5, s. 3 and 6.

45 See: European Union, "Regulation (EU) 2016/679 (General Data Protection Regulation) (April 27, 2016), online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679; European Union, "Directive (EU) 2016/680 (on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties" (April 27, 2016), at article 38, online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680. Specifically, see GDPR article 22, "Automated individual decision-making, including profiling," online: https://gdpr-info.eu/art-22-gdpr/.

46 European Union, "Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016" (April 27, 2016), at article 9, online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680.

47 Fair Trials, "Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU: Policy Paper" (2022), at p. 6, online: https://www.fairtrials.org/app/uploads/2022/01/Regulating-Artificial-Intelligence-for-Use-in-Criminal-Justice-Systems-Fair-Trials.pdf.

48 Fair Trials, "Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU: Policy Paper" (2022), at p. 6, online: https://www.fairtrials.org/app/uploads/2022/01/Regulating-Artificial-Intelligence-for-Use-in-Criminal-Justice-Systems-Fair-Trials.pdf.

49 See Law Commission of Ontario (Ryan Fritsch), "Law Enforcement Use of AI: Paper 2 in the LCO AI in Criminal Justice Project" (Toronto: April 2025), at s. 1.2, 2.1, online: https://www.lco-cdo.org/CrimAI. See also, Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (January 23, 2018).

50 Fair Trials, "Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU: Policy Paper" (2022), at p. 6, online: https://www.fairtrials.org/app/uploads/2022/01/Regulating-Artificial-Intelligence-for-Use-in-Criminal-Justice-Systems-Fair-Trials.pdf.

51 Athina Sachoulidou, "Going beyond the 'common suspects:' to be presumed innocent in the era of algorithms, big data and artificial intelligence" (Artificial Intelligence and Law, February 2023), at p. 52, online: https://www.researchgate.net/publication/368716175_Going_beyond_the_common_suspects_to_be_presumed_innocent_in_the_era_of_algorithms_big_data_and_artificial_intelligence.

52 European Union, "Directive (EU) 2016/680 (on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties" (April 27, 2016), at article 44, online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L0680.

53 Athina Sachoulidou, "Going beyond the 'common suspects:' to be presumed innocent in the era of algorithms, big data and artificial intelligence" (Artificial Intelligence and Law, February 2023), at. P 33, online: https://www.researchgate.net/publication/368716175_Going_beyond_the_common_suspects_to_be_presumed_innocent_in_the_era_of_algorithms_big_data_and_artificial_intelligence.

54 Athina Sachoulidou, "Going beyond the 'common suspects:' to be presumed innocent in the era of algorithms, big data and artificial intelligence" (Artificial Intelligence and Law, February 2023), at p 35, online: https://www.researchgate.net/publication/368716175_Going_beyond_the_common_suspects_to_be_presumed_innocent_in_the_era_of_algorithms_big_data_and_artificial_intelligence.

55 Fair Trials, "Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU: Policy Paper" (2022), at p. 6, online: https://www.fairtrials.org/app/uploads/2022/01/Regulating-Artificial-Intelligence-for-Use-in-Criminal-Justice-Systems-Fair-Trials.pdf.

56 See: United States Congress, *Justice in Forensic Algorithms Act of 2024* (H.R.7394, 118th Congress (2023-2024)), online: https://www.congress.gov/bill/118th-congress/house-bill/7394/text. As of February 2024, the Bill has been referred for consideration to the Committee on the Judiciary and to the Committee on Science, Space, and Technology. See also The Verge, "New bill would let defendants inspect algorithms used against them in court" (February 15, 2024), online: https://www.theverge.com/2024/2/15/24074214/justice-in-forensic-algorithms-act-democrats-mark-takano-dwight-evans.

57 See Rebecca Wexler, "Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System" (70 Stanford Law Review 2018), online: https://review.law.stanford.edu/wp-content/uploads/sites/3/2018/06/70-Stan.-L.-Rev.-1343.pdf.

58 *State v. Loomis* (881 N.W.2d 749, 760-61 (Wis. 2016)), *cert. denied*, 137 S. Ct. 2290 (2017).

59 See *Robinson v. Commonwealth* (No. 25 WDM 2016 (Pa. Super. Ct. Mar. 7, 2016), "Petition for Review Filed by Defendant Michael Robinson" (at p. 4), cited in Rebecca Wexler, "Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System" (70 Stanford Law Review 2018), online: https://review.law.stanford.edu/wp-content/uploads/sites/3/2018/06/70-Stan.-L.-Rev.-1343.pdf.

60 See: Human Rights Watch, "Letter to Matt Dummermuth, Principal Deputy Assistant Attorney General re: Child Protection System software suite" (February 1, 2019), online: https://www.documentcloud.org/documents/5788168-Porn-Story-Documents/#document/p17/a491807.

61 See Law Commission of Ontario (Armando D'Andrea and Gideon Christian), "AI and the Assessment of Risk in Bail, Sentencing and Recidivism: Paper 3 in the LCO AI in Criminal Justice Project" (Toronto: April 2025), at ss. 2.2, 2.3, 3.2.1, 3.2.2, 3.4.5, 3.5.1, online: https://www.lco-cdo.org/CrimAI.

62 At present see the NIST.gov, Computer Forensics Tool Testing Program, online: https://www.nist.gov/itl/ssd/software-quality-group/computer-forensics-tool-testing-program-cftt.

63 United States Congress, *Justice in Forensic Algorithms Act of 2024* (18th Congress, 2D Session, H. R. 7394), online: https://www.govinfo.gov/content/pkg/BILLS-118hr7394ih/pdf/BILLS-118hr7394ih.pdf.

64 See NIST Privacy Engineering Program, online: https://www.nist.gov/itl/applied-cybersecurity/privacy-engineering.

65 See 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.

66 See NIST, "AI Research", online: https://www.nist.gov/ai-research.

67 United States Congress, *Justice in Forensic Algorithms Act of 2024* (H.R.7394, 118th Congress (2023-2024)), online: https://www.congress.gov/bill/118th-congress/house-bill/7394/text.

68 United States Congress, *Justice in Forensic Algorithms Act of 2024* (H.R.7394, 118th Congress (2023-2024)), online: https://www.congress.gov/bill/118th-congress/house-bill/7394/text.

69 See United States Government Accountability Office, "Testimony of Dr. Karen L. Howard Before the Subcommittee on Criminal Justice and Counterterrorism, Committee on the Judiciary, U.S. Senate" (January 24, 2024), online: https://www.judiciary.senate.gov/imo/media/doc/2024-01-24_pm_-_testimony_-_howard.pdf.

70 United States Government Accountability Office, "Testimony of Rebecca Wexler Before the Subcommittee on Criminal Justice and Counterterrorism, Committee on the Judiciary, U.S. Senate" (January 24, 2024), online: https://www.judiciary.senate.gov/imo/media/doc/2024-01-24_pm_-_testimony_-_wexler.pdf.

71 New York City Council, *Creating comprehensive reporting and oversight of NYPD surveillance technologies* (NYC Local Law 2020/065 (enacted July 15, 2020), online: https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0.

72 See NYPD, Public Oversight of Surveillance Technology (POST) Act Impact and Use Policies, online: https://www.nyc.gov/site/nypd/about/about-nypd/policy/post-act.page.

73 *Canada Evidence Act* (R.S.C., 1985, c. C-5), online: https://laws-lois.justice.gc.ca/eng/acts/c-5/.

74 *R. v. Spencer* (2014 SCC 43) in which the reasonable expectation of privacy attached to subscriber information associated with an IP address. Followed in *R. v. Bykovets* (2024 SCC 6) in which the reasonable expectation of privacy attaches to am individual's IP address.

75 *R. v. Ward* (2012 ONCA 660) at para. 71.

76 R. v. Wise (1992 CanLII 125 (SCC)).

77 R. *v. Ahmad* (2020 SCC 11).

78 *R. v. Chehil* (2013 SCC 49) at para 39.

79 *R. v. Sharma* (2022 SCC 39).

80 Point conceded in argument by Crown in *R. v. B.H.D.* (2006 SKPC 32).

81 See *R. v. Stinchcombe* (1991 CanLII 45 (SCC)) followed, in the context of "advanced software tools capable of automated surveillance, detection, connection and downloading of child pornography from suspect users on peer-to-peer networks" in *R. v Hughes* (2022 ONSC 2164).

82 *R. v. McNeil* (2009 SCC 3) followed in *R. v Hughes* (2022 ONSC 5209).

83 See *Criminal Code* s. 493.2.

84 See *Criminal Code* s. 515(13.1)

85 See *Criminal Code* s. 718.2; *R. v. Morris* (2021 ONCA 680); *R. v. Anderson* (2021 NSCA 62).

86 See detailed discussion in chapter 7, "AI and Evidence Law" in Jesse Beatson, Gerald Chan, Jill R. Presser (eds.), *Litigating Artificial Intelligence* (Toronto: Emond, May 2020).

87 See *M.A.B. v. M.G.C.* (2021 ONSC 8572) following W*hite Burgess Langille Inman v. Abbott and Haliburton Co.* (2015 SCC 23); *R. v. Abbey (No. 2)* (2017 ONCA 640).

88 *R. v. Mohan* ((1994), 2 SCR 9) at para. 25.

89 See for instance *R. v. Edwards* ([1996] 1 SCR 128), though this does not address larger arguments about *Charter* s.7 implications.

90 The Citizen Lab, *To Surveil and Predict A Human Rights Analysis of Algorithmic Policing in Canada* (September 1, 2020), at p. 145, online: https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/.

91 The limited scope of remedies will be addressed in the discussion that follows.

92 *R. v. Orlandis-Habsburgo* (2017 ONCA 649) at para. 41.

93 See discussion below with respect to the growth of the common law powers of arrest and detention without legislative constraints.

94 See conclusion of Kaitlynd Hiller, "Predictive Policing and the Charter" (44-6 *Manitoba Law Journal* 224 (2021)), online: https://canlii.ca/t/tssw.

95 *R. v. Chehil* (2013 SCC 49) at para. 40.

96 *R. v. Chehil* (2013 SCC 49) at para. 40

97 Kaitlynd Hiller, "Predictive Policing and the Charter" (44-6 *Manitoba Law Journal* 224 (2021)), online: https://canlii.ca/t/tssw.

98 See analysis in the following: Vanessa MacDonnell, "Assessing the Impact of the Ancillary Powers Doctrine on Three Decades of Charter Jurisprudence" (The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference 57 (2012)), online: https://digitalcommons.osgoode.yorku.ca/sclr/vol57/iss1/10; James Stribopoulos, "A Failed Experiment? Investigative Detention: Ten Years Later" (41 Alta. L. Rev. 335 (2003)), at p. 380-81, 390-92.

99 *R. v. Clayton* ([2007] S.C.J. No. 32) at para. 79 *per* Binnie J.

100 Vanessa MacDonnell, "Assessing the Impact of the Ancillary Powers Doctrine on Three Decades of Charter Jurisprudence" (The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference 57 (2012)), at p. 236, online: https://digitalcommons.osgoode.yorku.ca/sclr/vol57/iss1/10.

101 James Stribopoulos, "A Failed Experiment? Investigative Detention: Ten Years Later" (41 Alta. L. Rev. 335 (2003)), at p. 381.

102 James Stribopoulos, "A Failed Experiment? Investigative Detention: Ten Years Later" (41 Alta. L. Rev. 335 (2003)), at p. 381.

103 James Stribopoulos, "A Failed Experiment? Investigative Detention: Ten Years Later" (41 Alta. L. Rev. 335 (2003)), at p. 381.

104 This analysis is adopted from Kent Roach, *Remedies for Human Rights Violations: A Two-Track Approach to Supra-national and National Law* (Cambridge: Cambridge University Press (2021)).

105 *R. v. Collins* ([1987] 1 SCR 265).

106 *R. v. Grant* ([2009] 2 SCR 353).

107 David Paciocco, "Section 24(2): Lottery or Law" – The Appreciable Limits of Purposive Reasoning" (58 C.L.Q. 15 (2011)), as quoted in Kent Roach, *Remedies for Human Rights Violations: A Two-Track Approach to Supra-national and National Law* (Cambridge: Cambridge University Press (2021)) at 329.

108 See Kent Roach, *Remedies for Human Rights Violations: A Two-Track Approach to Supra-national and National Law* (Cambridge: Cambridge University Press (2021)).

109 It is not, for example, a remedy to address illegal conditions of imprisonment. See Kent Roach, above.

110 Kent Roach, *Remedies for Human Rights Violations: A Two-Track Approach to Supra-national and National Law* (Cambridge: Cambridge University Press (2021)) at 118.

111 *R. v. Golden,* [2001] 3 SCR 679.

112 Kent Roach, *Remedies for Human Rights Violations: A Two-Track Approach to Supra-national and National Law* (Cambridge: Cambridge University Press (2021)) at 341.

113 *R. v. Im* (2016 ONCJ 383) at para. 27, followed in *R. v. Owusu* (2023 ONCJ 568).

114 *R. v. Sharma* (2022 SCC 39).

115 *R. v. Sharma* (2022 SCC 39) at para. 218.

116 See Colton Fehr, "Reflections on the Supreme Court of Canada's Decision in *R. Sharma*" (Alberta Law Review 60 (2023)) at 944.

117 *Ewert v. Canada* (2018 SCC 30).

118 *Ewert v. Canada* (2018 SCC 30) at para. 79.

119 There was a dissenting opinion from the majority's view that the government failed to meet its obligations under the *Correctional and Conditional Release Act*, see below.

120 *Ewert v. Canada* (2018 SCC 30) at para. 79.

121 *Corrections and Conditional Release Act* (S.C. 1992, c. 20), online: https://laws-lois.justice.gc.ca/eng/acts/C-44.6/.

122 *Ewert v. Canada* (2018 SCC 30) at para. 3.

123 Emily Hill and Jessica Wolfe, "Ewert v. Canada: Shining Light on Corrections and Indigenous People" (The Supreme Court Law Review: Osgoode's Annual Constitutional Cases Conference 94 (2020)), online: https://digitalcommons.osgoode.yorku.ca/sclr/vol94/iss1/15.

124 *R. v. Natomagan* (2022 ABCA 48).

125 *Ewert v. Canada* (2018 SCC 30) at para. 67.

126 The minority opinion in *Ewert* (at para. 124) is quite effective in calling attention to the challenges for CSC officials in determining precisely what "reasonable steps" are required to take in meeting its obligations under s.24(1) of the CCRA.

127 Professor Teresa Scassa provides an excellent summary of the *Ewert* decision in relation to AI regulation. See: Teresa Scassa, "Supreme Court of Canada Decision Has Relevance for Addressing Bias in Algorithmic Decision-Making" (June 14 2018), online: https://www.teresascassa.ca/index.php?option=com_k2&view=item&id=278:supreme-court-of-canada-decision-has-relevance-for-addressing-bias-in-algorithmic-decision-making&Itemid=80.

128 See *R. v. Mohan* ((1994), 2 SCR 9) at para. 25 and the discussion in "Tactical Challenges and Practical Considerations in Litigating AI" chapter 6 in Jesse Beatson, Gerald Chan, Jill R. Presser (eds.), *Litigating Artificial Intelligence* (Toronto: Emond, May 2020).

129 See the discussion in "Spies and Robots: Litigating the Use of AI in National Security Proceedings" in Jesse Beatson, Gerald Chan, Jill R. Presser (eds.), *Litigating Artificial Intelligence* (Toronto: Emond, May 2020), at p. 304.

130 See for example *R. v. Abbey* (2017 ONCA 640) and *R. v. J.-(L.J.)* (2000 SCC 51).

131 Emma Cunliff and Gary Edmond, "Gaitkeeping in Canada: Mis-steps in Assessing the Reliability of Expert Testimony"(92 Canadian Bar Review 327 (2014)), online: https://canlii.ca/t/28g1. To similar effect, see Gary Edmond, "Forensic Science and the Myth of Adversarial Testing" (32(2) Current Issues in Criminal Justice 1 (December 2019)), online: https://www.researchgate.net/publication/337678402_Forensic_science_and_the_myth_of_adversarial_testing.

132 Gary Edmond, Simon Cole, Emma Cunliffe and Andrew Roberts, "Admissibility Compared: The Reception of Incriminating Expert Evidence ( i.e., Forensic Science) in Four Adversarial Jurisdictions" (3 U Denver Crim L Rev 31 (2013)) at p. 89, online: https://commons.allard.ubc.ca/fac_pubs/79/.

133 Gary Edmond, Simon Cole, Emma Cunliffe and Andrew Roberts, "Admissibility Compared: The Reception of Incriminating Expert Evidence ( i.e., Forensic Science) in Four Adversarial Jurisdictions" (3 U Denver Crim L Rev 31 (2013)) at p. 71, online: https://commons.allard.ubc.ca/fac_pubs/79/.

134 Emma Cunliffe and Gary Edmond, "What Have Learned? Lessons from Wrongful Convictions" in *To Ensure Justice is Done, Essays in Memory of Marc Rosenberg* (Toronto: Thompson Reuters, 2017).

135 See Province of Ontario, The Inquiry into Pediatric Forensic Pathology in Ontario (2008), online: https://www.archives.gov.on.ca/en/e_records/goudge/.

136 Hon. J.C. Beaman. *Harmful Impacts: The reliance on hair testing in child protection, Report of the Motherisk Commission* (Ontario Ministry of the Attorney General, February 2018), online: https://www.archives.gov.on.ca/en/e_records/motheriskcommission/wp-content/uploads/Report-of-the-Motherisk-Commission.pdf.

137 See discussion in: Gary Edmond "What Lawyers Should Know About Forensic Sciences" 36 Adelaide Law Review *33* (2015)*;* and Samatha Savage, "The Reliability of Expert Evidence in Canada: Safeguarding Against Wrongful Convictions" (Wrongful Conviction Review 33 (2022)).

138 See: Province of Ontario, The Inquiry into Pediatric Forensic Pathology in Ontario (2008), *Volume 3: Policy and Recommendations*, online: https://www.fixcas.com/news/2008/Vol_3_Eng.pdf. The question of Legal Aid supports to challenge unreliable scientific evidence is a separate topic that is addressed below.

139 CM Milroy, "The Goudge Inquiry and Forensic Pathology in Canada" (13(2) Acad Forensic Pathol. 61 (June 2023)), online: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10338733/pdf/10.1177_19253621231167016.pdf.

140 See discussion in "Chapter 6 – Forensic Evidence and Expert Evidence" in *Innocence at Stake: The Need for Continued Vigilance to Prevent Wrongful Convictions in Canada: Report of the Federal/Provincial/Territorial Heads of Prosecutions Subcommittee on the Prevention of Wrongful Convictions* (2018), online: https://www.ppsc-sppc.gc.ca/eng/pub/is-ip/is-ip-eng.pdf.

141 Hon. J.C. Beaman. *Harmful Impacts: The reliance on hair testing in child protection, Report of the Motherisk Commission* (Ontario Ministry of the Attorney General, February 2018), at p. 110, online: https://www.archives.gov.on.ca/en/e_records/motheriskcommission/wp-content/uploads/Report-of-the-Motherisk-Commission.pdf.

142 Hon. J.C. Beaman. *Harmful Impacts: The reliance on hair testing in child protection, Report of the Motherisk Commission* (Ontario Ministry of the Attorney General, February 2018), at p 118, online: https://www.archives.gov.on.ca/en/e_records/motheriskcommission/wp-content/uploads/Report-of-the-Motherisk-Commission.pdf.

143 Emma Cunliffe & Gary Edmond, "Reviewing Wrongful Convictions in Canada" (64:3-4 Crim LQ 473 (2017)); and Emma Cunliffe and Gary Edmond, "What Have Learned? Lessons from Wrongful Convictions" in *To Ensure Justice is Done, Essays in Memory of Marc Rosenberg* (Toronto: Thompson Reuters, 2017).

144 This direct admission of evidence would likely require amendments to the *Criminal Code* and the *Canada Evidence Act*

145 See discussion in Emma Cunliffe & Gary Edmond, "Reviewing Wrongful Convictions in Canada" (Criminal Law Quarterly Law 473 (2017)).

146 See Government of Canada, Bill C-40, *An Act to amend the Criminal Code, to make consequential amendments to other Acts and to repeal a regulation (miscarriage of justice reviews)* (Royal Assent December 17, 2024), online: https://www.parl.ca/documentviewer/en/44-1/bill/C-40/royal-assent.

147 Hon. Harry LaForme and Hon. Juanita Westmoreland-Traoré, *A Miscarriages of Justice Commission: Final Report* (November 2021), online: https://www.justice.gc.ca/eng/rp-pr/cj-jp/ccr-rc/mjc-cej/docs/a-miscarriages-of-justice-commission-published-version.pdf.

148 See Law Commission of Ontario, *Regulating AI: Critical Issues and Choices* (Toronto: April 2021)l; "Tactical and Practical Considerations in Litigating AI," chapter 6 in Jesse Beatson, Gerald Chan, Jill R. Presser (eds.), *Litigating Artificial Intelligence* (Toronto: Emond, May 2020); and Fair Trials, "Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU: Policy Paper" (2022), at p. 6, online: https://www.fairtrials.org/app/uploads/2022/01/Regulating-Artificial-Intelligence-for-Use-in-Criminal-Justice-Systems-Fair-Trials.pdf.

149 Eligible persons may apply for and receive a Legal Aid certificate, which is like a voucher that covers the cost of a lawyer for a certain number of hours. Certificates are issued for matters in different areas of law including criminal, family, and immigration and refugee law.

150 See Legal Aid Ontario, "A legal strategy for bail" (2018), online: https://www.legalaid.on.ca/documents/a-legal-aid-strategy-for-bail/. This estimate accords with more recent Ontario Court of Justice 2021 data, where the majority of bail hearings are held, that approximately 65% of individuals were represented by LAO duty counsel. See Ontario Anti-Racism Directorate, "Annual progress report 2022: Ontario's Anti-Racism Strategic Plan" (September 20, 2022), online: https://www.ontario.ca/page/annual-progress-report-2022-ontarios-anti-racism-strategic-plan.

151 *R. v. Parsons* (2009 ONCJ 763) at para. 82.

152 *R. v. Ghany* (2006 CanLII 24454 (ON SC)) at para. 62, citing Trotter J., *The Law of Bail in Canada* (Toronto: Carswell Thomson Profession Publishing, 1999).

153 Legal Aid Ontario, "2022-2023 Annual Report", online: https://www.legalaid.on.ca/wp-content/uploads/LAO-annual-report-2022-23-EN.pdf.

154 Legal Aid Ontario, "Legal Aid Services Rules Made under the *Legal Aid Services Act, 2020*" (consolidated March 3, 2025), online: https://www.legalaid.on.ca/wp-content/uploads/Legal-Aid-Services-Act-2020_Rules-EN.pdf.

155 Legal Aid Ontario, "Legal Aid Services Rules Made under the *Legal Aid Services Act, 2020*" (consolidated March 3, 2025), online: https://www.legalaid.on.ca/wp-content/uploads/Legal-Aid-Services-Act-2020_Rules-EN.pdf. Note that duty counsel do not generally bring bail reviews on behalf of clients.

156 See Legal Aid Ontario, "New expedited habeas corpus certificate application process for bail hearings" (October 23, 2023), online: https://www.legalaid.on.ca/in-briefs/new-expedited-habeas-corpus-certificate-application-process-for-bail-hearings/.

157 The block fees are set out in schedules attached to the Legal Aid Service Act Rules. The fees that are available depend on the type of matter (summary [$887.28] or indictable [$1,495.68]), how the matter is resolved (guilty plea or withdrawn), and whether there whether other ancillary block fees that are available (i.e. bail hearings and reviews [see above], use of a Gladue or IRCA report [$502.53] or a "mental health enhancer" [$251.27]). There are slightly higher block fees for matters in the Northern regions of the province. These are the block fees that are available as of April 1, 2024. As set out in the Rules, they are subject to an increase on April 1, 2025.

158 The pay rate was updated in April 2025. See Schedule 2 to the Legal Aid Services Rules (made under the Legal Aid Services Act, 2020 (consolidated March 31, 2025)), online: https://www.legalaid.on.ca/wp-content/uploads/Legal-Aid-Services-Act-2020_Rules-EN.pdf.

159 See Legal Aid Services Rules.

160 Further description about these categories is provided in the LAO Rules setting out the tariff, and the offences themselves are provided on LAO's website,

161 For example, Indictable 2 charges, which are the most serious, provides 22 hours for preparation for a contested trial, and 4 hours per diem preparation after the trial commences, and no maximum for in-court trial attendance. Additional hours may be billed in the event of "ancillary proceedings", for example, of a *Charter* application (8 hours), a bail review (10 hours) or the use of a Gladue or IRCA Report on sentencing (5 hour each).

162 See Legal Aid Services Rules.

163 Legal Aid Ontario, "Tariff reform 2024: Summary of changes, Phase 2 (No. 1)" (February 28, 2024), online: https://www.legalaid.on.ca/wp-content/uploads/Tariff-reform-2024_Summary-of-changes_Phase2A-EN.pdf.

164 Legal Aid Ontario, "2022-2023 Annual Report", online: https://www.legalaid.on.ca/wp-content/uploads/LAO-annual-report-2022-23-EN.pdf.

165 Legal Aid Ontario, "2022-2023 Annual Report", online: https://www.legalaid.on.ca/wp-content/uploads/LAO-annual-report-2022-23-EN.pdf.

166 See Legal Aid Services Rules.

167 These factors are listed and discussed in Legal Aid Ontario, "Tariff and billing handbook" (updated July 29, 2024), online: https://www.legalaid.on.ca/wp-content/uploads/LAO-tariff-and-billing-handbook-EN.pdf.

168 See Leal Aid Ontario, Complex Case Rate, online: https://www.legalaid.on.ca/lawyers-legal-professionals/case-management/big-case-management/complex-case-rate/.

169 See Province of Ontario, The Inquiry into Pediatric Forensic Pathology in Ontario (2008), online: https://www.archives.gov.on.ca/en/e_records/goudge/, Final Report, Volume 3, Recommendation 120.

170 See Legal Aid Ontario, Second Chair Program, online: https://www.legalaid.on.ca/lawyers-legal-professionals/mentoring-opportunities-at-legal-aid-ontario/second-chair-progra.

171 "Tactical and Practical Considerations in Litigating AI," chapter 6 in Jesse Beatson, Gerald Chan, Jill R. Presser (eds.), Litigating Artificial Intelligence (Toronto: Emond, May 2020).

172 See Legal Aid Ontario, Test Case Funding, online: https://www.legalaid.on.ca/lawyers-legal-professionals/test-cases/.

173 Legal Aid Ontario, "2022-2023 Annual Report", online: https://www.legalaid.on.ca/wp-content/uploads/LAO-annual-report-2022-23-EN.pdf.

174 See Government of Canada, Court Challenges Program, online: https://www.canada.ca/en/canadian-heritage/services/funding/court-challenges-program.html.

175 United Nations Human Rights Council, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (September 13, 2021), online: https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session48/Documents/A_HRC_48_31_AdvanceEditedVersion.docx; United Nations, Office of the High Commissioner for Human Rights, "Artificial intelligence risks to privacy demand urgent action – Bachelet" (September 13, 2021), online: https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet#:~:text=GENEVA%20(15%20September%202021)%20%E2%80%93,safeguards%20are%20put%20in%20place.

176 Office of the Privacy Commissioner of Canada, "Principles for responsible, trustworthy and privacy-protective generative AI technologies" (December 7, 2023), online: https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/.

177 Ontario Human Rights Commission, "Submission on Ontario's Trustworthy Artificial Intelligence (AI) Framework" (June 14, 2021), online: https://www.ohrc.on.ca/en/news-center/submission-ontarios-trustworthy-artificial-intelligence-ai-framework; Canadian Human Rights Commission, "Facial recognition technology use in Policing(April 15, 2022), online: https://www.chrc-ccdp.gc.ca/en/about-human-rights/publications/facial-recognition-technology-use-policing.

178 Law Commission of Ontario, "Accountable AI" (June 2022), online: https://www.lco-cdo.org/wp-content/uploads/2022/06/Accountable-AI-reduced-size.pdf.

179 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/.

180 Canadian Civil Liberties Association, "Submission to the Standing Committee on Industry and Technology regarding Bill C-27" (September 12, 2023), online: https://ccla.org/wp-content/uploads/2023/09/Bill-C-27-Submission-to-INDU-CCLA.pdf.

181 For an excellent index of various AI provisions introduced around the world, see OECD, "Emerging AI-related regulation", online: https://oecd.ai/en/dashboards/policy-instruments/Emerging_technology_regulation.

182 Information and Privacy Commissioner of Ontario, "Joint statement by the Information and Privacy Commissioner of Ontario and the Ontario Human Rights Commission on the use of AI technologies" (May 25, 2023), online: https://www.ipc.on.ca/en/media-centre/news-releases/joint-statement-information-and-privacy-commissioner-ontario-and-ontario-human-rights-commission-use.

183 Information and Privacy Commissioner of Ontario, "Joint statement by the Information and Privacy Commissioner of Ontario and the Ontario Human Rights Commission on the use of AI technologies" (May 25, 2023), online: https://www.ipc.on.ca/en/media-centre/news-releases/joint-statement-information-and-privacy-commissioner-ontario-and-ontario-human-rights-commission-use.

184 These principles have since been superseded by Ontario's "Responsible Use of Artificial Intelligence Directive" (published January 07, 2022, updated March 12, 2025), online: https://www.ontario.ca/page/responsible-use-artificial-intelligence-directive.

185 Law Commission of Ontario, "Submission on *Bill 194: Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*" (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.

186 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), online: https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194.

187 Law Commission of Ontario, "Submission on *Bill 194: Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*" (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.

188 Law Commission of Ontario, "Submission on *Bill 194: Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*" (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.

189 Law Commission of Ontario, "Submission on *Bill 194: Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*" (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.

190 Law Commission of Ontario, "Submission on *Bill 194: Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*" (June 2024), at p. 11, online: https://www.lco-cdo.org/wp-content/uploads/2024/06/LCO-Submission-to-Government-of-Ontario-Bill-194-Consultations-June-2024.pdf.

191 EU Artificial Intelligence Act, "The AI Office: What is it, and how does it work?", online: https://artificialintelligenceact.eu/the-ai-office-summary/.

192 This could function similar to the manner in which the Human Rights Tribunal of Ontario (HRTO) treats policies published by the OHRC, in that the HRTO looks to OHRC policies for guidance on interpreting the *Human Rights Code*.

193 See MIT Technology Review, "Congress used to evaluate emerging technologies. Let's do it again" (February 19, 2025), online: https://www.technologyreview.com/2025/02/19/1111573/congress-office-technology-assessment-emerging-innovation/. See also: Brookings.edu, "It is time to restore the US Office of Technology Assessment" (February 10, 2021), online: https://www.brookings.edu/articles/it-is-time-to-restore-the-us-office-of-technology-assessment/; and Princeton University, "The Office of Technology Assessment Legacy", online: https://www.princeton.edu/~ota/.

194 For a quick overview of these institutions and their intersecting roles, see IAPP.org, "EU AI Act Stakeholder Map" (May 2024), online: https://iapp.org/media/pdf/resource_center/eu_ai_act_stakeholder_map.pdf.

195 For a quick overview of these institutions and their intersecting roles, see IAPP.org, "EU AI Act Stakeholder Map" (May 2024), online: https://iapp.org/media/pdf/resource_center/eu_ai_act_stakeholder_map.pdf.

196 See Gillian K. Hadfield & Jack Clark, "Regulatory Markets: The Future of AI Governance" (April 2023), online: https://arxiv.org/pdf/2304.04914.

197 See Sandra Mayson, "Bias In Bias Out" (128 Yale Law Journal 2218 (2019)), online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3257004.

198 See for example, Simone Fabbrizzi et al. "A survey on bias in visual data sets," (Computer Vision and Image Understanding 223 (Oct 2022)), online: https://www.sciencedirect.com/science/article/abs/pii/S1077314222001308.

199 See, Law Commission of Ontario (Paula Thompson and Eric Neubauer), *AI at Trial and On Appeal: Paper 4 in the LCO AI in Criminal Justice Project* (Toronto: April 2025), at s. 2.1.8, online: https://www.lco-cdo.org/CrimAI.

200 Though some may be looking into the use of synthetic data soon (see for example IBM, "What Is Synthetic Data?" (online: https://research.ibm.com/blog/what-is-synthetic-data), synthetic data carries its own privacy risks and is not a panacea (see Khalid El Emam, Anita Fineberg, Elizabeth Jonker & Luch Mosquera, "Pan-Canadian Descriptive Study of Privacy Risks from Synthetic Data Generation Practices within the Evolving Canadian Legislative Landscape" (March 2022), online: https://5571861900.saas.quicksilk.com/web/default/files/users/1/opc_synthetic_consolidated-v12.pdf.

201 See Law Commission of Ontario, "Accountable AI" (June 2022), online: https://www.lco-cdo.org/wp-content/uploads/2022/06/Accountable-AI-reduced-size.pdf; and Office of the Privacy Commissioner of Canada, "Principles for responsible, trustworthy and privacy-protective generative AI technologies" (December 7, 2023), online: https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/.

202 Jane Bailey, Jacquelyn Burkell, and Brenda McPhail, "Submissions on Bill C-27 *The Digital Charter Implementation Act*", online: https://www.ourcommons.ca/Content/Committee/441/INDU/Brief/BR12605252/br-external/Jointly3-e.pdf.

203 See: EU Law Enforcement, "The Dutch benefits scandal: a cautionary tale for algorithmic enforcement" (April 30, 2021), online: https://eulawenforcement.com/?p=7941; Politico.com, "Dutch scandal serves as a warning for Europe over risks of using algorithms" (March 29, 2022), online: https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/.

204 Ontario Ministry of Education, "Review of the Peel District School Board" (February 28, 2020), online: https://files.ontario.ca/edu-review-peel-dsb-school-board-report-en-2023-01-12.pdf. See also Forbes.com, "The Dark Side Of AI Recruiting: Depersonalization And Its Consequences On The Modern Job Market" (July 7, 2023), online: https://www.forbes.com/sites/benjaminlaker/2023/07/07/the-dark-side-of-ai-recruiting-depersonalization-and-its-consequences-on-the-modern-job-market/?sh=65b6b0c068c8.

205 See The Citizen Lab, To Surveil and Predict A Human Rights Analysis of Algorithmic Policing in Canada (September 1, 2020), at p. 145, online: https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/. See also MIT Technology Review, "Predictive policing algorithms are racist. They need to be dismantled" (July 17, 2020), online: https://www.technologyreview.com/2020/07/17/1005396/predictive-policing-algorithms-racist-dismantled-machine-learning-bias-criminal-justice/.

206 See for example CBC News, "RCMP reveals use of secretive cellphone surveillance technology for the first time," (April 5 2017), online: https://www.cbc.ca/news/science/rcmp-surveillance-imsi-catcher-mdi-stingray-cellphone-1.4056750.

207 Global News, "RCMP has used spyware to access targets' communications as far back as 2002: Senior Mountie," (August 8, 2022), online: https://globalnews.ca/news/9044296/rcmp-cellphone-hacking-privacy/.

208 CBC News, "Toronto Police used Clearview AI facial recognition software in 84 investigations," (December 23, 2021), online: https://www.cbc.ca/news/canada/toronto/toronto-police-report-clearview-ai-1.6295295.

209 Washington Post, "Police seldom disclose use of facial recognition despite false arrests" (October 6, 2024), online: https://www.washingtonpost.com/business/2024/10/06/police-facial-recognition-secret-false-arrest/.

210 United Nations Human Rights Council, "The right to privacy in the digital age: Report of the United Nations High Commissioner for Human Rights" (September 13, 2021), online: https://www.ohchr.org/sites/default/files/HRBodies/HRC/RegularSessions/Session48/Documents/A_HRC_48_31_AdvanceEditedVersion.docx; United Nations, Office of the High Commissioner for Human Rights, "Artificial intelligence risks to privacy demand urgent action – Bachelet" (September 13, 2021), online: https://www.ohchr.org/en/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet#:~:text=GENEVA%20(15%20September%202021)%20%E2%80%93,safeguards%20are%20put%20in%20place.

211 See Law Commission of Ontario, "Submission on *Bill 194: Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*" (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. See also EU AI Act, Chapter II: Prohibited Artificial Intelligence Practices, Article 5, online: https://artificialintelligenceact.eu/article/5/#:~:text=The%20EU%20AI%20Act%20prohibits,risk%20of%20committing%20a%20crime.

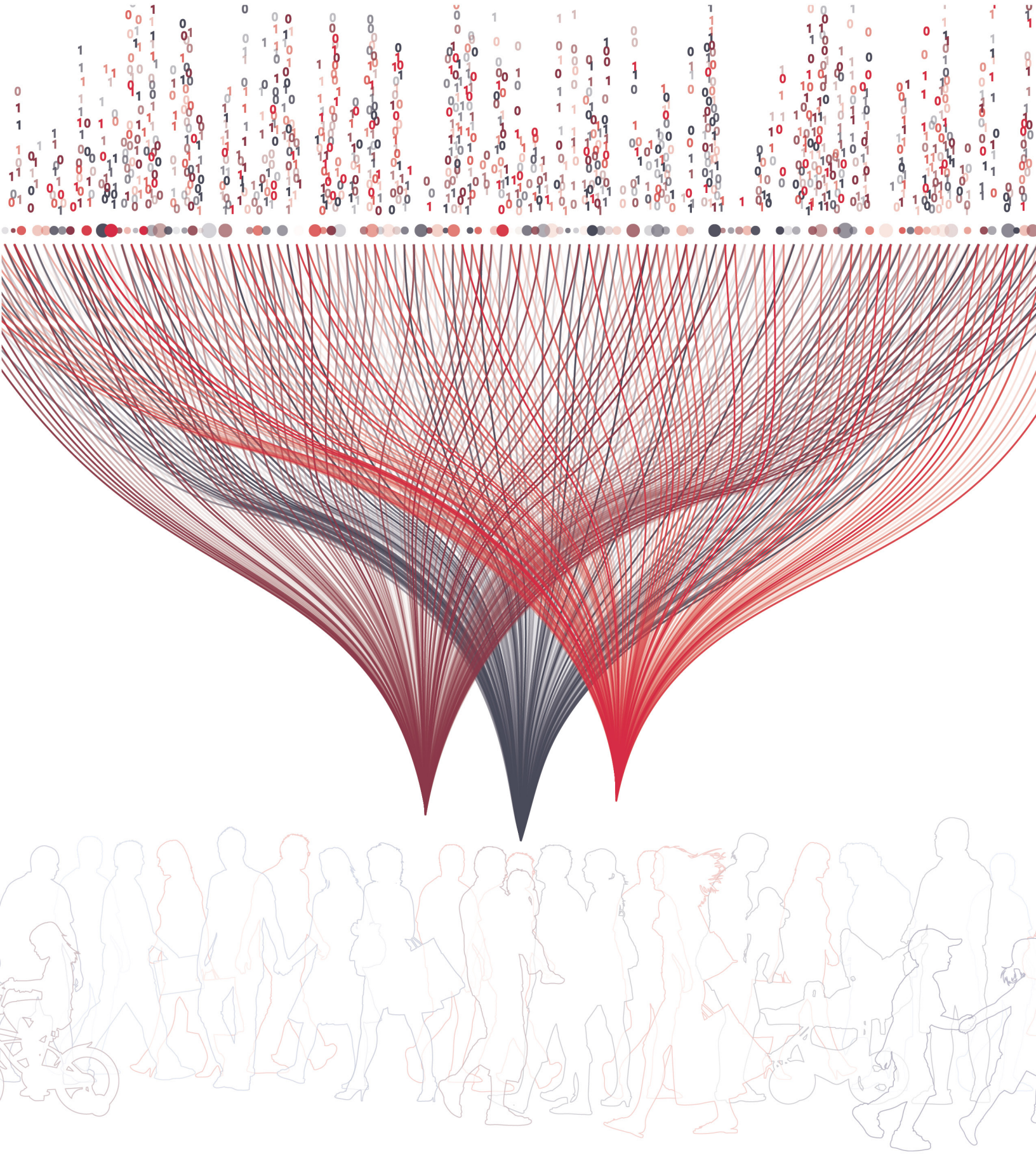
212 See Law Commission of Ontario, "Submission on *Bill 194: Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*" (June 2024), online: https://www.lco-cdo.org/wp-content/uploads/2024/06/LCO-Submission-to-Government-of-Ontario-Bill-194-Consultations-June-2024.pdf. See also EU AI Act, Chapter III: High-Risk System, online: https://artificialintelligenceact.eu/chapter/3/.

213 See Law Commission of Ontario, "Submission on *Bill 194: Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*" (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. The LCO can provide a compendium of such legislation upon request.

214 See Law Commission of Ontario, "Accountable AI" (June 2022), online: https://www.lco-cdo.org/wp-content/uploads/2022/06/Accountable-AI-reduced-size.pdf. See also Ontario Human Rights Commission, "Submission on Ontario's Trustworthy Artificial Intelligence (AI) Framework" (June 14, 2021), online: https://www.ohrc.on.ca/en/news-center/submission-ontarios-trustworthy-artificial-intelligence-ai-framework

215 Law Commission of Ontario, "Accountable AI" (June 2022), online: https://www.lco-cdo.org/wp-content/uploads/2022/06/Accountable-AI-reduced-size.pdf. See also Ontario Human Rights Commission, "Submission on Ontario's Trustworthy Artificial Intelligence (AI) Framework" (June 14, 2021), online: https://www.ohrc.on.ca/en/news-center/submission-ontarios-trustworthy-artificial-intelligence-ai-framework

216 Ontario Human Rights Commission, "Letter to Ann Morgan, Chair Toronto Police Services Board re Approval of high-risk technologies under the Toronto Police Services Board's Policy on the use of artificial intelligence technology" (January 10 2024), online: https://www3.ohrc.on.ca/en/news_centre/approval-high-risk-technologies-under-toronto-police-services-boards-policy-use-artificial. See also Information and Privacy Commissioner of Ontario, "Letter from Commissioner Patricia Kosseim to Ann Morgan, Chair, Toronto Police Services Board re: Update on the Implementation of the Board's Policy on Use of Artificial Intelligence Technology" (January 10, 2024), online: https://www.ipc.on.ca/sites/default/files/legacy/2024/01/2024-01-10-submission-to-the-january-11-2024-toronto-police-services-board-public-meeting-ai-policy-and-the-toronto-fr-mugshot-database-program-e.pdf.



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