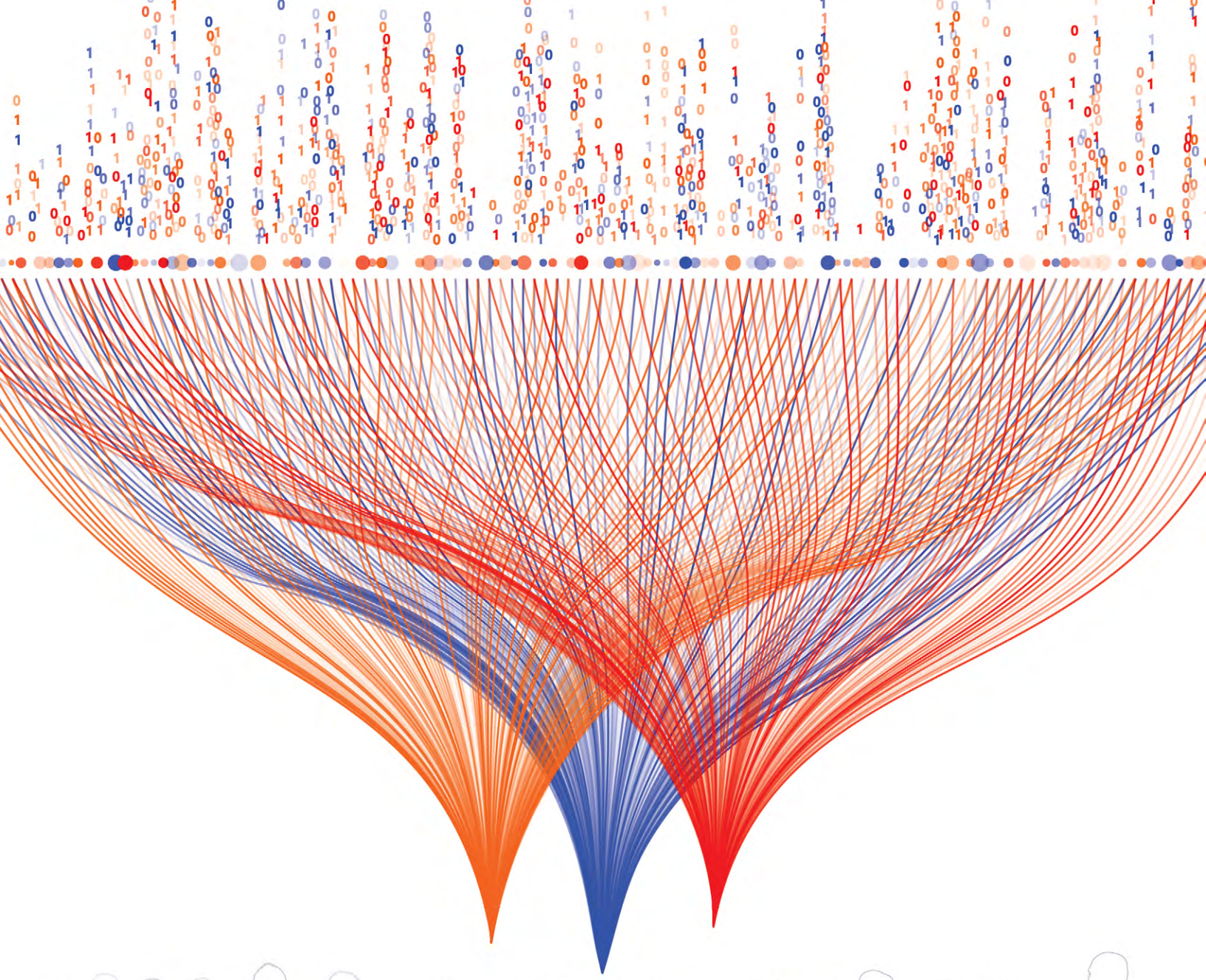


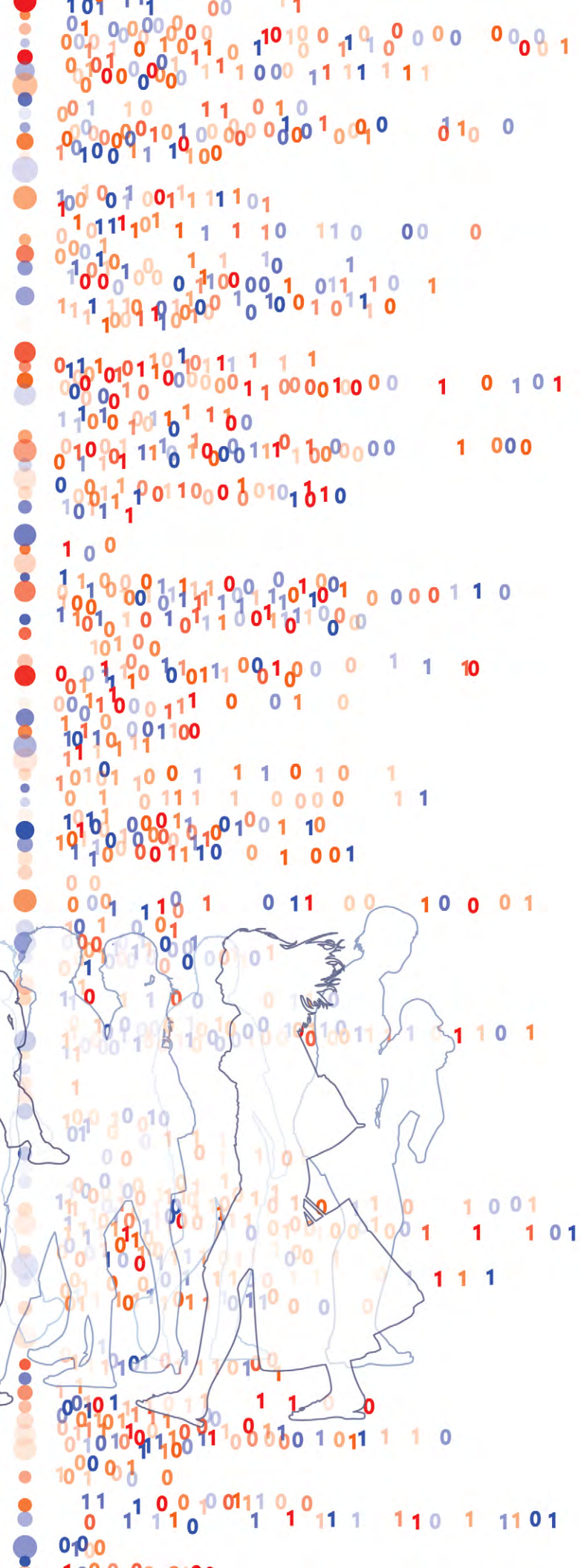
Law Commission of Ontario

AI IN CRIMINAL JUSTICE PROJECT | PAPER 1

Introduction and Summary

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.

Recent LCO reports and submissions addressing AI 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.

The LCO AI in Criminal Justice Project

Paper 1	Introduction and Summary: LCO AI in Criminal Justice Project Nye Thomas, Executive Director, LCO Ryan Fritsch, Counsel, LCO
Paper 2	Use of AI by Law Enforcement Ryan Fritsch, Counsel, LCO
Paper 3	AI and the Assessment of Risk in Bail, Sentencing, and Recidivism Armando D'Andrea, Staff Lawyer, Provincial Office, Legal Aid Ontario Gideon Christian, Professor of Law, Faculty of Law, University of Calgary
Paper 4	AI at Trial and on Appeal Paula Thompson, Strategic Initiatives, Ministry of the Attorney General Eric Neubauer, Defense Counsel, Neubauer Law, and Co-Chair, Criminal Lawyers Association Technology Committee
Paper 5	AI and Systemic Oversight Mechanisms in Criminal Justice. Brenda McPhail, Senior Technology & Policy Advisor, Information and Privacy Commissioner of Ontario Marcus Pratt, Senior Advisor, Policy Department, Legal Aid Ontario, and Chair of the LAO Test Case Committee Jagtaran Singh, Legal Counsel Ontario Human Rights Commission
Annex A	Executive Summary and Consultation Questions
Annex B	Project Case Studies

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

Series Editors

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

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, 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

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, ***Introduction and Summary: 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.

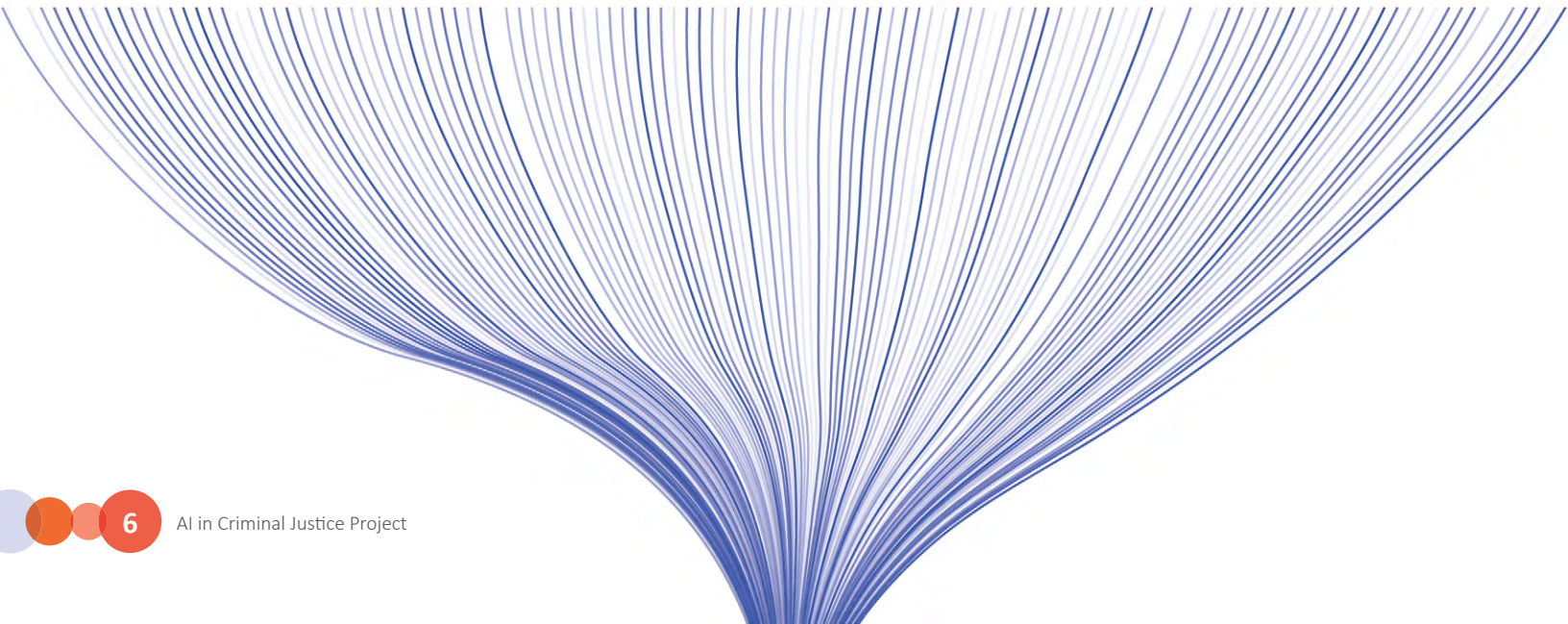
The Law Foundation of Ontario
Advancing access to justice

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's (LCO) AI in Criminal Justice Project is a groundbreaking 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 institutions, policymakers and stakeholders about the law reform issues, choices, opportunities, and challenges in this complex and fast-moving area.

This paper (Paper 1) is an introduction to the project and a summary of our four Issue Papers. Each Issue Paper considers AI in a distinct phase of the criminal justice process, including:

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.

This Introduction also provides an overview of "trustworthy criminal AI" issues and initiatives. It identifies AI systems currently used in criminal justice and summarizes their respective benefits and risks. The paper also summarizes criminal AI governance initiatives internationally and in Canada and concludes with an assessment of "trustworthy criminal AI" in Canada and Ontario.

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

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

To their credit, Canadian Privacy Commissioners, some 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 are or may 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*, the *Criminal Code of Canada*, procedural fairness, evidence law, 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:

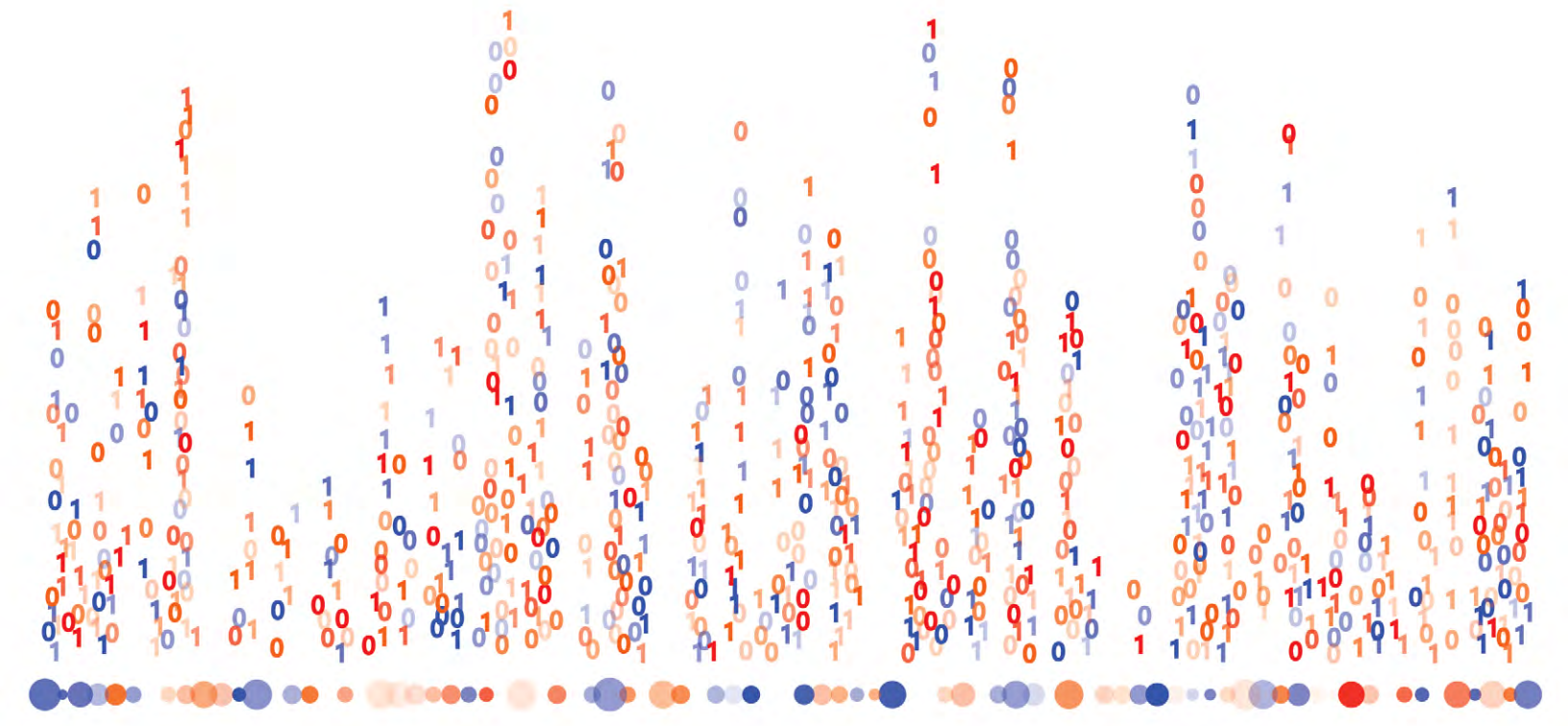
- What can we learn from the experience of other jurisdictions that have confronted these issues?
- How have Canadian policymakers, courts, and others responded to the emerging challenges?
- Are there gaps in Canada's current criminal AI regulatory landscape?

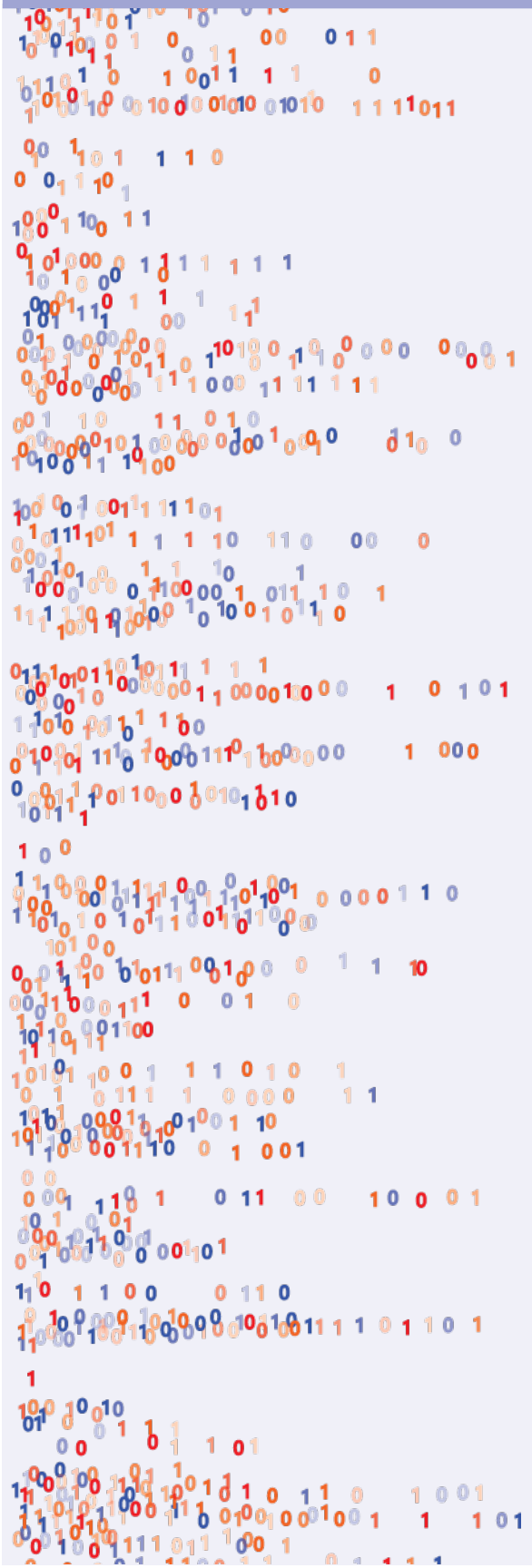
Finally, the project tries to foreshadow or predict what is likely to happen in Canadian criminal justice if action is not taken. In other words, what is likely to happen if we fail to address these issues? What can we learn from the experience in other jurisdictions?

Like other LCO projects, this series of Issue Papers are designed to facilitate discussion and consultation. These papers do not present final or specific law reform recommendations. Instead, each Issue Paper includes a series of questions for future consideration by Canadian criminal AI policymakers and stakeholders. In this manner, the LCO hopes these 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 invites justice sector institutions, academics, legal practitioners, law enforcement, civil society groups and individuals to contact us with feedback or to organize a consultation session. The LCO will analyze and summarize the feedback we receive in a Final Report that 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.





Defining Artificial Intelligence

A challenge in defining "artificial intelligence" is that AI is a technology of general application adaptable to a limitless array of purposes.

The Organisation for Economic Co-operation and Development (OECD) first proposed a regulatory definition of AI in 2019. This definition was subsequently adapted and debated in the European Union (EU) leading to its enactment in Chapter I, Article 3 of the EU *Artificial Intelligence Act* (EU *AI Act*) in May 2024, which states that an AI system is:

…a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions, that influence physical or virtual environments.[1]

To date, the EU *AI Act* is the most comprehensive national-level AI legislation in the world. The EU *AI Act* definition is widely recognized as a broadly inclusive, technology-neutral, uniform definition for AI that could be applied to future AI systems, including those in criminal justice. It also distinguishes AI from less sophisticated automated algorithms, which are generally heuristic or determinative.

A similar definition is recognized in proposed Canadian legislation, including section 2 of the federal government's proposed *Artificial Intelligence and Data Act* (AIDA):

artificial intelligence system *means a technological system that, autonomously or partly autonomously, processes data related to human activities through the use of a genetic algorithm, a neural network, machine learning or another technique in order to generate content or make decisions, recommendations or predictions.*[2]

Section 1(1) of Ontario's *Enhancing Digital Security and Trust Act, 2024* defines AI as:

(a) a machine-based system that, for explicit or implicit objectives, infers from the input it receives in order to generate outputs such as predictions, content, recommendations or decisions that can influence physical or virtual environments, and
(b) such other systems as may be prescribed; ("système d'intelligence artificielle").[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. 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 any of our reports.

Project Lead and Contact

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

The LCO can be contacted at:

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

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

Author and Project Editors

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

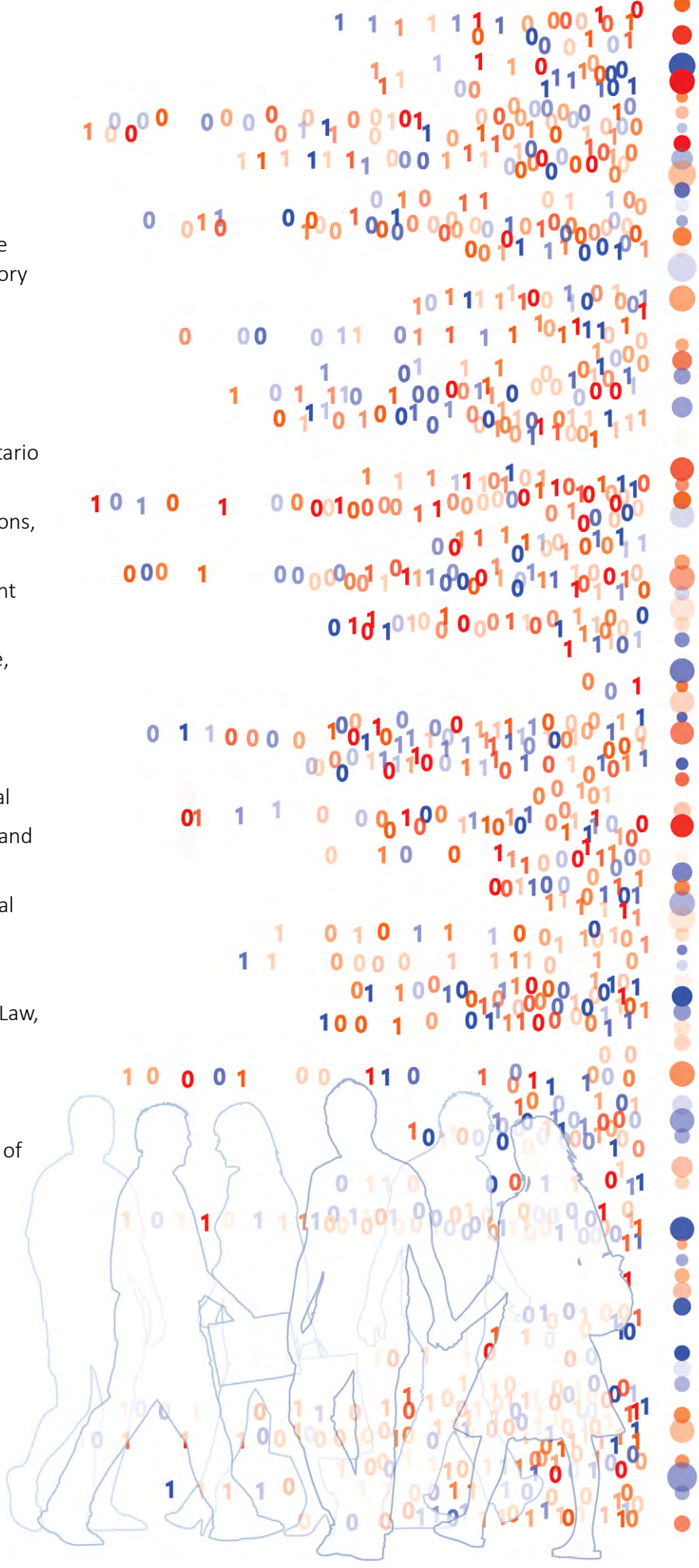
Project authors include:

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

Advisory Committee

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

- Alpha Chan, Chief Information Security Officer, 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
- Professor Ben Perrin, Peter A. Allard School 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 in Criminal Justice: Uses and Benefits

The criminal justice system has been at the forefront of the adoption of AI. Criminal jurisdictions outside of Canada employ AI to improve police investigations, analyze evidence, assist judicial decision-making, improve data analysis, and target limited resources. AI technologies used today include facial recognition and biometric surveillance, predictive policing, social media analysis, licence plate readers, AI-generated evidence, bail and sentencing algorithms and many other applications.

There have already been several examples of AI in Canadian criminal justice, including facial recognition systems, predictive policing, automated fingerprint identification, automatic licence plate readers, de-encryption of digital devices, object recognition of images and video, and classification of purportedly high-risk inmates.[4]

AI technology is seen as particularly beneficial in policing, where many commentators see AI as transformative. For example, facial recognition technology has been described as a "game-changer" in criminal investigations that allows police services "to respond swiftly to emerging threats and prevent crimes before they occur."[5]

The potential benefits of AI in policing are summarized in a recent EUROPOL report, *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement*, which stated that:[6]

> *Artificial Intelligence (AI) will profoundly alter the landscape of law enforcement, offering innovative tools and opportunities to enhance our capabilities in safeguarding public safety. This flourishing technological field* ***promises to revolutionize*** *how we analyze complex data sets, improve forensic methodologies, and develop secure communication channels. [Emphasis added.]*
>
> ***[AI] has emerged as a transformative tool, bringing capabilities that could completely reshape policing****...*[7] *[Emphasis added.]*

This report further states that:

> *The power of AI in processing vast amounts of data, and filtering for relevant content, its data modelling capabilities, and its ability to identify patterns and trends previously undetectable by human investigators* ***highlight its transformative potential****. Beyond that, the use of AI for repetitive and resource-intensive tasks, allows [law enforcement agencies] to work more efficiently with their limited resources and lets police officers focus on and prioritise their most important tasks.*[8] *[Emphasis added.]*

This section of the Introduction highlights several of the most significant criminal justice AI technologies. The LCO's goal in this section is to both introduce the technology and identify variations or choices within that technology that readers may not be aware of. Each project Issue Paper discusses these technologies, and others, in more detail.

2.1 Predictive Analytics/Predictive Policing

Statistical analysis has been used to prioritize police interventions and police resources for some time. The best known, and most controversial, predictive analytic tool is predictive policing.

The use of predictive policing technology is often characterized as a "technological promise" aimed at "revolutionizing law enforcement."[9] Professor Andrew Ferguson, a leading US scholar on predictive policing, writes of the promise where

> *…data-driven insights [are] operationalized into concrete decisions about police priorities and resource allocation…offering police administrators the ability to identify higher crime locations, to restructure patrol routes, and to develop crime suppression strategies based on the new data.*[10]

Predictive policing is discussed in the LCO's second project Issue Paper, *Law Enforcement Use of AI,* written by LCO Counsel Ryan Fritsch.[11]

What Would Happen if We Failed To Establish "Trustworthy Criminal AI" in Canada?

Governments, police services, courts, legal organizations, and NGOs around the world have concluded that the benefits of AI in criminal justice will only be achieved if AI risks and harms are addressed proactively. Collectively, these jurisdictions and organizations have recognized the importance of adopting "trustworthy AI" principles to govern AI systems in the criminal justice systems.

It is fair to ask what is likely to happen if Canadian governments do not establish trustworthy criminal AI. This is not a hypothetical question. Criminal AI systems have been in use in other jurisdictions for several years. Provincial policymakers thus have a detailed record of well-documented and widely publicized risks and harms, including:

- Risk of false arrest or imprisonment.
- Data bias and discrimination.
- Inconsistent judicial decisions.
- Compounding existing overrepresentation of low-income, racialized, and Indigenous communities in criminal justice.
- Inconsistent and inefficient operations.
- Lack of legal accountability.
- Risks to privacy, human rights, and procedural fairness.
- Loss of public trust in the criminal justice system.

Failure to establish trustworthy criminal AI in Ontario could mean that predictive policing, facial recognition surveillance, automated bail and sentencing risk assessments, and a myriad of other AI technologies could be introduced in this province without appropriate "guardrails" or accountability requirements. Absent effective regulation, the harm to criminal defendants, criminal courts, and public trust in the criminal justice system is foreseeable and significant.

Predictive policing is a generic name for AI technology that processes and analyses large and complex datasets much more quickly than humans. The EUROPOL report cited above defines predictive policing as

> *…a sophisticated statistical method [that] extract valuable new insights from vast datasets, for instance on crime records, events and environmental factors identified in criminological insights. This approach empowers police agencies to identify patterns related to the occurrence of crime and unsafe situations, and to deploy forces according to these insights to minimize risks.*
>
> *The AI model identifies patterns within historical data, associating indicators with the likelihood of a crime occurring, and then generates risk scores as predictive outputs.*[12]

Predictive policing has many applications but is commonly understood as AI systems that to try to predict or 'forecast' future crime. In its 2020 report, *To Surveil and Protect*, The Citizen Lab at the University of Toronto states that there are two main categories of predictive policing:

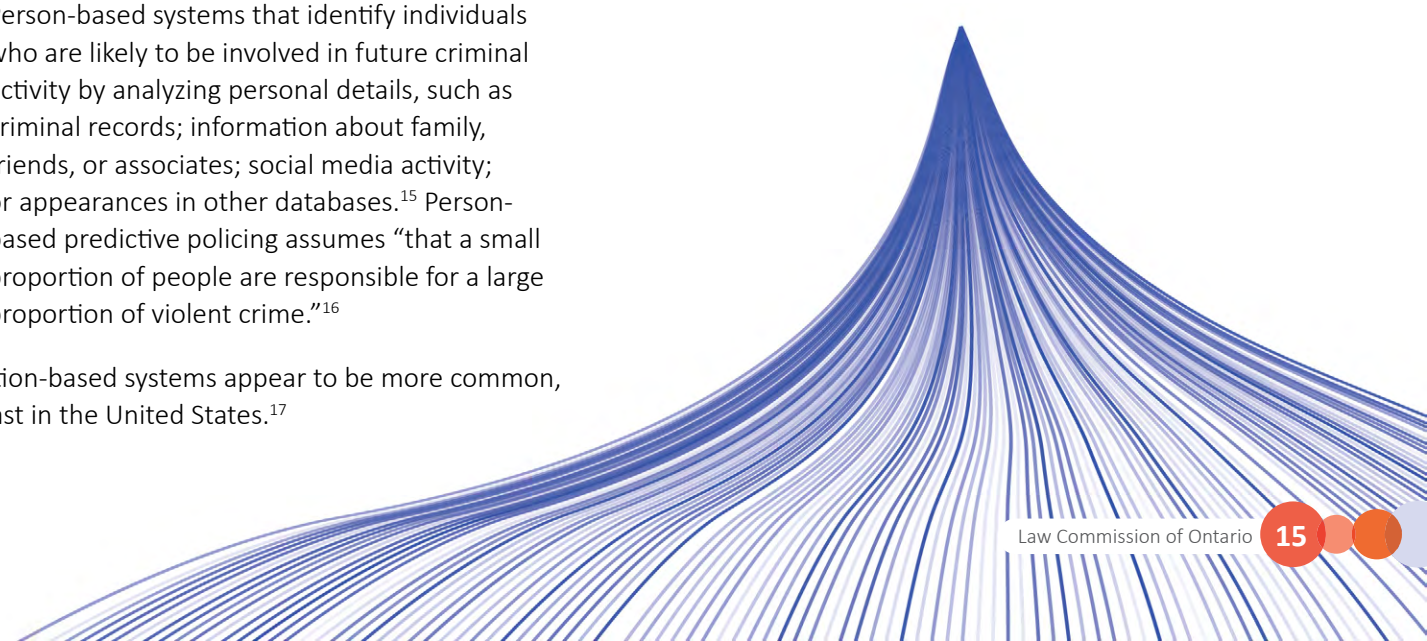
- Location-based systems that identify where and when potential criminal activity might occur by analyzing patterns and correlations in police and other data.[13] Location-based predictive policing is based an assumption that "crime is not distributed evenly across society but instead follows identifiable patterns…leading to crime "hot spots."[14]
- Person-based systems that identify individuals who are likely to be involved in future criminal activity by analyzing personal details, such as criminal records; information about family, friends, or associates; social media activity; or appearances in other databases.[15] Person-based predictive policing assumes "that a small proportion of people are responsible for a large proportion of violent crime."[16]

Location-based systems appear to be more common, at least in the United States.[17]

The variations within and between predictive policing systems can have wide ranging implications for public safety, police investigations, and individual rights. For example, location-based systems have been variously used to manage police patrols, identify times and locations where specific crimes are likely to occur, and identify areas where community interventions could be helpful to reduce crime.[18] Person-based predictive policing, on the other hand, has been used predict which individuals are more likely to be involved with crime ("targeted offender lists"), to promote officer safety when responding to 911 calls, and/or to promote "focussed deterrence."[19]

The use of predictive policing is gradually spreading across the US.[20] Well-known examples of predictive policing include LASER, a system that was used by the Los Angeles Police Department to identify areas where gun violence was likely to occur; PredPol and Palantir, the most commonly used predictive policing systems in the U.S; and the Chicago Police Department's "strategic subject list" system.[21] Canadian police services are also reported to have used or tested predictive policing, including the Vancouver Police Department (GeoDASH) and Calgary Police Department (Palantir Gotham).[22]

It is important to note that predictive policing is evolving, and that many of the early predictive policing systems "have come and gone."[23] Indeed, many predictive policing systems have been discontinued or altered in the face of significant criticisms, discussed below.



2.2 Facial Recognition and Biometric Technology

Facial recognition technology (FRT) is defined by the Information and Privacy Commissioner of Ontario as:

> *…an artificial intelligence (AI) technology that collects and processes sensitive personal information to identify or verify an individual's identity. FRT uses image processing software to analyze an individual's facial features, such as the width of the nose, the length of the jawline, and the distance between the eyes (e.g., as they appear in a photograph). FRT algorithms turn facial features into a faceprint of an individual. A facial recognition system can then compare two faceprints and return a similarity score or match faceprints by searching a reference database of a large number of images for a list of potential candidates whose similarity score is at, or above, a given threshold.*[24]

In addition to FRT, other forms of AI-enhanced biometric identification include fingerprints, voice recognition, iris scans, and gait analysis.

According to INTERPOL, "law enforcement agencies around the world use facial recognition technology to support the investigation of suspects, victims, missing persons, unknown dead bodies and even witnesses."[25] Police services often believe FRT and biometrics have significant potential to improve public safety, police investigations, and efficiency:

> ***In this rapidly evolving landscape, computer vision and biometrics have emerged as game-changers for law enforcement, both from prevention and investigation standpoints****. As cities and communities are facing a surge of digital imagery from sources like CCTV cameras to personal devices, it is essential to use this vast visual data effectively. Coupled with biometric techniques that utilize the unique physiological traits of individuals,* ***these technologies promise a new frontier in policing****. The fusion of biometrics and AI can deliver a blend of efficiency and accuracy, offering in-depth insights to swiftly and effectively identify criminals while at the same time protecting the privacy of non-relevant individuals.*[26]
>
> ***[FRT]…has become an invaluable tool for law enforcement agencies.*** *For instance, the technology helps swiftly identify suspects by comparing facial data collected within the course of a criminal investigation against historical data or databases of criminals available to the police. Additionally, it plays a crucial role in locating missing persons and children by matching unidentified individuals 'images against databases of those reported missing.*[27] *[Emphasis added.]*

FRT and biometric systems can be used for a wide range of purposes and in many different contexts, including:

- To support a range of criminal investigations, including terrorist threats, missing person or children's investigations, human trafficking and other types of sexual exploitation, serious crime investigations, public order events, or traffic stops.
- To scan mugshot databases.
- To support investigations or general surveillance in public, private, or secure spaces.
- For real-time personal identification through police body cams or drone videos.
- To analyze images or video collected by third parties.[28]

These are not the only potential uses of FRT. For this reason, the Ontario Human Rights Commission has noted the possibility of facial recognition "function creep."[29]

The challenge of balancing public safety and rights in police FRT systems was clearly stated in a May 2022 joint statement by federal, provincial and territorial Privacy Commissioners:

> *FR technology has emerged as a tool of significant interest to police agencies. Used responsibly and in the right circumstances, FR may assist police agencies in carrying out a variety of public safety initiatives, including investigations into criminal wrongdoing and the search for missing persons.*
>
> *At the same time, FR has the potential to be a highly invasive surveillance technology.*
>
> *The use of FR involves the collection and processing of sensitive personal information. This information speaks to the very core of individual identity, and its collection and use by police supports the ability to identify and potentially surveil individuals.*[30]
>
> *The prospect of police agencies integrating FR technology into law enforcement initiatives thus raises the possibility of serious privacy harms unless appropriate privacy protections are put in place…The nature of these risks calls for collective reflection on the limits of acceptable FR use.*[31]

Like predictive policing, it is important to note important variations and distinctions between and within policing FRT systems. These distinctions can have wide ranging implications for public safety, police investigations, and individual rights. For example, one of the major concerns about FRT systems is the risk of mass, untargeted, or unjustified surveillance. Surveillance risks are present in all FRT systems, but the scope of that risk depends in part on the potential source of FRT probe and reference images. Sources of FRT probe images could include public or private security cameras, police body cameras, drones, or home security cameras. Potential sources of FRT reference images could include mugshot databases, specialized police databases, internet scraping, or even driver's license pictures. There is also an important distinction between real-time FRT (live face recognition or LFR) and FRT systems used retrospectively (post-event facial recognition).[32]

FRT is widely deployed in the United States and internationally. For example, in 2021, the United States Government Accountability Office found that nearly half of 42 federal agencies employing law enforcement officers used FRT.[33] FRT systems are reported to be used in some form by hundreds of law enforcement agencies in the United States.[34]

The best-known example of FRT in Canada is the use of Clearview AI by the RCMP. Clearview AI's software scrapes images from the Internet, creating a massive database to identify individuals through FRT. A 2021 investigation by the Office of the Privacy Commissioner of Canada and the Privacy Commissioners of Alberta, British Columbia and Quebec concluded that Clearview AI and the RCMP violated federal and provincial privacy statutes. The investigation also raised concerns about the accuracy and potential biases in FRT.[35] The RCMP has confirmed that it has stopped using Clearview AI.[36]

Beyond the Clearview AI example, it is difficult to know if or how police are using FRT in Canada due to the lack of mandatory disclosure of policing AI systems across Canada. Notably, the Toronto Police Service has disclosed that it uses a FRT technology called NeoFace Reveal to compare a "criminal suspect image captured in relation to a criminal occurrence to a database of lawfully obtained criminal record images (booking photographs)."[37]

2.3 Object Recognition

FRT is a form of AI object recognition.[38] AI object recognition systems automatically recognize and report certain features in video or audio data. In addition to FRT, law enforcement agencies use other forms of AI object recognition, including:

- Licence plate readers.
- Enhanced video analysis.
- Gunshot detectors.
- Pattern analytics and crime scene evidence detection.

Automatic Licence Plate Readers/Vehicle Surveillance

Automated license plate readers (ALPRs) read and record the license plates of vehicles scanned by infrared cameras on roads and highways and check them against a database using pattern recognition software. ALPRs are widely used by police services across North America.[39] ALPRs can be used to support police investigations, to increase security at events or facilities, and to improve traffic management.[40]

It is not clear how widely ALPRs are deployed in Ontario. The Toronto Police Service has reported that it uses licence plate readers to "receive real-time alerting in patrol vehicles to arrest wanted criminals, recover stolen vehicles and locate missing persons that are on various hotlists."[41]

Enhanced Video Analysis

AI-enhanced video analysis can "uncover crucial details that may go unnoticed by human investigators [from] identifying objects [such as guns] and individuals to detecting anomalies in behaviour, these tools [can] contribute significantly to the depth and accuracy of investigations.[42]

Gunshot Detection

The U.S. National Institute of Justice states that AI gunshot detection technology has the potential to

> *…develop algorithms to detect gunshots, differentiate muzzle blasts from shock waves, determine shot-to-shot timings, determine the number of firearms present, assign specific shots to firearms, and estimate probabilities of class and caliber, all of which could help law enforcement in investigations.*[43]

ShotSpotter is the best-known gunshot detection technology. According to the company's website, more than 170 American cities use the technology as of December 2024.[44] The technology relies on thousands of microphones installed across cities to automatically detect gunshot sounds and to dispatch police.[45]

ShotSpotter and related technologies have been criticized due to concerns about accuracy, effectiveness, cost, and potential impact on privacy, mass surveillance, and racialized communities. In the last few years, several American cities, including Atlanta, Chicago, and San Diego have declined to renew their ShotSpotter contracts due to these concerns.[46]

Not much is known about the use of gunshot detection technology in Canada. The City of Toronto and the Toronto Police Service were considering acquiring Shotspotter in 2018 and 2019. The plan was subsequently dropped due to some of the concerns discussed above.[47]

2.4 Drones

According to an industry website, "AI-powered drones, equipped with sophisticated cameras, sensors, and real-time data processing capabilities, have redefined video surveillance and security measures." [48]

The RCMP states that remotely piloted aircraft systems (i.e. drones),

> *…are used for aerial surveillance activities. These aircraft systems are equipped with electro-optical and/or infrared cameras.* ***These are used to support a multitude of critical RCMP operations, such as major crime scenes, search and rescue missions, traffic collision scenes and high-risk situations involving the RCMP Emergency Response Team****.*[49] *[Emphasis added]*

The RCMP also states that drones reduce the risk to police officers in certain situations by sending the technology into high-risk environments.[50]

Drones are already used by over 1,400 US police departments.[51]

2.5 Bail and Sentencing Algorithms

Bail, sentencing, and post-sentencing decisions have long relied on professional risk assessments to predict an accused or offender's potential danger to the public. Bail and sentencing algorithms are AI or algorithmic tools that aid criminal courts in bail or sentence decision-making.

These systems are considered in the second LCO Issue Paper, *AI and the Assessment of Risk in Bail, Sentencing, and* Recidivism, written by Armando D'Andrea, Criminal Panel Manager and former Criminal Duty Counsel, Legal Aid Ontario and Gideon Christian, Professor of Law, University of Calgary Faculty of Law, and an early LCO AI paper, *The Rise and Fall of Algorithms in the American Justice System: Lessons for Canada.*[52]

The use of bail and sentencing algorithms expanded rapidly across the United States in the 2010s.[53] The growth was driven largely by the American bail reform movement, the purpose of which is "end wealth-based [bail] system and move pretrial justice systems to a risk-based model."[54] Algorithmic pretrial risk assessments quickly emerged as the "favored reform" to advance these initiatives.[55] According to the Center on Court Innovation, a New York-based non-profit research organization, "[the] appeal of pretrial risk assessment—especially in large, overburdened court systems—is of a fast and objective evaluation, harnessing the power of data to aid decision-making."[56]

The expansion of bail and sentencing algorithms was the catalyst for an unprecedented and rapid evaluation of how AI and algorithmic tools in criminal justice are designed, developed, and deployed. Many of the early deployments of these systems were criticized for being systemically biased, opaque, and difficult to litigate.

2.6 Other AI Systems Used in Criminal Justice

The technologies discussed in this section are not the only AI systems that have been used in criminal justice systems around the world. The Issue Papers discuss how AI has also been used or considered to support open-source intelligence (OSINT) and social media intelligence (SOCINT)[57]; AI-generated evidence[58]; emergency responses[59], and for real time crime analysis.[60]

AI systems have also been considered to support police report writing[61], post-conviction analysis[62], digital forensics[63], police services strategic planning[64], criminal record expungement[65], victim support[66] and to monitor police conduct.[67]

Finally, many general AI technologies could be adapted to criminal justice, including systems that prepare legal research, summaries, and public legal information[68]; draft pleadings and legal submissions[69]; evaluate evidence[70]; test testimony[71]; improve the efficiency and affordability of legal services[72]; improve services for self-represented litigants[73]; and improve research and data analysis.[74]

3. AI in Criminal Justice: Risks and Issues

The previous section discussed the potential uses and benefits of AI technology in the criminal justice system. This section discusses criminal AI's risks and potential harms.

The risks of AI in government decision-making (including the criminal justice system) were discussed at length in the LCO's *Accountable AI*, *Regulating AI*, and *The Rise and Fall of Algorithms in the American Justice System: Lessons for Canada* reports.[75] The LCO reports and others document how AI systems such as biometric surveillance, predictive policing, and bail and sentencing algorithms have high risks to *Charter* rights, human rights, civil liberties, privacy protections, and procedural fairness.

LCO reports also discuss how the risks of these systems fall disproportionately on low-income, Indigenous, racialized, or otherwise vulnerable communities and individuals, potentially worsening the overrepresentation of these communities in Canada's criminal justice system.[76]

A major focus of the LCO's Criminal AI project is whether, or how, criminal AI systems conform to Canadian criminal law and institutions. Criminal justice relies on a sophisticated body of law and procedure specific to Canada. The *Charter*, *Criminal Code*, criminal common law, evidentiary law, and principles of procedural fairness work together to check state power, protect individual rights, and promote public safety.

The project Issue Papers discuss the risks of specific technologies in detail. A summary of these risks is presented below.

1. Bias and Discrimination

AI systems can be biased or discriminatory against individuals on the grounds of race, age, disability, sex, family structure or other protected grounds.[77] Bias in an AI system can also intersect across multiple grounds.

Data bias and discrimination in criminal justice AI systems have been discussed extensively. For example, issues respecting the quality and potential bias of AI training sets ("bias in, bias out") are well-known.[78]

Many FRT systems have been shown to be biased and discriminatory. The International Network of Civil Liberties Organizations (INCLO) has noted that

> *Studies on FRTs have clearly demonstrated that racial and gender biases, meaning women and people of colour, are more likely to be misidentified by FRT and, therefore, potentially more likely to be wrongfully accused by police who use FRT than light-skinned men.*[79]

INCLO also states that "some authorities are more likely to apply FRT to marginalized communities a which are already over-surveilled, over-policed, and over-incarcerated."[80]

Concerns about FRT bias are the foundation for many proposals to strictly regulate police FRT systems.[81] Indeed, many advocates believe that FRT bias is conclusive proof that FRT systems should be banned in whole or in part[82]. Others believe that FRT bias is a diminishing issue and that better training data can mitigate bias errors in FRT systems.[83]

Many predictive policing system have also been shown to be biased and discriminatory.[84] As noted by the Ontario Human Rights Commission (OHRC), predictive policing systems based on "good data, good decisions and appropriate deployment – in full compliance with the Code and the Charter – can produce positive public safety outcomes."[85] However, "the opposite can happen when predictive policing is used improperly."[86]

The OHRC's 2019 report *Policy on Eliminating Racial Profiling in Law Enforcement*, the OHRC identifies several bias-related concerns about predictive policing, including:

- Biased data;
- Self-justifying feedback loops;
- Data inputs that correlate with race by proxy;
- Biased police deployment;
- Perpetuating existing biases; and
- Conducting risk assessments based on social networks.[87]

The OHRC emphasizes how "law enforcement use of predictive policing must be attuned to the dangers of *Human Rights Code* violations and adverse impacts and take measures to make sure such dangers do not emerge… [such as by] conducting impact assessments of predictive technologies before they are procured and used and amending or abandoning these technologies if they are found to generate discriminatory outcomes."[88]

Concerns about biased predictive policing have led to the withdrawal of many systems in the face of legal challenges and public outcry.[89]

2. Privacy and Surveillance

Privacy and surveillance are one of most widely discussed risks of criminal AI systems, particularly FRT systems. The INCLO report discussed above states:

> *Should a policing FRT system enable member of the public to be identified in public spaces, and/or their movements, interests and associations to be tracked, either in real time or in retrospect, they are at risk of losing not only their privacy rights but also the associated rights built on privacy. These include the right to protest, to freely associate with others and to express one's sexuality, religious belief and/or political affiliation.*
>
> *The manner in which FRT engages the right to privacy can be exacerbated when the FRT system is used live from a distance or in retrospect, without the person's consent, active involvement or knowledge.*[90]

Two recent reports by Canadian Privacy Commissioners, *Police use of Facial Recognition Technology in Canada and the Way Forward*[91] and *Facial Recognition and Mugshot Databases: Guidance for Police in Ontario*[92], describe the privacy risks of police FRT technology comprehensively.

It is important to note that FRT is not the only criminal AI system that can raise privacy and surveillance concerns. The Brennan Center for Justice, an American law and policy institute, describes privacy risks of other technologies as follows:

Video Analytics
Video analytics allow for persistent surveillance as individuals move throughout the city, challenging traditional expectations of privacy.

Social Media
Social media monitoring challenges individuals' reasonable expectations of privacy in online communications.

Predictive Policing
Predictive policing undermines constitutional requirements that police should target individuals based on individualized suspicion, not statistical probability.

ALPRs
Automatic licence plate reader data can provide a detailed account of an individual's movements. It can be used to target people who visit sensitive places, such as immigration clinics, protests, or houses of worship.

Drones
Drones can engage in forms of surveillance that can redefine reasonable expectations of privacy. Drones can also be used to collect information about bystanders who are not connected to a law enforcement investigation.[93]

As with bias risks, privacy risks have led to many proposals to strictly regulate or ban certain criminal AI applications. For example, the Privacy Commission reports cite above set out detailed guidance for how police FRT systems should be governed and implemented to reduce privacy-related risks in certain systems.[94]

3. Disclosure and Transparency

One of ongoing criticisms of AI systems, including AI systems used in the criminal justice system, has been their lack of disclosure and transparency.[95] Disclosure and transparency are fundamental elements of legal and public accountability, especially in the context of criminal prosecutions.[96]

AI disclosure and transparency concerns can arise in three ways:

- Lack of disclosure of the existence of an AI system.
- Lack of disclosure about key elements of an AI systems.
- Lack of disclosure about how an AI system makes decisions.

AI systems in criminal justice have been criticized on all three grounds.[97] In particular, there have been many public controversies about the lack of disclosure of FRT and predictive policing systems. The RCMP's use of Clearview AI is the most prominent Canadian criminal AI transparency controversy. This controversy arose, in part, because the RCMP's use of Clearview AI was not disclosed.[98]

Criminal AI disclosure and transparency concerns have led to many proposals for regulatory and policy reform. The Office of the Privacy Commissioner of Canada's (OPC) *Privacy guidance on facial recognition for police agencies* includes detailed recommendations for disclosing FRT system to both the general public and individuals who may be affected.[99] The Information and Privacy Commissioner of Ontario's *Facial Recognition and Mugshot Datebases: Guidance for Police in Ontario* includes similar recommendations.[100]

4. The "Black Box" Problem

AI systems can embed a complex mix of legal, technical, statistical and operational decisions into code. The complexity and opacity of AI tools may make AI-aided decisions "even more inscrutable than human judgments."[101] As a result, even simple algorithmic and AI systems can be complex and opaque "black boxes." Opacity and a lack of explainability is a particular problem in criminal justice.[102]

5. Data Accuracy, Reliability, and Validity

The accuracy, reliability and validity of data is foundational to the success and legitimacy of AI systems used by police, governments, or courts.[103] FRT and predictive policing systems in particular have been subject to strident criticisms of their training data.[104] Concerns about data accuracy, reliability, and validity are closely related to concerns about data bias. These concerns have led to many proposals to continuously test and evaluate the data used to train criminal AI systems.[105]

Issues around data accuracy, reliability, and validity in criminal AI systems go above and beyond questions of training data. For example, the accuracy, reliability, and validity of FRT systems can be influenced depending on how and when it is used. INTERPOL notes that "the accuracy of [FRT systems]…varies widely depending on the quality of the image fed into the system." FRT systems are less accurate, for example, if they use low quality images, such as side-view images or images captured with low-resolution webcams.[106]

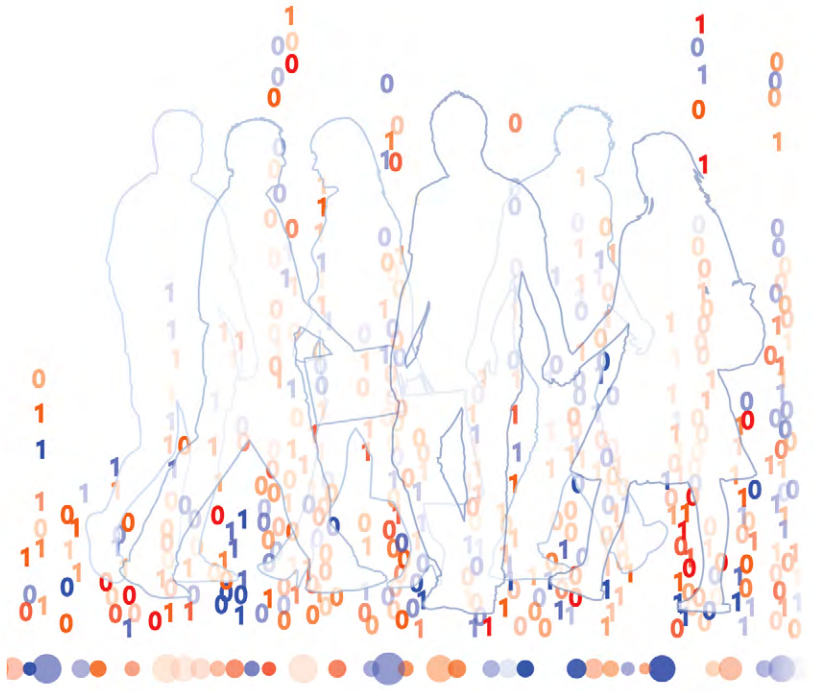
For many advocates, data accuracy, reliability and validity issues suggest the need for extensive testing and monitoring of criminal AI data.[107] Many groups also advocate for the the need to test AI technologies in real-life contexts.[108]

6. Effective Oversight

Criminal AI systems raise several oversight risks, including:

- **Governance Gaps.** Without clear and consistent legal policies or guardrails, there could be gaps in AI legal accountability. For example, not all police services could have AI policies.
- **Inconsistent or Incomplete Judicial Oversight.** Absent consistent rules, courts may have to decide complex AI issues on a case-by-case basis, risking inconsistent or incomplete oversight; delays; and increased litigation costs.
- **Loss of Judicial Independence/Reduced Discretion.** Over-reliance on AI predictions may compromise the appearance or reality of judicial independence. Automation bias may lead decision-makers to limit their discretion, even when there is a "human-in-the-loop."[109]
- **Lack of Public Engagement.** Many criminal AI systems have been criticized by communities who believe they were not consulted or informed about systems that affect them.[110]

These risks could erode *Charter* rights, procedural fairness, the reliability of evidence, and precedents.



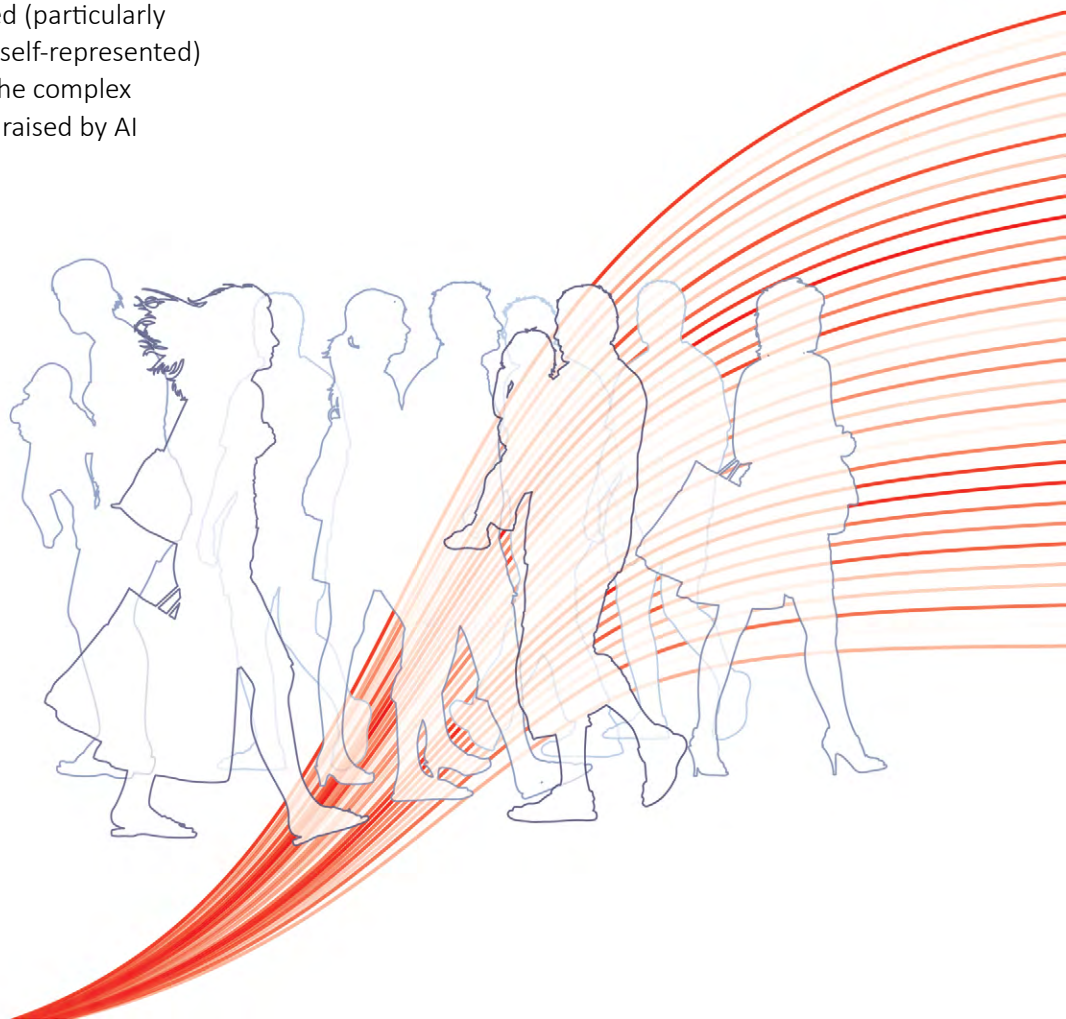
7. Access to Justice

AI litigation places extraordinary legal and financial burdens on the individuals wishing to challenge government AI-based decisions that affect them.[111] These issues are discussed extensively in the LCO's third criminal AI Issue Paper, *AI at Trial and Appeal*, written by Paula Thompson and Eric Neubauer.

The LCO's *American Lessons* Issue Paper discussed the "limits of litigation" extensively, concluding that

> *Litigation has an important role in regulating AI and algorithms in the criminal justice system. Many issues will always be best addressed in open court with the benefit of an evidential record and high-quality and experienced counsel…*
>
> *Litigation, while obviously necessary to address specific cases, is insufficient to address the systemic statistical, technical, policy and legal issues that have been addressed in this report so far.*[112]

The LCO further noted it would be practically impossible for many criminal accused (particularly accused represented by legal aid or self-represented) to mount an effective challenge to the complex statistical, technical and legal issues raised by AI systems.[113]



4. Overview of the Issue Papers

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

The 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, legal aid representatives, court administrators, 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.

The AI in Criminal Justice Project consists of an Introduction and Summary (Paper 1) and four Issue Papers. Each Issue Paper considers the use of AI in a distinct phase of the criminal justice process, including:

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.

4.1 Use of AI by Law Enforcement

The LCO's second project paper addresses the use of AI by law enforcement. This paper was written by LCO Counsel, Ryan Fritsch.

This paper discusses the types of AI-enabled technologies used by law enforcement, both internationally and within Canada, and considers how the use of specific AI-enabled technologies like facial recognition, predictive policing, object recognition, and generated evidence (including "deep fakes") raise novel legal, societal, and constitutional issues.

Issues considered in this paper include:

- How are AI-enabled technologies different from other technologies used by law enforcement?
- What governance frameworks are needed to ensure use of AI by law enforcement meets prerequisites for reliability, necessity and proportionality?
- Are existing legal rules (such as the *Charter*, *Criminal Code*, disclosure obligations, and criminal procedure) sufficient to govern AI technologies, or are reforms needed?
- What governance frameworks are needed to regulate the highest-risk technologies, and what are key elements of such a framework?
- How effective are police self-regulatory policies, such as the Toronto Police Service AI Policy?
- How best to ensure consistent standards and practices across many police services?

The paper further addresses the second step of a criminal proceeding, that being the Crown's assessment of charges and the advice function between Crowns and law enforcement. While law enforcement and Crown prosecutors are constitutionally independent, police often consult with the Crown when deciding whether and how to use AI technologies. Concerns about admissibility, disclosure requirements, or privacy issues associated with AI-enabled investigative tools may influence the Crown's decision not to pursue a charge if there is no reasonable possibility of conviction or it is not in the public interest.

In Canada, the rules governing Crown-police collaboration in the context of AI are not clear. Judicial and professional regulatory policies also offer limited or conflicting guidance. This paper addresses important questions, including:

- Are law enforcement self-regulation policies such the TPSB Use of AI Policy sufficient to ensure *Charter* protections and procedural fairness in police uses of AI?
- How should the Crown advise police on the admissibility and reliability of different kinds of AI evidence?
- What operating procedures will police need to follow for the Crown to fulfill its disclosure requirements with regard to AI evidence?
- How will courts distinguish between investigative and internal police uses of AI, especially when the Crown intends to invoke investigative privilege to protect AI evidence from disclosure?
- Are current interactions between law enforcement and the Crown able to proactively address foreseeable legal challenges with procuring and deploying new AI systems?

4.2 AI and the Assessment of Risk in Bail, Sentencing, and Recidivism

The LCO's third project paper addresses AI, algorithms, and bail. The lead authors of this paper are Armando D'Andrea, Staff Lawyer, Provincial Office, Legal Aid Ontario; and Gideon Christian, Professor of Law, University of Calgary, Faculty of Law.

The use of bail and sentencing algorithms has been the subject of considerable controversy in the US and was considered in an early LCO AI paper, *The Rise and Fall of Algorithms in the American Justice System: Lessons for Canada.*[114]

Bail, sentencing, and post-sentencing decisions have long relied on professional risk assessments to predict an accused or offender's potential danger to the public. However, AI-enabled risk assessments bring new complications, such as the inability to cross-examine "black box" algorithms; technological deference when humans over-rely on AI-generated recommendations; the need to balance the protection of trade secrets against *Charter* and due process rights; and AI systems' potential perpetuation of racist and colonialist systemic biases.

These issues may be amplified by the unique nature of bail hearings, which tend to be quicker and more informal, and sentencing and post-sentencing hearings, in which the presumption of innocence is no longer operative. This paper addresses several critical questions including:

- Does AI-enabled risk assessment meet the threshold for admissibility as expert opinion, a demonstrative aid, or some other kind of evidence?
- Are AI-enabled risk assessments based on group characteristics compatible with the need to tailor individualized conditions on bail?
- How can the criminal justice system balance the need for transparency with the proprietary rights of commercial corporations that design AI risk assessment tools?
- Do courts and other criminal justice actors have the resources necessary to protect rights and ensure procedural fairness when using AI-enabled risk assessments, particularly considering the fast-paced nature of bail hearings?
- What legislative or regulatory measures should be introduced to ameliorate the deficiencies of AI-enabled risk assessment systems before their deployment in the criminal justice system?

4.3 AI at Trial and on Appeal

The LCO's fourth project paper addresses AI at trial and appeal. This paper was written by Paula Thompson, Strategic Initiatives, Ministry of the Attorney General and Eric Neubauer, Defense Counsel, Neubauer Law, and Co-Chair, Criminal Lawyers Association Technology Committee.

AI raises novel issues that are fundamental to ensure fair trial process and protection of liberty and constitutional rights. Trials and appeals ensure a fair and transparent proceeding by relying on the *Charter of Rights and Freedoms*; common law principles guiding case interpretation and procedural fairness; and evidence law. The introduction of AI—both as evidence and in analytical tools employed by litigants and officers of the court—raises new concerns about disclosure, admissibility, bias, and access to justice that are not directly addressed by existing legislation and case law. The criminal justice system's incorporation of evidence from complex technologies such as breathalyzers and body cams offer some guidance. However, courts will still have to grapple with a variety of critical questions, including:

- How are *Charter*, procedural fairness, and common law rights affected by AI-enabled technologies, and how will existing law apply?
- Are the existing processes and timing for introducing and contesting evidence, including complex technological evidence such as breathalyzers and body cams, sufficient for AI evidence?
- How will courts and other criminal justice actors maintain the professional competence required to assess AI tools and evidence and mitigate the risk of technological deference?
- How will AI impact courts' existing concerns about systemic issues like bias and discrimination and access to justice?
- How will courts exercise their jurisdiction over trials, appeals, and justice-involved institutions with regard to AI-enabled technologies?
- What statutory, regulatory, evidentiary, or other changes are necessary to ensure that the use of AI-enabled technologies complies with the law?

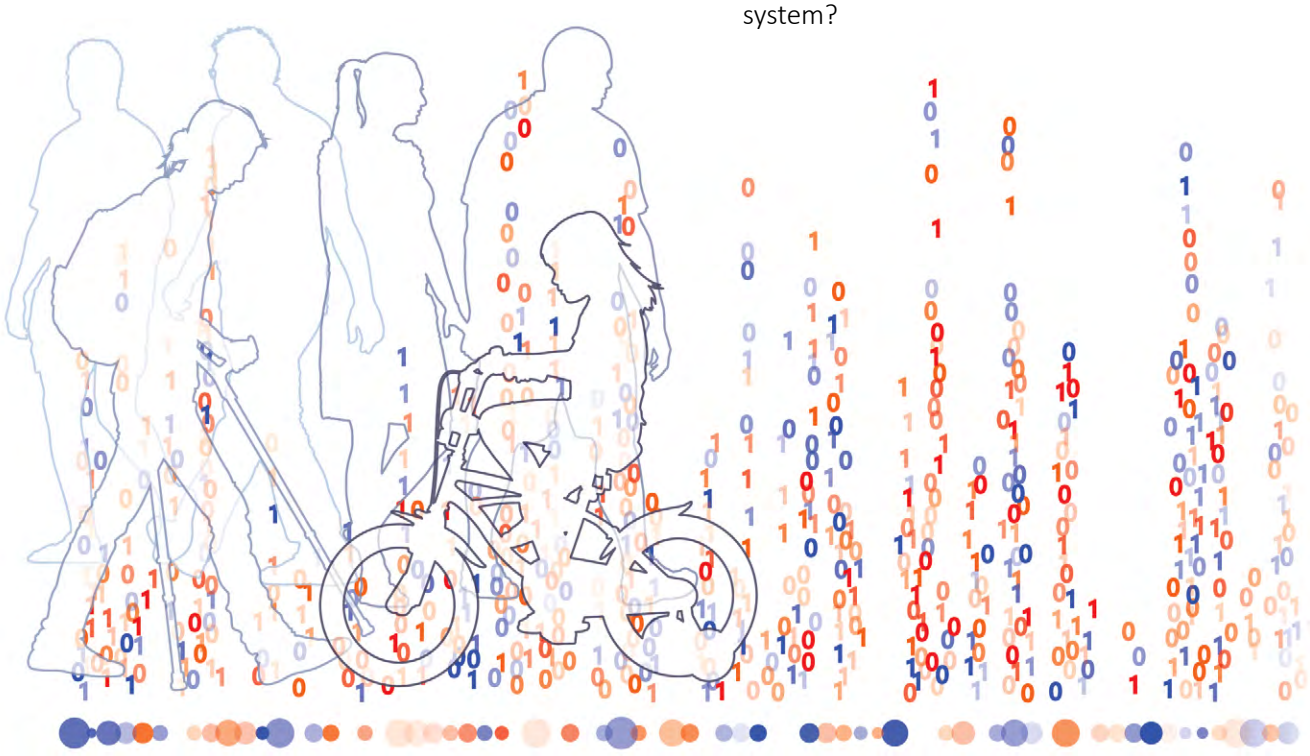
4.4 AI and Systemic Oversight Mechanisms

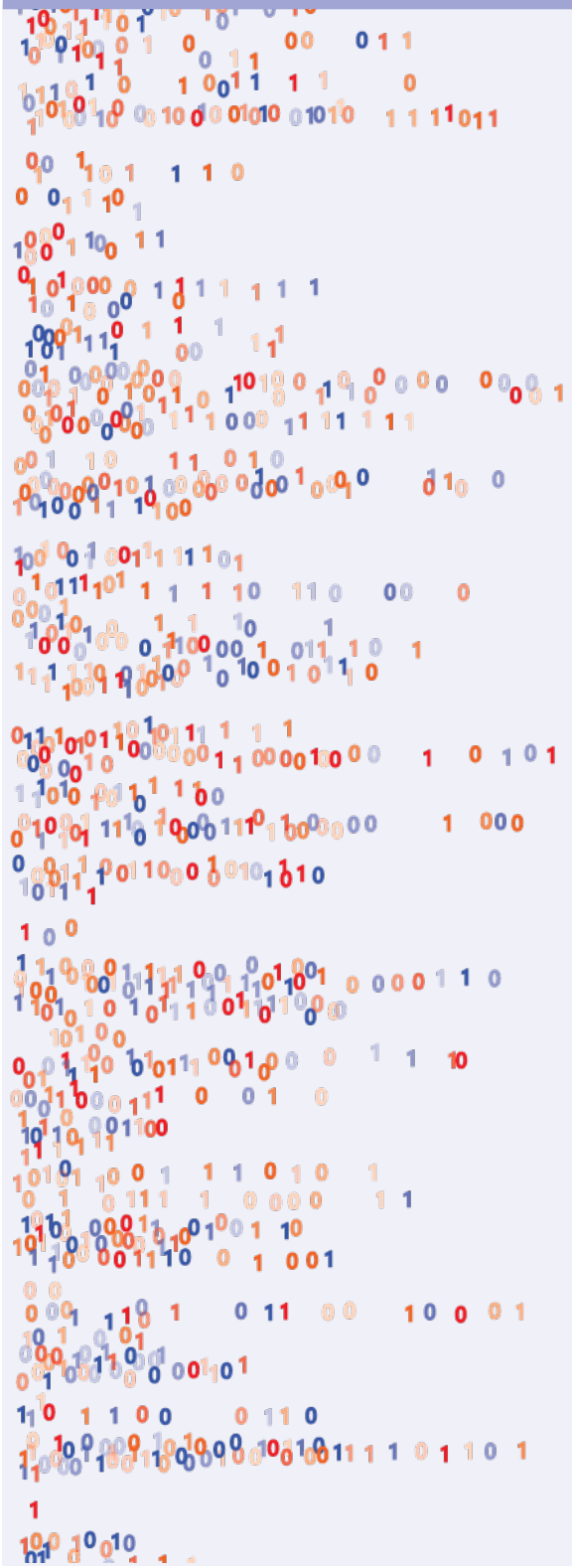
The final LCO project paper addresses systemic oversight. The authors of this paper are Brenda McPhail, Senior Technology and Policy Advisor, Office of the Information and Privacy Commissioner of Ontario; Marcus Pratt, Director of Policy, Legal Aid Ontario; and Jagtaran Singh, Legal Counsel, Ontario Human Rights Commission.

The introduction of AI technologies into criminal law comes with a variety of legal, ethical, and practical concerns that are only partially addressed by existing law and procedure. Even individuals who are neither accused of a crime nor otherwise involved in the criminal justice system may have their privacy rights breached by police or other government uses of AI. Without robust legal, regulatory, and policy frameworks, the criminal law process is limited in its ability to oversee the use of AI by state actors and mitigate potential abuses.

While the federal Bill C-27 and Ontario's *EDSTA* contain some important regulatory measures, their application to criminal law is limited. Key issues include the lack of access to remedies for rights breaches, the lack of independent oversight bodies, and the relatively narrow understanding of privacy rights reflected in current legislation and case law. New and proposed legislation from jurisdictions such as the EU and the US may offer guidance; however, these approaches also have gaps. Many questions remain unanswered, including:

- What are the limits of *Charter*, evidentiary, and *Criminal Code* rights and remedies when it comes to protecting individuals from the threats posed by state uses of AI?
- What oversight mechanisms are required to ensure that individuals' privacy rights are protected from state uses of AI, and that individuals have access to remedies when their privacy rights are breached?
- How can the criminal justice system ensure the safety, transparency, and accountability of AI technologies and their use by police and government actors?
- How have other jurisdictions sought to address the challenges AI poses to the criminal justice system?





Who Will Be Affected by AI in Ontario's Criminal Justice System?

The LCO's Issue Papers demonstrate the wide, diverse, and decentralized provincial network of institutions and actors who could be involved in developing, operating, overseeing, litigating, or adjudicating AI issues in Ontario's criminal justice system, including

- All 53 police services in Ontario.
- Police service boards, municipalities, and regional governments.
- The provincial Ministry of the Solicitor General.
- 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.
- Provincial oversight agencies (including the Ontario Human Rights Commission, Ontario Information and Privacy Commissioner, and Inspectorate of Policing).

Criminal charges alone may result in prolonged detention, disrupted lives, loss of child custody, loss of housing and income, plea deals accepted under pressure, criminal records, lasting social stigma, and loss of opportunity. There is a litany of well documented "secondary consequences" that flow from both criminal charges and convictions.[115] The LCO believes the breadth or complexity of this network is an important factor influencing criminal justice AI regulation and governance. This wide and decentralized actors and institutions potentially involved in criminal justice AI underscores the need for provincial coordination and consistency to avoid the risks and harms discussed in this paper.

5. Trustworthy Criminal AI

The potential benefits, risks, and harms of AI in criminal justice are widely documented and acknowledged by governments, police services, prosecutors, defence counsel, academics, and NGOs around the world. This acknowledgement has led to an extraordinary range of laws, policies, frameworks, and other initiatives based on the principle that harnessing AI's benefits depends on dedicated and sophisticated rules to minimize risks and harms.

The need to ensure trustworthy criminal AI in Canada is just as urgent. AI in the criminal justice system affects some of most important issues and rights in Canadian society, including public safety, *Charter* rights, human rights, civil liberties, privacy protections, procedural fairness, and public trust in key public institutions, including courts and the police.

To their credit, some Canadian police services and agencies have taken important initiatives to address criminal AI risks. Unfortunately, there are still wide and consequential gaps in the legislative and legal framework governing these systems.

As will be seen, Canadian law makers 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. Canadian readers may be surprized by the speed, range, and sophistication of these efforts, many of which include the following elements:

- Mandatory disclosure of criminal AI systems, including public "AI registers".
- Prohibitions on highest risk criminal AI systems
- Criteria to identify prohibited or high-risk systems.
- Purpose and use limitations.
- Mandatory and transparent AI impact assessments.
- Mitigation requirements.
- Mandatory obligations to measure, correct and audit bias.
- Procedural protections, such as warrant requirements for high-risk systems.
- Mandatory "human in the loop" requirements and training.
- Mandatory auditing and evaluation requirements.
- Independent oversight of individual systems and government AI generally.

International initiatives to develop trustworthy criminal AI are often related to, but separate from, the unprecedented range and complexity of public sector "trustworthy AI" legislation, frameworks, and policies that have been adopted around the world.[116] The LCO and other organizations have surveyed many of these initiatives in earlier reports.[117]

It is difficult to generalize these initiatives, but readers should note that AI legislation and regulations are much more sophisticated today than they were even three or four years ago. Initiatives such as the EU *Artificial Intelligence Act*, legislation and regulations in the United States, and the Government of Canada's *Artificial Intelligence and Data Act* and Directive on Automated Decision-making have established important benchmarks for public sector AI legislation and regulation.

The LCO does not believe any single international precedent or framework can or should be adopted in Canada. The details within various "trustworthy AI" legislation, regulations, and policies vary considerably. Most importantly, any governance framework in Canada must be tailored to our criminal justice system and institutions, including the *Charter*, *Criminal Code,* privacy laws, evidence laws, criminal procedure, and the criminal common law.

That said, the LCO believes Canadian policymakers and stakeholders can learn important lessons about how to address documented AI risks and harms from the experience of other jurisdictions. As a result, the following section summarizes criminal justice AI governance and regulation in the EU and the United States. Subsequent sections of this Introduction summarize criminal AI governance and regulation in Canada. These issues are considered in more detail in our project Issue Papers.

6. Criminal Justice AI Governance and Regulation

6.1 European Union Artificial Intelligence Act

The European Union *Artificial Intelligence Act* (EU *AI Act)* came into force in August 2024.[118] Its provisions will be implemented gradually, with the Act being fully implemented by August 2027. The EU *AI Act* is sweeping, framework legislation governing the development and use of AI systems across the European Union, including systems used in both the private and public sector.

The EU *AI Act* incorporates a sliding-scale AI risk assessment framework with four levels of risk: unacceptable, high risk, limited risk and minimal.[119]

Unacceptable Risks/Prohibited Systems

Chapter II, Article 5 of the EU *AI Act* sets out several "unacceptable risks" and prohibitions on specified AI systems. These provisions came into force in February 2025. These systems are deemed "unacceptable" because they are a clear threat to European values and fundamental rights. Article 5 prohibits two AI systems that are directly relevant to criminal justice:

1. *Real-time remote biometric identification in publicly accessible spaces for law enforcement.*

This prohibition is a partial ban on real time mass FRT and biometric surveillance. This prohibition is subject to several important exceptions. For example, the EU *AI Act* allows the use of real time remote biometric surveillance if law enforcement agencies are:

- Searching for missing persons, abduction victims, and people who have been human trafficked or sexually exploited.
- Preventing a substantial and imminent threat to life, or foreseeable terrorist attack.
- Identifying suspects in serious crimes.[120]

If real time biometric surveillance is used in these circumstances, the EU *AI Act* explicitly includes several accountability safeguards, including requirements to complete a fundamental rights impact assessment[121]; to obtain judicial or administrative authorization[122]; and to register the system in an EU database.[123]

2. *Assessing the risk of an individual committing criminal offenses solely based on profiling or personality traits.*

This prohibition is a partial ban on predictive policing AI systems.[124] This prohibition is also subject to important exceptions that allow law enforcement to use predictive policing in prescribed circumstances.[125]

High Risk AI Systems

In addition to outright prohibitions, Article III of the EU *AI Act* defines several criminal justice AI systems as "high-risk" due to their significant risk to rights and freedoms, including bail and sentencing algorithms and AI-generated evidence in criminal trials.[126]

The EU *AI Act* sets out important accountability safeguards if police or governments want to deploy high-risk systems, including requirements respecting:

- Risk management throughout the system's lifecycle.
- Data governance, validation, and testing.
- Technical documentation.
- Record-keeping for identifying national level risks.
- Human oversight.
- Accuracy, robustness, and cybersecurity.
- Quality management to ensure compliance.[127]

6.2 US Federal Government Executive Orders on AI

In contrast to Europe, AI systems used by the US federal government and agencies had until recently been regulated by Executive Orders, not legislation.

In October 2023, the U.S. government issued Executive Order 14110 on "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence."[128] This lengthy policy setout detailed requirements for U.S. federal departments and agencies using AI.

Executive Order 14110 was followed in March 2024 with an Office of Management and Budget (OMB) guidance on the management of AI systems and applications used by federal agencies. This guidance (also known as Memorandum M-24-10) included detailed "trustworthy AI" governance requirements for "rights-impacting" AI systems used by U.S. departments and agencies covered by the Executive Order.[129] These requirements include an obligation to:

- Assess AI impact on equity and fairness and mitigate algorithmic discrimination.
- Consult and incorporate feedback from affected communities and the public.
- Conduct ongoing monitoring and mitigation for AI-enabled discrimination.
- Notify negatively affected individuals.
- Maintain human consideration and remedy processes.
- Maintain opt-out processes.[130]

Memorandum M-24-10 included a long list of AI systems that are "automatically *presumed* to be safety-impacting or rights-impacting [Emphasis in original]."[131] This list includes no fewer than 18 systems potentially used in criminal justice, including AI used to:

- Conducting biometric identification (e.g., iris, facial, fingerprint, or gait matching).
- Produce risk assessments about individuals.
- Predict criminal recidivism, criminal offenders, or victims of crime.
- Forecast crime.
- Track personal vehicles over time in public spaces, including license plate readers.
- Identify criminal suspects.
- Detect gunshots.
- Monitor social media.
- Forensically analyze criminal evidence.
- Conduct forensic genetics.
- Conduct physical location-monitoring or tracking of individuals.

- Make determinations related to sentencing, parole, supervised release, probation, bail, pretrial release, or pretrial detention.[132]

Executive Order 14110 and Memorandum M-24-10 established a comprehensive regime that adopts most, if not all, components of a trustworthy criminal AI framework.

In January 2025, both Executive Order 14110 and Memorandum M-24-10 were rescinded by the new Trump administration.[133] To date, it is not clear if the new administration will be issuing a new AI Executive Order. Interestingly, the first Trump administration issued an Executive Order that included many trustworthy AI elements.[134]

6.3 US State and Municipal Criminal Justice AI Statutes and Policies

In addition to the federal orders discussed above, there have been dozens of U.S. state and municipal statutes and policies governing AI systems, including AI used in law enforcement.[135] For example, statutes governing police use of FRT is common, with more than 30 state or municipal statutes prohibiting or limiting the use of FRT as of November 2024.[136] There are also numerous state and local statutes governing predictive policing, license plate readers, lateral surveillance, and other forms of technology-aided policing and surveillance.[137]

American FRT legislation is a good example of the range and scope of potential Canadian legislation. Many US statutes limit FRT use to specific use cases and include extensive accountability mechanisms.[138]

The AINow Institute, an American research organization, recently published an overview of U.S. facial recognition legislation.[139] The report states that "[t]here is now widespread agreement that regulation is necessary, even as lawmakers, advocates, law enforcement, and other stakeholders may disagree on exactly what that looks like."[140]

AINow states there are three approaches to regulating FRT in the U.S., including bans, temporary or directive moratoria, and regulatory bills.[141] Common elements of regulatory bills include:[142]

- Establishing a Task Force or Working Group.
- Requirements on companies, including bias testing, data access.
- Accountability and transparency reports.
- Process regulations, including officer training, reviews, disclosure to defendants.
- Explicit civil rights protections, including prohibiting FRT surveillance based on race, immigration status, sexual orientation, etc.
- Data and access restrictions, such as limits on use of state drivers' licence records.
- Targeted bans, including banning "real time" FRT or used with body cameras, drones.
- Court order Requirements, including warrant requirements to run FRT searches.

There are also many helpful models for proposed FRT legislation. For example, the Policing Project at the New York University School of Law has produced a comprehensive package of resources to provide "actionable guidance to legislators seeking to address the risks posed by ongoing, unregulated use" of FRT.[143] A summary of their "legislative checklist for State Lawmakers" is included in the text box on the next page.

The Policing Project: Legislative Checklist for Law Enforcement Use of FRT

The Policing Project at the New York University School of Law has developed "minimum legislative requirements… for the most common law enforcement use of FRT."[144] Notable requirements include:

DEMOCRATIC AUTHORIZATION

- Police FRT should be banned unless authorized by democratically accountable body.
- FRT use should be centralized in single agency. If local agencies are permitted to use FRT, use must be approved by local democratically accountable body.
- Legislation should authorize FRT only for a limited pilot period.

TRANSPARENCY AND DATABASES

- Require legislative authorization for FRT databases. If non-law enforcement databases are authorized (such as drivers' licence databases) the public should be notified.
- Prohibit FRT searches on private databases including social media scrapping.
- Require policing agency to have public comprehensive use policy.
- Require details of FRT use in individual cases to be included in case files.
- Require public annual FRT use reports and audits.

TESTING AND TRAINING

- Require comprehensive technology, scenario and operational testing.
- Require specialized training.
- Require FRT review by a trained human-in-the-loop before match determined.

PROHIBITIONS, USE LIMITATIONS, AND PROCEDURAL REQUIREMENTS

- Ban FRT for surveillance and for use to identify suspects who are minors.
- Limit FRT searches the investigation of serious felonies or to identify deceased, incapacitated, or missing persons.
- Require warrants for FRT searches.
- Require disclosure to accused.

ENFORCEMENT

- Remedies for statutory violations should include exclusion, injunctive relief, administrative remedies, and civil actions.

6.4 Police Service "Trustworthy AI" Policies

Finally, the LCO wants to highlight the range and sophistication of trustworthy criminal AI policies that have been adopted by police services in the United States and internationally. Examples include the New York City Police Department (NYPD) FRT policy[145], the Los Angeles Police Department FRT policy[146], and INTERPOL's *Principles for Responsible AI Innovation*.[147] The INTERPOL principles are summarized on pages 37 and 38.

These policies are notable for several reasons: First, they acknowledge the risks with criminal AI systems. Second, many, if not most, of these policies are broadly consistent with the trustworthy AI principles the LCO has identified so far. Finally, they demonstrate that police services themselves recognize that initiatives harnessing AI benefits depends on adopting dedicated and sophisticated rules to minimize its risks and harms.

The 2023 New York Police Department Facial Recognition Technology policy is an interesting example of how the NYPD limits FRT to specific use cases. Under the policy, NYPD use of FRT is only authorized in the following prescribed circumstances:

> *AUTHORIZED USES - Facial recognition technology must only be used for legitimate law enforcement purposes. Specifically, the following are the only authorized uses for employing facial recognition technology:*
>
> *a. To identify an individual when there is a basis to believe that such individual has committed, is committing, or is about to commit a crime,*
>
> *b. To identify an individual when there is a basis to believe that such individual is a missing person, crime victim, or witness to criminal activity,*
>
> *c. To identify a deceased person,*
>
> *d. To identify a person who is incapacitated or otherwise unable to identify themselves,*
>
> *e. To identify an individual who is under arrest and does not possess valid identification, is not forthcoming with valid identification, or who appears to be using someone else's identification, or a false identification, or*
>
> *f. To mitigate an imminent threat to health or public safety (e.g., to thwart an active terrorism scheme or plot, etc.).*[148]

The policy further states that a FRT image match does not establish probable cause for an arrest or search warrant but "may generate investigative leads."[149] The policy also states that the FRT matching process must be undertaken by a dedicated NYPD Facial Identification Section. Finally, the policy establishes additional guardrails, including limitations regarding body cameras, security cameras, rallies, and images from social media and government databases, such as driver's license photos.[150] It should be noted that many community and civil society organizations have criticized these policies for being too permissive and failing to address the impact of FRT and surveillance technology on racialized communities.[151]

Interpol "Principles for Responsible AI Innovation"

Interpol, the International Criminal Police Organization, has developed a seven-part AI Toolkit as "a practical guide for law enforcement agencies on developing and deploying artificial intelligence responsibly, while respecting human rights and ethics principles."[152]

The Toolkit's "Principles for Responsible AI Innovation" are "designed to guide law enforcement agencies across the world in integrating AI systems into their work in ways that align with good policing practices and AI ethics, and respect human rights."[153]

The Interpol AI Principles outline a comprehensive framework to govern the development, deployment, and oversight of AI systems used by police services. Interpol's principles and recommendations include:

LAWFULNESS

[A]gencies must follow the applicable laws and regulations throughout the design, development, and use of AI systems.

Respecting human rights is also an essential part of lawfulness.

[L]aw enforcement agencies should ensure legitimacy, necessity, and proportionality whenever they engage with AI systems in ways that could have an impact on human rights.

Before procuring the AI system, the agency should conduct a human rights impact assessment.

MINIMIZATION OF HARM

[L]aw enforcement agencies prevent, eliminate, or mitigate the risk of harm to individuals and communities that can arise in the context of AI development, procurement, and use.

To ensure robustness, law enforcement agencies should confirm that the AI systems they intend to use are both reliable and secure.

[Law enforcement agencies should verify] that any system they are developing and/or intend to use is highly accurate…[B]efore deploying an AI system into mainstream application in the law enforcement context, such system needs to be subject to rigorous and scientific testing.

HUMAN CONTROL AND OVERSIGHT

[L]aw enforcement agencies [need] to ensure that humans remain in charge during use, as well as to confirm that the necessary organizational structures are in place to ensure that humans have the last word regarding certain decisions.

Interpol "Principles for Responsible AI Innovation"

HUMAN AGENCY

[L]aw enforcement agencies need to ensure that the AI systems they aim to use do not compromise the ability of the users of those systems (law enforcement officers, other personnel, citizens, etc.) to act and make decisions independently.

TRANSPARENCY AND EXPLAINABILITY

[L]aw enforcement agencies are advised to verify that the developers of their AI system (internal or external) disclose all the necessary information and documentation to its users.

It is crucial that the AI systems deployed by law enforcement agencies are explainable so that the people that use these systems or are affected by them can make sense of and meaningfully react to their outputs.

EQUALITY AND NON-DISCRIMINATION

Respecting equality and non-discrimination within AI innovation in law enforcement means ensuring equal treatment and opportunities for all stakeholders and refraining from unjustifiably discriminating against individuals or groups throughout the AI life cycle.

[L]aw enforcement agencies need to ensure that the AI systems they use are trained with data sets containing the appropriate quality and quantity of data and that any identifiable and discriminatory biases are removed.

PROTECTING VULNERABLE GROUPS

[L]aw enforcement agencies should pay particular attention and due consideration to those groups who are most vulnerable to and at risk of being disadvantaged by the use of specific AI systems.

CONTESTABILITY AND REDRESS

The principle of contestability means that law enforcement agencies should ensure that the necessary technological and organizational measures are in place to allow both users and those affected by decisions based on the output of an AI system to challenge these decisions.

The principle of redress means that agencies should go one step further and ensure that, when AI supported decisions have an unjust negative impact, those affected are able to formally seek redress through adequate and accessible processes.

GOOD GOVERNANCE

[G]ood governance means that agencies should aim to set up an overarching structure for audits and accountability and to foster a culture of responsible AI innovation, including traceability, auditability, and ensuring stakeholders know who is responsible for AI decision-making.

7. Trustworthy Criminal AI in Canada

The previous section surveyed international initiatives to promote trustworthy criminal AI. This section considers five potential sources of trustworthy criminal AI in Canada:

- Existing *Charter* protections, the *Criminal Code of Canada,* human rights law, evidence law, common law rules and related statutes.
- New or pending Canadian AI legislation.
- Federal and provincial AI policies or directives.
- Canadian law enforcement AI policies.
- AI guidance from other organizations or agencies, such as courts or privacy commissions.

7.1 Current Law and Policies Applicable to Criminal AI Systems

The LCO's project Issue Papers analyze how existing *Charter* protections, the *Criminal Code,* statutes, human rights law, common law rules, criminal procedure, and rules of evidence can or will be used to respond to the challenges of AI in each stage of the criminal justice system. The Issue Papers present a comprehensive analysis of the strengths and gaps of this complex legal framework.

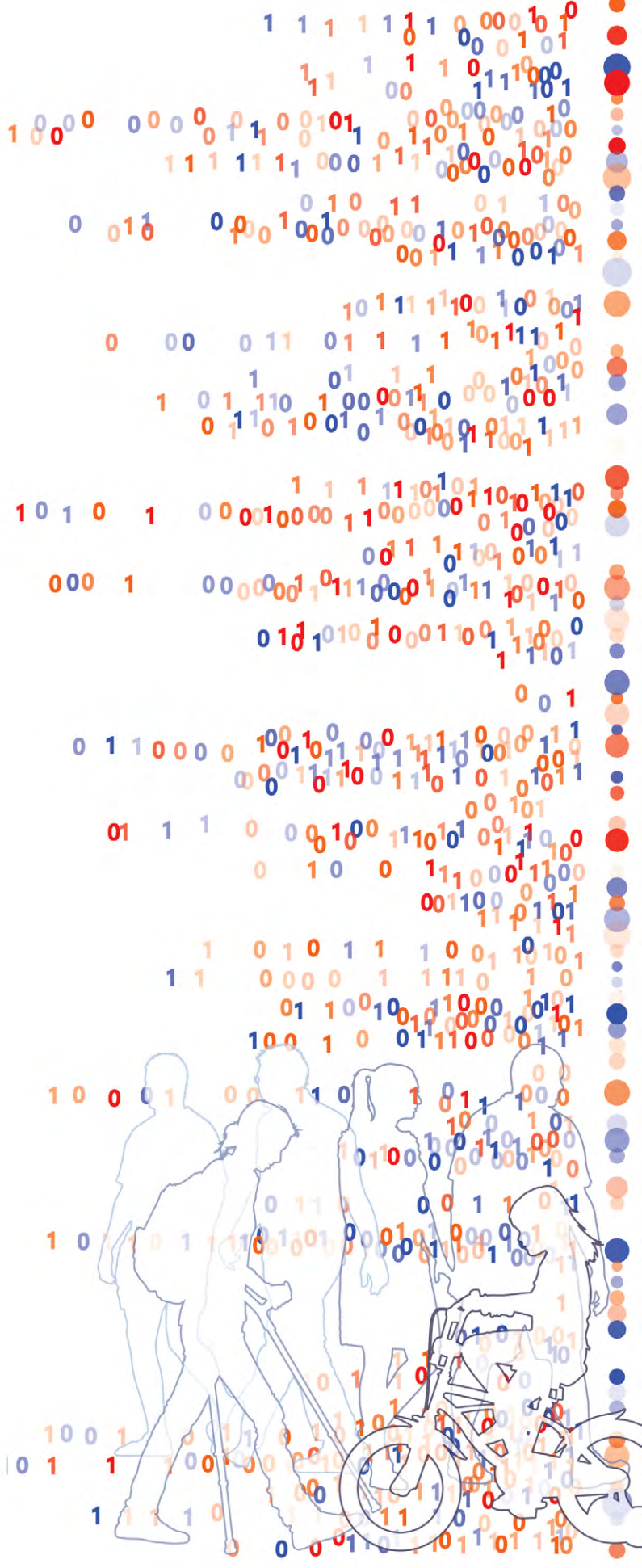
The text box on the page 41 summarizes how the Canadian justice system currently ensures new technology is consistent with *Charter* protections, human rights law, evidence law, common law rules and statutes.

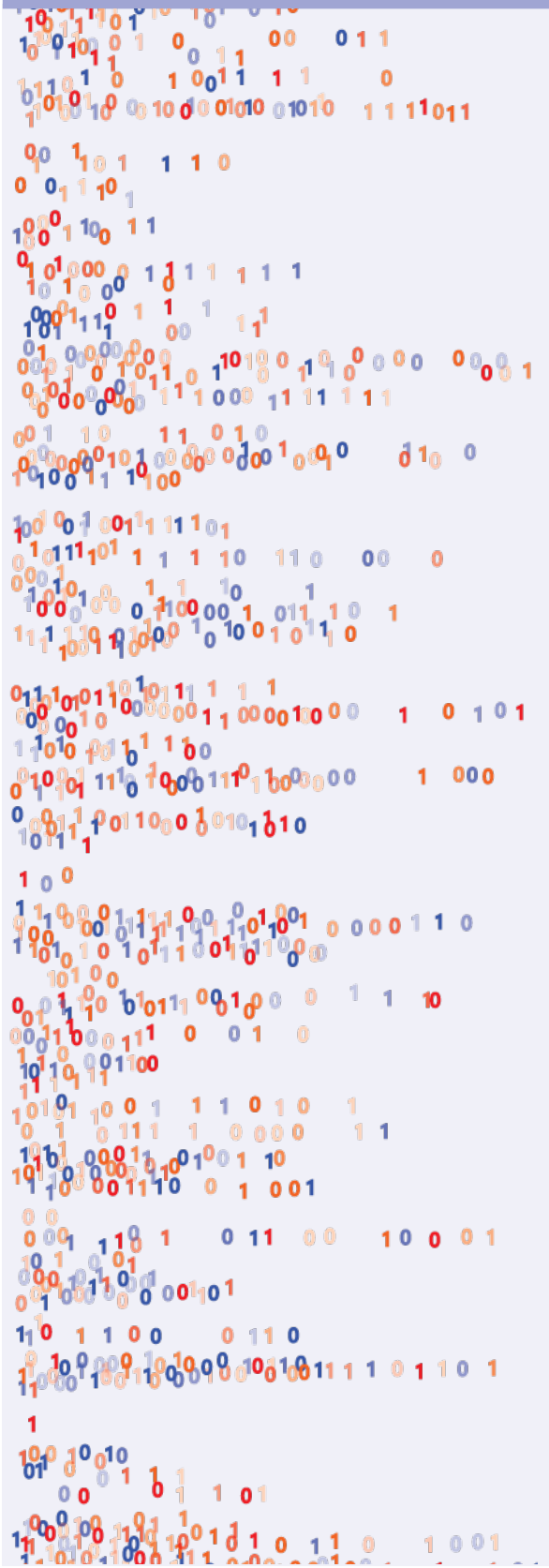
Readers should refer to specific Issue Papers for detailed analysis of specific technologies and procedures.

In summary, the LCO and our project authors have concluded that, while existing legal rules and procedures have many strengths, they do not establish a comprehensive framework establishing trustworthy criminal AI in Canada. In short, the LCO and our project authors have concluded that:

- AI raises novel, complex, and consequential issues and choices at each stage of a criminal proceeding.
- Improperly designed or operated AI systems could have profound implications for liberty interests, constitutional rights, privacy, access to justice, criminal procedure, court efficiency, and public trust in the Canadian criminal justice system.
- There is a need for AI accountability at each stage of the criminal justice system. These accountability issues will be compounded if AI is implemented across several stages simultaneously.
- There are important questions about whether agencies and courts will be able to determine or apply consistent disclosure obligations, bias and privacy testing, reliability criteria, etc.
- "Regulation by litigation" is likely not sufficient to address the systemic, complex and compounding challenges of AI. It is possible that only the best resourced and most sophisticated criminal accused will be able to challenge AI-aided police charges and prosecutions. AI places many new burdens on criminal accused which are likely to compound existing overrepresentation of low-income, racialized, and Indigenous communities in Canadian criminal justice.

These concerns will be compounded in the wide, diverse, and decentralized provincial network of institutions and actors who will be involved in developing, operating, litigating, or overseeing AI in Ontario's criminal justice system. The coordination, access to justice, and legal accountability challenges across this network will be pervasive and difficult.





How Does the Canadian Criminal Justice System Ensure New Technology Is Consistent With Rights?

The Canadian criminal justice system has a long history of regulating new and novel technologies, including Breathalyzers, body cameras, tasers, mobile phone tracking and triangulation, decryption, DNA identification, and aerial surveillance, to name a few. In many cases these technologies have been controversial.

Several pillars of the criminal justice system work to ensure new technologies are consistent with Canadian law, including the *Charter*, human rights codes, the *Criminal Code of Canada*, evidence acts, rules of criminal procedures, Crown policy manuals, court decisions, etc.

Governments, law enforcement agencies, and other justice institutions often develop dedicated safeguards or rules governing the approval, use, and oversight of new technology, including:

- Presumptive prohibitions on the use of specific technologies.
- Judicial authorization or warrant requirements.
- Dedicated "responsible use" policies.
- Procurement rules.
- External technical and performance assessments and reports.
- Training programs and performance measures.

The regulation of intoxilyzers in Canadian criminal proceedings is a good example of a dedicated "responsible use" framework. Section 320 of the *Criminal Code* sets out detailed procedural requirements governing how intoxilyzers may be used, including certification standards, independent performance criteria, and rules respecting their admissibility of the evidence. See ***Annex B: Project Case Studies*** for a longer discussion of the suitability of intoxilyzer-style regulation for AI technologies.

AI systems in criminal justice could be subject to equivalent procedural safeguards.

7.2 Canadian Federal AI Legislation and Government Directives

Unlike the EU *AI Act*, there is no general or framework AI legislation governing criminal AI systems in Ontario or Canada.

The proposed federal *Artificial Intelligence and Data Act* (*AIDA*) and recently passed Ontario *Enhancing Digital Security and Trust Act, 2024 (EDSTA)* are the two most prominent proposals to regulate some aspects of AI in Canada. This section will discuss these statututes and two relevant government directives: the federal government's Automated Decision-making Directive and Ontario's new Responsible Use of Artificial Intelligence Directive.

7.2.1 The Federal Artificial Intelligence and Data Act (*AIDA*)

In June 2022, the federal Minister of Industry, Science and Economic Development (ISED) introduced the draft *Artificial Intelligence and Data Act* (AIDA) as part of Bill C-27.[154]

Like the EU *AI Act*, *AIDA* proposed a risk-based approach to AI governance. Unlike the EU *AI Act*, however, *AIDA* did not directly regulate the use of AI in the public sector or criminal justice system. Rather, *AIDA* would have applied to private sector organizations responsible for the "development, deployment, use or making available of AI systems" and not government institutions. [155]

Unlike the EU *AI Act, AIDA* did not include explicit bans or prohibitions on AI systems that have unacceptable risks. *AIDA* stated, however, that the minister would have the power to order any party to cease using a high-impact system if the minister believes the system could cause serious risk of imminent harm.[156]

As drafted, *AIDA* included several significant trustworthy AI principles: For example, although *AIDA* did not include detailed risk criteria or categories, it stated that "high-impact systems" were those that met criteria "that are established in regulations."[157] *AIDA* also required persons responsible for AI systems to assess whether their systems were high-impact and to "establish measures to identify, assess and mitigate the risks of harm or biased output" in accordance with *AIDA* regulations.[158] Finally, *AIDA* required persons responsible for high-impact systems to "publish on a publicly available website" plain language descriptions of how the system would be used, mitigation measures, etc.[159]

When it was introduced, *AIDA* was heavily criticized for being "shell" legislation that left most of the details to be determined through regulations. This structure was intentional, as the federal government believed *AIDA* would create a set of "agile" rules that could adapt to changing technology. [160] Many stakeholders and commentators disagreed with this approach, believing that specificity was needed to ensure the legislation was effective. There was also considerable criticism about the lack of consultation in creating the Bill.[161]

The federal government responded to these criticisms by releasing a companion document in March 2023 and a November 2023 letter with several proposed amendments.

The federal government's November 2023 amendments included references to high impact AI systems used in criminal justice. Most notably, the federal government committed to *AIDA* amendments that would define seven "classes of systems that would be considered high impact", including three relevant to criminal justice:

> *Class 3: The use of an artificial intelligence system to process biometric information in matters relating to:*
>
> *a. the identification of an individual, other than in cases in which the biometric information is processed with the individual's consent to authenticate their identity; or*
>
> *b. the assessment of an individual's behaviour or state of mind.*
>
> *Class 6: The use of an artificial intelligence system 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.*

Class 7: The use of an artificial intelligence system to assist a peace officer, as defined in section 2 of the Criminal Code, in the exercise and performance of their law enforcement powers, duties and functions.[162]

The federal government's proposed amendments did not assuage *AIDA*'s critics. Many organizations continued to call on the federal government to withdraw the legislation.[163] For example, a March 2024 "AIDA Priority Recommendation Package" endorsed by the International Civil Liberties Monitoring Group and Privacy & Access Council of Canada criticized the amended legislation for:

- The lack of public consultation in developing *AIDA*.
- The need for ongoing public consultation and reports.
- The need to strengthen *AIDA* human rights protections, including impact assessments.
- The need to conduct good faith and comprehensive consultation and cooperation with Indigenous Peoples to fix the many elements of Bill C-27 which infringe Indigenous rights.
- The need for an outright prohibition of "unacceptable risk" uses of AI — e.g. biometric identification/FRT in public places.
- The inappropriateness of defining "high-impact" based on intended uses alone, and the lack of legislative criteria or guiding principles to define high-impact systems and levels of risk.
- The need to address the use of AI in the public sector.[164]

AIDA was not passed by the federal government before Parliament was prorogued in January 2025.

7.2.2 The Federal Automated Decision-making Directive

AIDA is not the only relevant federal AI governance instrument. In 2021, the federal government enacted the Automated Decision-making Directive (federal ADM Directive) and its companion, the Algorithmic Impact Assessment (AIA). The federal ADM Directive and AIA apply to a broad range of federal technology systems, not just AI systems.[165]

The LCO has written at length about federal ADM Directive and AIA, noting its strengths and weaknesses.[166] In general, we have praised both as leading examples of tools and strategies that incorporate procedural fairness protections into the design and operation of automated government decision-making.[167] For the purpose of this report, however, the Federal Directive and AIA's most notable feature is that they do not apply to federal law enforcement agencies.[168]

Importantly, the federal ADM Directive and AIA have both been updated since their adoption, including the release of a comprehensive guide to help organizations complete the AIA.[169] Indeed, the federal government is currently undertaking its fourth review of the federal ADM Directive and AIA.[170] This review includes proposals to strengthen the Directive's human rights provisions and more explicit criteria addressing prohibited or banned federal AI systems. These proposals, while welcome, do not extend the reach of the Federal Directive and AIA to federal law enforcement agencies.

7.2.3 RCMP

In response the OPC's special report, the RCMP created the National Technologies Onboarding Program (NTOP). RCMP policy requires that any RCMP unit considering the use of a technology-based tool, technique, device software, application or dataset used to support investigations or intelligence gathering must consult the NTOP before testing, purchasing, developing or deploying any operational technology that is primarily intended to collect or use personal for investigation and/or intelligence gathering. Artificial intelligence and privacy intrusive technologies are NTOP's highest priorities.[171]

The NTOP's first transparency report, *Transparency Blueprint: Snapshot of Operational Technologies* (RCMP Transparency Blueprint), was released in September 2024.[172] In contrast to the Toronto Police Service Board's AI Policy, discussed below, the RCMP Transparency Report is a public report rather than a detailed operation policy.

The RCMP Transparency Blueprint outlines how the institution is implementing a more proactive approach to establishing technology assessment and transparency to better achieve responsible use of technology including AI. NTOP's "Responsible use of operational technologies – key principles" include

- Accountability
- Transparency
- Privacy
- Specificity
- Accuracy
- Training
- Impact
- Limitations
- Security
- Evaluation.[173]

The RCMP Transparency Blueprint describes how NTOP conducts evaluations and assessments of operational technologies before procurement and may evaluate existing technologies. This process involves an in-depth review of the technology including its intended use, effectiveness, and compatibility with existing systems and policies, as well as *Charter* and *Privacy Act* compliance. NTOP also states that it is committed to consult with third party vendors to determine how personal information is collected, used, and disclosed, and how the technology is intended to function.[174] The RCMP Transparency Blueprint states that NTOP has evaluated 28 technologies as of September 2024.[175]

7.2.4 Assessing Federal Initiatives to Promote Trustworthy Criminal AI

The LCO believes the federal government should be complemented for many of AI governance initiatives, particularly the Federal Directive and AIA. The RCMP's NTOP program is also commendable.

The Federal Directive and AIA were, and remain, leading examples of how to ensure procedure fairness in public sector AI systems. The current review of the Directive and AIA could make these instruments even stronger.

If passed, a revised *AIDA* would have included limited provisions to promote trustworthy AI in Canada. The addition of prescribed "high-impact" AI systems in biometrics, courts, and policing would have been helpful additions to the legislation. Other positive aspects of *AIDA* included publication and plain language notice requirements, mandatory bias and mitigation requirements, and notable penalties for non-compliance.

Even if *AIDA* had been passed, it would have not establish trustworthy criminal AI in federal law enforcement or the criminal justice system. Some of our concerns would be addressed if the Federal Directive and AIA applied to criminal AI systems, but it does not.

The federal government's inaction in this area is disappointing. It has also been approximately five years since the enactment of the first Federal ADM Directive, yet there is still no dedicated federal legislation, Directive, or policy establishing trustworthy criminal AI across the full range of federal criminal

justice system actors or law enforcement agencies. The lack of federal government action in this area contrasts unfavourably with the EU and US, both of which have taken important steps to address the unique and serious risks of criminal AI systems.

The notable exception to this broad assessment of federal criminal AI governance is the RCMP's NTOP program. This program and the recent RCMP Transparency Blueprint are sophisticated initiatives that incorporate many of the trustworthy criminal AI principles discussed in this report. The RCMP Transparency Blueprint includes important details about how the RCMP assesses technology and its potential use within the RCMP. However, neither NTOP nor the RCMP Transparency Blueprint appear to include detailed information on prohibited uses, risk categories or mitigation requirements. The LCO hopes these issues will be addressed in future RCMP policies.

7.3 Ontario AI Legislation, Government Directives, and Law Enforcement

7.3.1 *EDSTA* and Ontario's Responsible Use of AI Directive

The Government of Ontario has taken two important steps to establishing trustworthy AI in Ontario's public sector. First, the provincial government introduced Bill 194, the *Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024*, in May 2024. The Bill was subsequently passed as the *Enhancing Digital Security and Trust Act, 2024 (EDSTA)* in November 2024.[176] The province then adopted a *Responsible Use of Artificial Intelligence Directive* in December 2024.[177] Both documents are discussed below.

The provincial government stated that the purpose of Bill 194 was to "…[s]et a definition of artificial intelligence (AI) to create consistency across the public sector and establish protections to ensure responsible use of AI systems."[178]

The LCO has written at length about Bill 194 and *EDSTA*. We have concluded that the legislation fails to establish a comprehensive trustworthy AI framework for public sector AI systems in Ontario:

> *The LCO believes Bill 194 must incorporate [trustworthy AI] benchmarks if it hopes to regulate public sector AI systems effectively. Unfortunately, as currently drafted, Bill 194 falls short of this ideal. Most critically, the Bill is brief and lacks key provisions needed to ensure public sector AI use is beneficial, lawful, and accountable. More specifically, the Bill does not address several widely acknowledged Trustworthy AI priorities, including:*
>
> - *Human rights and procedural fairness.*
> - *AI systems used in the criminal justice system.*
> - *AI systems used in courts and tribunals.*
> - *Public AI registries.*
> - *Risk categories and mitigation strategies.*
> - *Impact assessments.*
> - *Explainability requirements.*
> - *Governance.*
>
> *Bill 194 does not include provisions addressing human rights, civil liberties, non-discrimination, equality, or fairness. Nor does Bill 194 include provisions requiring explanations or guaranteeing a process to challenge decisions.*[179]

Most importantly for this report, however, is that *EDSTA* does not apply to AI systems used in Ontario's criminal justice system, including AI systems used in policing or by courts.[180] As a result, *EDSTA* does not establish a framework for trustworthy criminal AI in Ontario.

The provincial government followed up *EDSTA* quickly with its "Responsible Use of Artificial Intelligence Directive" ("the Ontario AI Directive"), which became effective December 1, 2024.[181]

The Ontario AI Directive is more comprehensive than *EDSTA* and addresses several of the LCO's ongoing concerns about provincial AI policy.

The purpose of the Ontario AI Directive is to "set out the requirements for the transparent, responsible and accountable use of Artificial Intelligence".[182]

The Ontario AI Directive also appears to:

- Have broad application.[183]
- Identify AI governing principles.[184]
- Include AI risk management requirements.[185]
- Include disclosure and transparency obligations.[186]
- Establish an AI accountability structure within the provincial government.[187]

Notwithstanding these strengths, the LCO's early analysis is that the the Ontario AI Directive also has several significant gaps or uncertainties. For example, the Ontario AI Directive:

- Does not apply explicitly to provincial law enforcement agencies or any other provincial police service.[188] Ministries may be exempt from the Directive.[189]
- Does not include several trustworthy AI elements identified by the LCO in our reports.[190]
- Does not establish consistent or transparent AI risk criteria or prohibitions.[191]
- Does not establish consistent and comprehensive disclosure obligations.[192]
- Does not establish a remedial regime and lacks access to justice provisions.[193]

Finally, it is not yet clear how the Ontario AI Directive relates to the regulatory powers established in *EDSTA*.[194]

From the LCO's perspective, the Ontario AI Directive is clearly a step forward in establishing trustworthy AI in the provincial government and provincial agencies. That said, there are many outstanding questions regarding its application generally and to criminal AI systems specifically.

7.3.2 Toronto Police Service Board "Use of AI Technology Policy"

The most significant law enforcement AI policy in Canada is the Toronto Police Services Board's (TPSB) "Use of AI Technology Policy." ("TPS AI Policy").[195] The TPS Board introduced the "Use of AI Policy" in February 2022 following a public consultation process. The LCO participated in this process and made extensive submissions, many of which appear to have been adopted.[196] At the time of writing, the TPS AI Policy appears to be one of a small handful of municipal law AI enforcement policies in Canada.

The TPS AI Policy is a sophisticated document that incorporates many trustworthy criminal AI principles.

The TPS AI Policy acknowledges that advances in technology can pose new concerns for "privacy, rights, (including the rights to freedom of expression, freedoms of association, and freedom of assembly, dignity and equality of the individuals affected by [AI applications].[197]

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

1. Legality: All technology used, and all use of technology, must comply with applicable law, including the *Police Services Act* (and its regulations, as well as successor legislation), Ontario's *Human Rights Code*, and the *Charter of Rights and Freedoms*, and be compatible with applicable due process and accountability obligations.
2. Fairness: Use of AI technology must not result in the increase or perpetuation of bias in policing and should diminish such biases that exist.
3. Reliability: AI technology must result in consistent outputs or recommendations and behave in a repeatable manner.

4. Justifiability: The use of AI technology must be shown to further the purpose of law enforcement in a manner that outweighs identified risks.
5. Personal Accountability: Service Members are accountable, through existing professional standards processes, for all the decisions they make, including those made with the assistance of AI technology or other algorithmic technologies.
6. Organizational Accountability: All use of AI technology must be auditable and transparent, and be governed by a clear governance framework.
7. Transparency: Where the Service uses AI technology that may have an impact on decisions that affect members of the public, the use of that technology must be made public to the greatest degree possible. Where full transparency may unduly endanger the efficacy of investigative techniques or operations, the Service will endeavour to make publicly available as much information about the AI technology as possible, to assure the public of the reliability of the AI technology and the justifiability of its use. Where a decision assisted by AI technology may lead to the laying of criminal or other charges against an individual, the possible influence of the AI technology must be included in the disclosure provided to the Crown.
8. Privacy: Use of AI technology must, to the greatest degree practicable, preserve the privacy of the individuals whose information it collects in line with 'privacy by design' principles.
9. Meaningful Engagement: The adoption of specific AI technologies must be preceded by meaningful public engagement commensurate with the risks posed by the technology contemplated.[198]

Significantly, the TPS AI Policy includes explicit risk criteria, including "Extreme Risk Technologies which may not be considered for adoption." [199] This category includes several of the highest risk technologies discussed in this report, including:

- Any application where there is no "human-in-the-loop."
- Where the AI system results in "mass surveillance defined as monitoring of a population or a significant component of a population…"
- "Any application that is known or likely to cause harm or have an impact on individual's rights, despite use of mitigation techniques, due to bias or other flaws."

The complete list TPS AI Policy risk categories are set out in the text box on the following pages.

The TPS AI Policy also includes:

- A broad definition of AI technology as "... any goods or services whose procurement, deployment or use require that a privacy impact assessment be conducted in advance of its deployment or use."[200]
- Obligations to identify the operational need the technology is intended to address and how it will improve operations.
- Data requirements, including obligations to Identify the source of training data; identify how data will be collected and retained; and identify accuracy, validity, and security requirements.
- Detailed disclosure requirements.[201]
- Risk mitigation, audit, and ongoing evaluation requirements.[202]
- Detailed approval and reporting procedures, including the need for privacy assessments and "an analysis of possible unintended consequences of the proposed use of the AI technology from legal and human rights perspectives…"[203]
- Requirements to develop public engagement strategies "commensurate with the risk level assigned to the new AI technology, to transparently inform the public of the use of the new AI technology", and a process by which the public can bring their concerns to the Toronto Police Services Board.[204]
- Establishes a process by which Service Members can use new AI technologies, depending on their perceived "risk category".[205]

The TPS has already made its first public disclosure under the new policy. In January 2024, a TPSB report disclosed the use of five AI-enabled systems by the TPS. The TPS also self-assessed the level of risk each technology poses. One system was classified as "high-risk:" an AI-enabled facial recognition system that automates mugshot identification. Four other AI-enabled technologies were classified as "low-risk," including:

- An automated fingerprint identification system
- Two automated license plate recognition systems.
- A video-based object recognition system capable of identifying and differentiating between uniformed people, vehicle make and model, and other "unique object classes" as defined by the system user.[206]

7.3.3 Durham Regional Police Use of Artificial Intelligence Policy

At least one other police service in Ontario has adopted an AI policy. In October 2024, the Durham Regional Police Services Board adopted its "Use of Artificial Intelligence" Policy (Durham Police AI Policy).[207]

The Durham Police AI Policy includes many of the trustworthy criminal AI principles discussed in this Introduction. The Durham Regional Police Service is much smaller than the Toronto Police Service. As a result, it is understandable that the Durham Police AI Policy is less detailed and proscriptive than the TPS AI Policy. Nonetheless, there are some significant differences. For example, unlike the TPS AI Policy, the Durham Police AI Policy does not include risk categories or prohibited "Extreme Risk Technologies." Rather, the policy includes a general statement that "AI technologies that pose a serious risk of harm or bias against any particular community, group, or individual or the privacy of citizens will not be procured or used."[208] Nor does the Durham Police AI Policy include detailed mitigation requirements or reporting requirements.

7.3.4 Assessing Provincial Initiatives to Promote Trustworthy Criminal AI

There are three significant trustworthy AI laws or policies in Ontario: *EDSTA*, the Ontario AI Directive, and the TPS AI Policy.

Like the federal government, the provincial government's commitment to AI governance has not extended to AI systems used in provincial law enforcement or the provincial criminal justice system. As a result, there is simply no dedicated legislation, Directive, or policy establishing trustworthy criminal AI in Ontario:

As discussed above, *EDSTA* does not establish a comprehensive trustworthy AI framework for provincial public sector AI systems generally or the criminal justice system specifically.

The Ontario AI Directive is more comprehensive than *EDSTA* and addresses several of the LCO's ongoing concerns about provincial AI policy, but there are many outstanding questions. For the purpose of this report, the Ontario AI Directive's most salient feature is that it does not create a trustworthy criminal AI framework in Ontario.

The most significant criminal justice AI policy in Ontario is TPS AI Policy. As discussed above, the TPS AI Policy is a sophisticated and comprehensive document that incorporates many criminal trustworthy AI principles identified by the LCO and other jurisdictions. The LCO commends the Toronto Police Services Board and Toronto Police Service for its work in this complex area.

For all its strengths, however, the TPS AI Policy has important limitations as a trustworthy criminal AI governance instrument:

First, the TPS AI Policy is not legally binding. The TPS AI Policy does not create enforceable rights or include remedial provisions or penalty provisions for non-compliance. As a result, the TPS AI Policy does not create a legal accountability regime.

Second, the TPS AI Policy is self-regulating. It does not create an independent oversight body or any external review mechanism. Self-regulation can lead to criticisms that the policy will be interpreted loosely. Indeed, the TPS recently attracted criticism of the Ontario Human Rights Commission and the Information and Privacy Commissioner of Ontario for categorizing their use of certain AI technologies – including automated license plate readers and fingerprint identification – as "low risk technologies" with fewer assessment and oversight requirements. This is despite candid acknowledgement by the Toronto Police Service that such technologies "could be used to assist in the identification of individuals for the purpose of their arrest, detention or questioning."[209]

Third, and most significantly, the TPS AI Policy is an administrative policy governing one police service in Ontario. In other words, the TPS AI Policy does not establish a provincial AI standard for either policing generally or any other part of Ontario's justice system.

The TPS AI Policy demonstrates the difficulty and risks of relying on individual police services and boards to regulate policing AI systems. There are 53 police services in Ontario. To date, the Toronto and Durham Police Services appear to be the only two provincial police services that have adopted dedicated AI policies. This means that 51 police services in Ontario *are not* subject to AI prohibitions, risk criteria, disclosure and consultation requirements, etc. In other words, one or more of the 51 remaining police services in Ontario could adopt "Extreme Risk" AI systems (such as real time FRT or predictive policing) without any disclosure, guardrails, or accountability requirements. This a worst-case scenario, but not an impossible one. Even where police services do adopt AI policies, there can be significant differences, as demonstrated by the contrast between the TPS and Durham Policy AI Policies.

Moreover, police services are not the only criminal justice institution or actor in Ontario likely to be affected by AI systems. Others include the Ministries of Solicitor General and Attorney General, courts, Crowns, the defence bar, Legal Aid Ontario, and others. As of April 2025, there are no dedicated criminal AI laws or rules governing to use or interpretation of criminal AI systems by these organizations.

Absent provincial action, these institutions will have to develop their own AI policies, which may or may not conform with existing legal rules, protect rights, or incorporate trustworthy criminal AI principles. Experience demonstrates that patchwork or sliding-scale policing AI rules may put residents in some areas of the province at greater risk of AI discrimination, false arrest, privacy violations, and more.

Toronto Police Services Board AI Policy Risk Categories

Extreme Risk Technologies, which may not be considered for adoption, including:

- Any application where there is no qualified "human-in-the-loop".
- Where use of the application results in mass surveillance defined as the monitoring of a population or a significant component of a population, or the analysis of indiscriminately collected data on a population or a significant component of a population.
- Any application of AI in a life-safety situation, i.e., an application where the action of the AI technology could slow down the reaction time of the human operator, resulting in potential risk to life of members of the public or Service Members.
- Any application that is known or is likely to cause harm or have an impact on an individual's rights, despite the use of mitigation techniques, due to bias or other flaws.
- Any application used to predict or assign likelihood of an individual or group of individuals to offend or reoffend.
- Any application making use of data collected in accordance with the Board's *Regulated Interaction with the Community and the Collection of Identifying Information* Policy, or any Historical Contact Data as defined in that Policy; or,
- Where training or transactional data is known or thought to be illegally sourced, or where it is from an unknown source.

High Risk Technologies, including:

- Where training or transactional data is known or thought to be of poor quality, carry bias, or where the quality of such data is unknown;
- Where training data can be influenced or biased by malicious actors;
- Applications which link biometrics to personal information (e.g. facial recognition);
- Where the proposed system could be used to assist in the identification of individuals for the purpose of their arrest, detention or questioning;
- Where the process involved suggests an allocation of policing resources;
- Where a system that otherwise merits a Moderate risk assessment lacks independent validation; or,
- Where a system cannot be fully explainable in its behaviour;

Moderate Risk Technologies, including where the "human-in-the-loop" may have difficulty identifying bias or other decision failures of the AI or where training data is based on existing Service data.

Low Risk Technologies, including any AI technology that both does not fall under the categories of Extreme High Risk, High Risk, or Moderate Risk, and assists Members in identifying, categorizing, prioritizing or otherwise making administrative decisions pertaining to members of the public; and,

Minimal Risk Technologies, including any AI technology that does not fall under any of the preceding categories.

7.4 Guidance From Canadian Privacy Commissioners and Courts

A final source of criminal trustworthy AI rules and policies is emerging from Canadian privacy commissioners and courts.

Canadian Privacy Commissioners have taken a prominent and important leadership role in promoting trustworthy criminal AI in Canada. To date, Privacy Commissioners have completed at least five investigations, reports or guidance documents on FRT in Canadian policing:

- A Joint Investigation of Clearview AI by the Privacy Commissioners of Canada, Quebec, British Columbia and Alberta (February 2021).[210]
- An Office of the Privacy Commissioner of Canada report on the use of FRT by the RCMP, *Police use of Facial Recognition Technology in Canada and the Way Forward* (June 2021).)[211]
- A joint statement by the Privacy Commissioners of Canada on police FRT (May 2022).[212]
- Two Guidances from the Information and Privacy Commissioner of Ontario addressing mugshot databases and automatic license plate readers.[213]

These reports include sophisticated evaluations and recommendations regarding how police services can and should use FRT technology. Each report is discussed in more detail in our *AI and Law Enforcement* Issue Paper. The LCO expects these organizations will continue addressing criminal justice AI issues in the future.

In addition to the Privacy Commissioner's Guidance, several courts in Canada have adopted AI policies. For example, the Federal Court has adopted policies to guide the use of AI by the court and to direct the use of AI by parties and professionals appearing before the court.[214] Courts in other provinces have adopted similar AI policies including Alberta, Manitoba, and Quebec.[215]

The Federal Court's December 2023 *Interim Principles and Guidelines on the Court's Use of Artificial Intelligence* are an interesting and important statement of intent regarding that court's potential use of AI systems.[216] The Interim Principles state that

> *The following principles will guide the potential use of AI by members of the Court and their law clerks:*

- ***Accountability:*** *The Court will be fully accountable to the public for any potential use of AI in its decision-making function;*
- ***Respect of fundamental rights:*** *The Court will ensure its uses of AI do not undermine judicial independence, access to justice, or fundamental rights, such as the right to a fair hearing before an impartial decision-maker;*
- ***Non-discrimination:*** *The Court will ensure that its use of AI does not reproduce or aggravate discrimination;*
- ***Accuracy:*** *For any processing of judicial decisions and data for purely administrative purposes, the Court will use certified or verified sources and data;*
- ***Transparency:*** *The Court will authorize external audits of any AI-assisted data processing methods that it embraces;*
- ***Cybersecurity:*** *The Court will store and manage its data in a secure technological environment that protects the confidentiality, privacy, provenance, and purpose of the data managed; and,*
- ***"Human in the loop":*** *The Court will ensure that members of the Court and their law clerks are aware of the need to verify the results of any AI-generated outputs that they may be inclined to use in their work.*

For the potential use of AI by members of the Court and their law clerks, the Court will adhere to the following guidelines:

1. *The Court will not use AI, and more specifically automated decision-making tools, in making its judgments and orders, without first engaging in public consultation. For greater certainty, this includes the Court's determination of the issues raised by the parties, as reflected in its Reasons for Judgment and its Reasons for Order, or any other decision made by the Court in a proceeding…*

The Canadian Judicial Council subsequently produced a thoughtful set of *Guidelines for the Use of Artificial Intelligence in Canadian Courts* in October 2024.[217] These guidelines emphasized that the use of AI in Canadian courts "must firmly uphold the fundamental principle of judicial independence, encompassing its individual and institutional dimensions."[218] The Guidelines also noted the complexity and uniqueness of AI use by Canadian courts, including but not limited to the need for stringent information security requirements and to ensure explainability.[219]

Guidance from Privacy Commissioners and courts are important efforts to establish trustworthy AI principles in their respective domains. They do not, however, establish comprehensive accountability for criminal AI systems either nationally or provincially. In a properly structured regulatory system, the IPC and court guidance would supplement legislative requirements, not substitute for them.

7.5 Conclusion: Assessing Trustworthy Criminal AI in Canada

There have been many positive developments in AI governance at the federal level and in Ontario. Both governments have taken important steps to establish "trustworthy AI" in the federal and provincial public sectors. Privacy Commissioners and the Toronto Police Service have also taken important steps to address criminal AI risks. Unfortunately, there are still wide and consequential gaps in the legislative or legal framework governing criminal AI systems in Canada.

Federal Government

The federal government's proposed amendments to *AIDA* would have advanced limited aspects of trustworthy criminal AI at the federal level. These amendments were necessary but did not explicitly govern federal law enforcement agencies or the criminal justice systems.

The federal ADM Directive and AIA are notable efforts to govern AI systems in the federal government. Potential revisions to these policies could include more detailed risk criteria and provisions banning prohibited AI systems. That said, the federal ADM or AIA are still not applicable to federal law enforcement or criminal justice.

The RCMP has taken important steps to adopt trustworthy criminal AI policies. The RCMP's NTOP program, for example, establishes thoughtful rules governing the procurement of AI by the RCMP. Like the TPS AI Policy, however, the NTOP program and other RCMP initiatives have important limitations as an overall governance framework. NTOP and related initiatives lack the specificity, enforcement, and comprehensiveness necessary to address the full range of potential risks and harms of federal criminal AI systems.

Ontario

The Government of Ontario's *EDSTA* establishes a limited framework for the responsible use of artificial intelligence within Ontario's public sector. *EDSTA* does not, however, apply AI systems used in the Ontario's criminal justice system, including policing or courts.

The Ontario AI Directive establishes important and welcome trustworthy AI requirements for many provincial AI systems but there are many gaps and unanswered questions. Most importantly, the Ontario AI Directive does not explicitly apply to provincial law enforcement agencies or any other AI system used in Ontario's criminal justice system.

The TPS AI Policy is the most significant criminal AI governance policy in Canada to date. The TPS AI Policy was based on public consultation and adopts a comprehensive risk-based evaluation of AI technologies in use or proposed for use by TPS. The TPS AI Policy is commendable, but it has limitations, including its lack of enforcement and lack of applicability to other provincial police services, municipalities, and courts. In a properly structured regulatory system, the TPS AI Policy would supplement legislative requirements, not substitute for them.

International Trustworthy Criminal AI

Federal and provincial legislative efforts stand in contrast with the sophistication, substance, and form of criminal justice AI governance in Europe and the United States. For example, the EU *AI Act* identifies AI tools in "law enforcement" and the "administration of justice" as being presumptively high-risk and thus subject to more detailed regulatory requirements. In the United States, detailed criminal justice AI legislation, executive orders, policies, and rules have been adopted by the federal government and many states and municipalities.

The form and substance of these regimes differ between jurisdictions. The overarching theme, however, is that consistent and comprehensive regulation is needed to establish trustworthy criminal AI. In comparison to Canada, our peer jurisdictions have enacted or proposed complex frameworks governing:

- Mandatory disclosure of criminal AI systems, including public "AI registers".
- Prohibitions on highest risk criminal AI systems
- Criteria to identify prohibited or high-risk systems.
- Purpose and use limitations.
- Mandatory and transparent AI impact assessments.
- Mitigation requirements.
- Mandatory obligations to measure, correct and audit bias.
- Procedural protections, such as warrant requirements for high-risk systems.
- Mandatory "human in the loop" requirements and training.
- Mandatory auditing and evaluation requirements.
- Independent oversight of individual systems and government AI generally.

Notable Gaps in Trustworthy Criminal AI in Canada

Gaps in the federal and provincial trustworthy criminal AI framework appear to include:

- **Lack of mandatory and consistent disclosure requirements.** At present, the overwhelming majority of police services in Ontario could implement predictive policing, FRT, or other forms of AI without having to disclose those systems publicly.
- **Lack of criminal AI prohibitions, "guardrails", or consistent risk criteria.** In Ontario, there are no legal "guardrails" prohibiting or regulating the highest risks criminal AI systems, such as real time mass surveillance and predictive policing. Nor are there transparent and consistent risk categories to consistently identify criminal AI risks and mitigation strategies.

- **Lack of mandatory impact assessments.** There is no provincial obligation for any actor in the criminal justice system to assess the impact of an AI system on *Charter* rights, human rights, privacy, or procedural justice.
- **Lack of criminal procedural protections.** In Canada (and by extension, Ontario), there are no explicit procedural protections governing police or court use of high-risk criminal AI systems. Unlike other jurisdictions, there are no warrant requirements for high-risk AI systems or explicit rules that AI system-generated evidence alone cannot be used to justify charges, etc.
- **Lack of mandatory obligation to test, audit, or evaluate criminal AI systems.** An AI system could be implemented in Ontario's criminal justice system without a legal to duty to audit or evaluate its accuracy, bias, or effectiveness.
- **Lack of obligation to undertake public consultations.** Unlike other jurisdictions, there is no obligation in Ontario to consult publicly on complex, controversial, and consequential AI systems in criminal justice.

The LCO acknowledges that these are comparatively early days for AI regulation in Canada and Ontario. The Canada ADM Directive and AIA, *EDSTA*, the Ontario AI Directive, and the TPS and Durham AI Policies were all adopted within the last few years. Nevertheless, the LCO believes federal and provincial policymakers should proactively address the evident gaps and risks in Ontario's trustworthy criminal AI framework.

The lack of national or provincial trustworthy criminal AI standards is particularly important considering the wide, diverse, and decentralized network of institutions and actors who will be involved in developing, operating, litigating, or overseeing AI in Ontario's criminal justice system. The lack of consistent AI disclosure, bias, or risk assessment requirements will mean that police, governments, counsel, and courts will struggle to determine the appropriate uses and limits of criminal justice AI systems.

What If We Do Not Regulate?

In these circumstances, it is fair to ask what is likely to happen if governments fail to regulate criminal justice AI systems. This is not a hypothetical question. Criminal AI systems have been in use in other jurisdictions for several years. Policymakers thus have a detailed record of well-documented and widely publicized risks and harms, including:

- Risk of false arrest or imprisonment.
- Data bias and discrimination.
- Lack of legal accountability.
- Risks to privacy, human rights, and procedural fairness.
- Inconsistent policing and judicial decision-making.
- Loss of public trust in criminal justice system.
- Risk of compounding existing overrepresentation of low-income, racialized, and Indigenous communities in criminal justice.

Failure to regulate AI in criminal justice could mean that predictive policing, facial recognition surveillance, automated bail and sentencing risk assessments, and a myriad of other AI technologies could be introduced in Ontario without appropriate "guardrails" or accountability requirements. Absent effective regulation, the potential harm to criminal defendants, criminal courts, and public trust in the criminal justice system is foreseeable and significant.

8. Next Steps and Consultations

One of the lessons of this project is that whether AI in criminal justice is harmful or beneficial depends on a complex series of technical, operational, policy, and legal choices. International precedents offer promising lessons and benchmarks for Canadian criminal justice AI legislation and regulation. Much has been learned about how to design, develop, implement and evaluate these systems. These precedents are helpful, but not conclusive for Canadian and provincial policymakers. Any governance framework in Canada must be tailored to our criminal justice system and institutions.

A second important lesson is that broad collaborations and consultations are crucial. Given the issues at stake, no one organization or stakeholder can or should act unilaterally. The LCO is confident that provincial policymakers, police services, judiciary, Crowns, defence counsel, civil society organizations and others are committed to addressing these issues constructively.

Finally, as noted at the start of this paper, unlike other LCO projects neither this Introduction nor the Issue Papers present final or specific law reform recommendations. Accordingly, each Issue Paper concludes with a series of questions for future consideration by Canadian policymakers. A consolidated list of those questions is attached to the Executive Summary of this project and is available on our project website.

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. Written submissions can be sent to the LCO's general email address at LawCommission@lco-cdo.org.

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

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

Endnotes

1 See: Organisation for Economic Co-operation and Development, *Scoping the OECD AI Principles: Deliberations of the Expert Group on Artificial Intelligence at the OECD* (November 2019), at 7, online: https://www.oecd.org/content/dam/oecd/en/publications/reports/2019/11/scoping-the-oecd-ai-principles_71e1b6dc/d62f618a-en.pdf; European Parliament, *Artificial Intelligence Act* (Regulation 2024/1689) (June 13 2024), at Article 3(1), online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202401689.

2 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* (Introduced June 16 2022; Second Reading April 24 2023), at s. 2, online: https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading.

3 Ontario, Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024 (Royal Assent November 25 2024), at s. 1, online: https://www.ola.org/en/legislative-business/bills/parliament-43/session-1/bill-194.

4 These examples are discussed in detail in the Issue Papers.

5 Brandon Epstein, "Navigating the Future of Policing" in Police Chief Magazine [Police Chief Magazine] (April 2024), online: https://www.policechiefmagazine.org/navigating-future-ai-chatgpt/.

6 Europol, *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement* [EUROPOL] (2024), online: https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing.

7 EUROPOL at 8.

8 EUROPOL at 8.

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

10 Ferguson 2019 at 491.

11 Law Commission of Ontario, Use of AI by Law Enforcement (Toronto: April 2025), online: https://www.lco-cdo.org/CrimAI [LCO Police AI Issue Paper]. For a good background on predictive policing, see also Ferguson 2019; National Academies of Sciences, Engineering, and Medicine, *Law Enforcement Use of Predictive Policing Approaches: Proceedings of a Workshop – In Brief* [NAS Predictive Policing] (2024), online: https://nap.nationalacademies.org/catalog/28037/law-enforcement-use-of-predictive-policing-approaches-proceedings-of-a; Tim Lau, Brennan Center for Justice, *Predictive Policing Explained* [Brennan Center Predictive Policing] (2020), online: https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained; and The Citizen Lab, To Surveil and Protect: A Human Rights Analysis of Algorithmic Policing in Canada [To Surveil and Protect] (2020), online: https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf.

12 EUROPOL at 15.

13 To Surveil and Protect at 41.

14 NAS Predictive Policing at 2.

15 To Surveil and Protect at 45-46.

16 NAS Predictive Policing at 4.

17 NAS Predictive Policing at 5.

18 Benjamin Carleton, Brittany Cunningham, and Zoe Thorkildsen, *The Use of Predictive Analytics in Policing* [Bureau Justice Assistance] (2020), online: https://www.cna.org/reports/2020/10/use-of-predictive-analytics at 4-6.

19 Bureau of Justice Assistance at 7-9.

20 See generally, NAS Predictive Policing and Bureau of Justice Assistance for a good description of the history, growth, and developments of predictive policing in the United States.

21 See generally, LCO Police AI Issue Paper and NAS Predictive Policing at 3-4.

22 To Surveil and Protect at 47.

23 NAS Predictive Policing at 1.

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

25 International Criminal Police Organization (INTERPOL), *Introduction to Responsible AI Innovation* (2024) [INTERPOL AI Introduction], online at https://www.interpol.int/en/How-we-work/Innovation/Artificial-Intelligence-Toolkit at 9.

26 INTERPOL AI Introduction at 21.

27 EUROPOL at 24.

28 See generally, EUROPOL at 21-29.

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

30 Privacy Commissioners of Canada, Joint Statement, *Privacy guidance on facial recognition for police agencies* [Privacy Commissioners Joint Police FRT Statement] (May 2022), online: https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/ at paras 6-8.

31 Privacy Commissioners Joint Police FRT Statement at paras 10, 15.

32 For a discussion of the distinction between real time and retrospective FRT systems see International Network of Civil Liberties Organizations, *Eyes on the Watchers: Challenging the Rise of Police Facial Recognition Technology* [INCLO Challenging FRT] (2025), online: https://inclo.net/pillars/surveillance-and-digital-rights/principles-for-use-of-frt/ at 16-17. Many people believe real time FRT use raises the prospect of mass surveillance and privacy violations, increased risk of misidentification of suspects, "police-state" surveillance tracking innocent individuals, and chilling speech/dissent. For a summary of a police view, see EUROPOL at 41 and International Criminal Police Organization (INTERPOL), Responsible AI Principles (2024) [INTERPOL *Responsible AI Principles*] (2024), online: https://www.interpol.int/en/How-we-work/Innovation/Artificial-Intelligence-Toolkit at 15.

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

34 According to the Atlas of Surveillance, an open-source research project of the Electronic Frontier Foundation, there could be as many as 900 locations or applications of FRT in various law enforcements and government agencies across the United States as of October 2023. Online at https://atlasofsurveillance.org/atlas

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

36 Office of the Privacy Commissioner of Canada, Report of findings: *Investigation into the RCMP's collection of personal information from Clearview AI (involving facial recognition technology)* (June 10, 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/ at para. 7.

37 https://www.tps.ca/police-reform/artificial-intelligence/

38 See generally, Abdirahman Osman Hashi et al, "Deep Learning Models for Crime Intention Detection Using Object Detection" in *Intl J Advanced Computer Science and Applications* (2023; Volume 14, No 4), online: https://thesai.org/Downloads/Volume14No4/Paper_34-Deep_Learning_Models_for_Crime_Intention_Detection.pdf at 300; Vishva Payghode et al, "Object Detection and Activity Recognition in Video Surveillance Using Neural Networks" in *International Journal of Web Information Systems* (April 20, 2023; Volume 19, No 3/4) at 123.

39 For an excellent summary of ALPR technology and issues, see Information and Privacy Commissioner of Ontario, *Guidance on the Use of Automated Licence Plate Recognition Systems by Police Services* [IPC ALPR Guidance] (Updated December 2024), online: https://www.ipc.on.ca/en/resources-and-decisions/guidance-use-automated-licence-plate-recognition-systems-police-services.

40 See generally IPC ALPR Guidance. For an industry perspective on the potential uses and benefits of ALPRs, see Scylla AI, *8 Reasons to Use Intelligent Licence Plate Recognition Systems* (accessed March 2025), online: https://www.scylla.ai/8-reasons-to-use-intelligent-license-plate-recognition-systems/.

41 Toronto Police Service, *Automatic License Plate Reader Technology in TPS Vehicles* (accessed March 2025), online: https://www.tps.ca/use-technology/automatic-licence-plate-reader/.

42 Police Chief Magazine.

43 NJI at 7.

44 SoundThinking Inc., *ShotSpotter Frequently Asked Questions* (accessed March 2025), online: https://www.soundthinking.com/faqs/shotspotter-faqs/.

45 Dhruv Mehrotra and Joey Scott, Wired Magazine, *Here Are the Secret Locations of ShotSpotter Gunfire Sensors* (February 22, 2024), online: https://www.wired.com/story/shotspotter-secret-sensor-locations-leak/.

46 See generally, CNN, *Critics of ShotSpotter gunfire detection system says it's ineffective, biased and costly* (February 24, 2024), online: https://www.cnn.com/2024/02/24/us/shotspotter-cities-choose-not-to-use/index.html.

47 CBC, *Toronto Police scrap plans to acquire controversial gun-shot detection system* (February 14, 2019), online: https://www.cbc.ca/news/canada/toronto/toronto-police-scrap-plans-to-acquire-controversial-gunshot-detection-system-1.5019110.

48 Scylla AI, *Enhancing Video Surveillance with AI-Powered Drones* (accessed March 2025), online: https://www.scylla.ai/enhancing-video-surveillance-with-ai-powered-drones/.

49 Royal Canadian Mounted Police, National Technology Onboarding Program, *Transparency Blueprint: Snapshot of Operational Technologies*, [RCMP Transparency Blueprint] (2024), online at https://rcmp.ca/en/corporate-information/publications-and-manuals/national-technology-onboarding-program-transparency-blueprint at 15.

50 RCMP Transparency Blueprint at 16.

51 Jay Stanley, American Civil Liberties Union, *Eye-in-the-Sky Policing Needs Stricter Limits* (July 26, 2023), online: https://www.aclu.org/documents/eye-in-the-sky-policing-needs-strict-limits at 1.

52 Law Commission of Ontario, *The Rise and Fall of Algorithms in American Criminal Justice: Lessons for Canada* [LCO American Lessons] (2020), online: https://www.lco-cdo.org/wp-content/uploads/2020/10/Criminal-AI-Paper-Final-Oct-28-2020.pdf.

53 See generally, LCO American Lessons.

54 John Logan Koepke and David G. Robinson, *Danger Ahead: Risk Assessment and the Future of Bail Reform* (2018) online: https://ssrn.com/abstract=3041622 at 1746.

55 The Champion, *Making Sense of Risk Assessments,* American National Association of Criminal Defense Lawyers, [The Champion] (2018), online: https://www.nacdl.org/Article/June2018-MakingSenseofPretrialRiskAsses.

56 Sarah Picard-Fritshe et al, Center on Court Innovation, *Beyond the Algorithm: Pretrial Reform, Risk Assessment, and Racial Fairness* (2019), online: https://www.courtinnovation.org/sites/default/files/media/document/2019/Beyond_The_Algorithm.pdf at 3.

57 AI-powered open-source intelligence (OSINT) and social media intelligence (SOCINT) allows police services to survey and process vast amounts of publicly available information to support investigations by "[providing] valuable insights into criminal activities, potential threats, and even the whereabouts of suspects." Police Chief Magazine. According to EUROPOL,
…the applications of an automated OSINT paradigm are limitless. Automated OSINT tools provide insights that strengthen early-stage investigations, helping investigators shift from merely reacting to actively preventing..these tools can reformat unstructured data, support targeted open-source searches and investigations, and offer real-time insights. EUROPOL at 17.

58 These issues are discussed in the fourth LCO Criminal AI Issue Paper, *AI at Trial and On Appeal*, and in Jesse Beatson, Gerald Chan, and Jill Presser, *Litigating Artificial Intelligence,* (2021).

59 Dispatch call centres in the US have begun using AI-powered systems for several purposes, including triaging low-priority or duplicate non-emergency calls. See generally, National Telecommunications and Information Administration, *Improving 9-1-1 Operations with Artificial Intelligence* (2024), online: https://www.ntia.gov/category/next-generation-911/improving-911-operations-with-artificial-intelligence.

60 According to Police Chief Magazine,
AI is being used by police services to "facilitate "real-time" crime analysis by continuously monitoring various data sources for suspicion activity. Real time crime analysis is said to allow law enforcement to respond swiftly to emerging threats and prevent crime before they occur. Real time crime analysis can integrate data from surveillance cameras, sensors (such as gunshot monitors0, licence plate readers, and other sources "to create a comprehensive and dynamic situational awareness.
See also Police 1, *An introduction to how AI is transforming real time crime centers* (2024), online: https://www.police1.com/tech-pulse/an-introduction-to-how-ai-is-transforming-real-time-crime-centers and iAcuty, *Speed vs Scrutiny: How AI is Revolutionizing Crime Analysis,* (2024), online: https://www.iacuityfintech.com/speed-vs-scrutiny-how-ai-is-revolutionizing-crime-analysis/.

61 Future Policing Institute, *The Impact Of Large Language Models on Police Report Writing and Beyond* (2024), online: https://www.futurepolicing.org/using-ai/the-impact-of-large-language-models-on-police-report-writing-and-beyond.

62 Future Policing Institute, *AI and Post-Conviction Review* (2024), online: https://www.futurepolicing.org/using-ai/ai-and-post-conviction-review-how-police-departments-can-restore-confidence.

63 According to EUROPOL,
Central to the advances in digital forensics is the role of AI in modern digital investigations. AI provides an advanced capability to sift through vast data repositories, automating processes that would traditionally take human experts extensive periods. For instance, while a human investigator might manually sort through thousands of files, AI can rapidly categorise, filter, and highlight relevan information based on predefined criteria or patterns. [Footnotes omitted.] EUROPOL at 20.

64 EUROPOL at 28-29.

65 In some US states, AI-powered legal services are currently available to help people expunge their criminal records, for example by using generative AI to draft personal statements. See Matt Reynolds, "Locked in: Criminal Justice Startups Tap into Generative AI's Early Promise," *ABA Journal* (2024), online: <https://www.abajournal.com/legalrebels/article/locked-in-criminal-justice-startups-tap-into-generative-ais-early-promise.

66 See LCO Police AI Issue Paper.

67 According to news reports, researchers are reported to be using AI to scrutinize police body-camera footage to analyze "the tone and word choice of officers in order to determine the frequency of unnecessary escalations and use the findings to improve training and promote accountability." Libor Jany, "LAPD to use AI to analyze body cam videos for officers' language use", *Los Angeles Times* (August 22, 2023), online: https://www.latimes.com/california/story/2023-08-22/lapd-to-use-ai-to-analyze-body-cam-videos-for-officers-language-use.

68 A new class of AI-powered research tools like Harvey.ai train large language models on legal-specific data, creating generative AI that aims to produce more detailed and specific legal analysis, summaries, and text. See generally, Harvey AI at https://www.harvey.ai. See also Law Society of Ontario, *Licensee use of generative artificial intelligence (White Paper)* (2024), online: https://lso.ca/lawyers/technology-resource-centre/practice-resources-and-supports/using-technology.

69 See for instance, Reuters, "Convicted Fugees rapper Pras Michel's lawyer used AI to draft bungled closing argument" (October 18, 2023), online: https://www.nbcnews.com/news/us-news/convicted-fugees-rapper-pras-michels-lawyer-used-ai-draft-bungled-clos-rcna120992. See also New York Times, "Michael Cohen Used Artificial Intelligence in Feeding Lawyer Bogus Cases" (December 29 2023), online: https://www.nytimes.com/2023/12/29/nyregion/michael-cohen-ai-fake-cases.html.

70 Kari Paul, "Microsoft releases AI tool for photorealistic copying of faces and voices", *The Guardian* (November 17, 2023), online: https://www.theguardian.com/technology/2023/nov/17/microsoft-azure-ai-video-deepfakes?CMP=Share_iOSApp_Other.

71 Some have proposed a role for AI in more accurately assessing testimony or submissions. Phys.org, "How AI tools can help assess verbal eyewitness statements" (March 2024), online: https://phys.org/news/2024-03-ai-tools-eyewitness-statements.html) reporting on Leigh, Lyman, and Heaton, "Assessing Verbal Eyewitness Confidence Statements Using Natural Language Processing" (Psychological Science March 2024), online: https://doi.org/10.1177/09567976241229028.

72 Numerous commentators have recognized that AI may speed up the processes of legal research, analysis, and drafting. Theoretically, this will allow lawyers to work faster and thus offer legal services more cheaply. It is worth noting, however, that some critics have suggested that the expansion of AI into the legal profession is in fact worsening the access to justice gap, since it provides disproportionate advantages to already well-resourced firms and litigants.

73 Many of the same AI applications that could make lawyers' work more efficient may also enable non-lawyers to pursue justice themselves. AI could help self-represented litigants draft submissions using legal terminology, understand their likelihood of success in court, identify and fill out necessary forms, and translate information between languages. See Irene Galea, "AI Might Soon Help People Who Represent Themselves in Court, Despite Ethical Concerns," *The Globe and Mail* (7 August 2023), online: <https://www.theglobeandmail.com/business/article-ai-could-help-people-represent-themselves-in-court-experts-warn-of/>; Stephen Joyce, "Illinois Task Force Explores How AI Could Speed Up Litigation," *Bloomberg Law* (13 March 2024), online: <https://news.bloomberglaw.com/artificial-intelligence/illinois-task-force-explores-how-ai-could-speed-up-litigation>.

74 AI has helped researchers efficiently analyze large amounts of criminal justice data. Some particularly promising applications use LLMs to automatically analyze lengthy texts such as survey responses or police reports.

75 Law Commission of Ontario, *Accountable AI*, (2022) [Accountable AI], online: https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/regulating-ai-critical-issues-and-choices/; Law Commission of Ontario, *Regulating AI: Critical Issues and Choices* [Regulating AI] (2021), online: https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/ and LCO American Lessons.

76 LCO American Lessons at 35-37.

77 The LCO and Ontario Human Rights Commission have recently developed the first AI human rights impact assessment (HRIA) based on Canadian law. The LCO/OHRC HRIA and an accompanying background paper is online at https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/human-rights-ai-impact-assessment/.

78 For an extensive discussion of the AI data bias and issues, see LCO American Lessons at 20-26.

79 INCLO Challenging FRT at 25. The best-known FRT bias study is a 2019 report by the National Institute of Standards and Technology study which found that "[t]he majority of commercial facial-recognition systems exhibit bias" and "falsely identified African-American and Asian faces 10 to 100 times more than Caucasian faces." National Institute of Standards and Technology (NIST), *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* [NIST FRT](2019), online: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf at 3. NIST also identified concerns regarding false negatives false positives, gender, and age.

80 INCLO Challenging FRT at 25.

81 See, for example, Policing Project, New York University School of Law, *Law Enforcement Use of Facial Recognition Technology Must Be Regulated Now. Here's How* [Policing Project FRT Regulation] (accessed March 2025), online: https://www.policingproject.org/regulating-police-use-of-face-recognition-technology at 1-2; Surveillance Technology Oversight Project (STOP), *Seeing Is Misbelieving: How Surveillance Technology Distorts Crime Statistics* (June 2024), online: https://www.stopspying.org/seeing-is-misbelieving; and INCLO Challenging FRT.

82 See, for example, American Civil Liberties Union, *When It Comes to Facial Recognition, There is No Such Thing as a Magic Number*, (February 7, 2024), online: https://www.aclu.org/news/privacy-technology/when-it-comes-to-facial-recognition-there-is-no-such-thing-as-a-magic-number. See also, Electronic Frontier Foundation, *Cities Should Act NOW to Ban Predictive Policing* (2023), online: https://www.eff.org/deeplinks/2023/10/cities-should-act-now-ban-predictive-policingand-stop-using-shotspotter-too.

83 For example, many trustworthy AI frameworks developed by police agencies include extensive guidance on data accuracy and the need for "rigorous and scientific testing" including the accuracy of FRT systems. INTERPOL Responsible AI Principles at 12 and 13.

84 The National Academy of Sciences report cited above includes an extensive discussion of predictive policing and bias. NAS Predictive Policing at 2: "…in practice, predictive algorithms have fueled hot spots policing that too often results in the over-policing of communities and residents, imposing biases that have detrimental impacts on people of color."

85 Ontario Human Rights Commission, *Policy on Eliminating Racial Profiling in Law Enforcement* [OHRC Eliminating Racial Profiling] (2019), online: https://www.ohrc.on.ca/en/policy-eliminating-racial-profiling-law-enforcement at s. 4.2.6.1.

86 OHRC Eliminating Racial Profiling at s. 4.2.6.1.

87 OHRC Eliminating Racial Profiling at s. 4.2.6.2.

88 OHRC Eliminating Racial Profiling at s. 4.2.6.2.

89 See, for example, NAS Predictive Policing; NAACP, *Artificial Intelligence in Predictive Policing Issue Brief* (accessed March 2025), online: https://naacp.org/resources/artificial-intelligence-predictive-policing-issue-brief; and Grace Thomas, *Politicians Move to Limit Predictive Policing After Years of Controversial Failures* (October 15, 2024), online: https://www.techpolicy.press/politicians-move-to-limit-predictive-policing-after-years-of-controversial-failures/.

90 INCLO Challenging FRT at 22.

91 OPC Way Forward.

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

93 Brennan Center for Justice, New York University School of Law, *New York City Police Department Surveillance Technology* (2019), online: https://www.brennancenter.org/our-work/research-reports/new-york-city-police-department-surveillance-technology.

94 For example, the IPC Mugshot Guidance report sets out detailed guidance addressing preimplementation issues, operational considerations, and program review and evaluation. IPC Mugshot Guidance at 4-33.

95 See the LCO's American Lessons report for a good summary of these issues. See also INTERPOL's "Transparency Principles" in INTERPOL, *A Policy Framework for Responsible Limits on Facial Recognition* [INTERPOL Policy Framwork] (2021), online: https://unicri.org/A-Policy-Framework%20-for-Responsible-Limits-on-Facial-Recognition at 15-16.

96 Transparency and disclosure in the context of criminal prosecutions are discussed extensively in all four Criminal AI Issue Papers. See specific papers for an analysis of these issues in the context of police investigations, bail, at trial, etc.

97 AI disclosure and transparency issues are discussed extensively in the LCO Criminal AI project papers.

98 "Toronto Police admit using secretive facial recognition technology Clearview AI," *CBC*, February 13 2020; Gillis, W., Allen, K., "Peel and Halton police reveal they too used controversial facial recognition tool," *The Star*, February 14 2020.

99 Office of the Privacy Commissioner of Canada, *Privacy guidance on facial recognition for police agencies* [OPC Police FRT Guidance] (2022), online: https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/#toc3-9 at paras 124-129.

100 IPC FRT Mugshot Guidance at 12-13.

101 David Freeman Engstrom & Daniel E. Ho, *Algorithmic Accountability in the Administrative State* (2020) Yale J on Reg 800, online: papers.ssrn.com/sol3/papers.cfm?abstract_id= 3965041 at 821.

102 These issues are described in several LCO Criminal AI project papers, including the LCO Police AI Issue Paper and *AI at Trial and Appeal* [LCO AI at Trial and Appeal] by Paula Thompson, Strategic Initiatives, Ministry of the Attorney General and Eric Neubauer, Defense Counsel, Neubauer Law, and Co-Chair, Criminal Lawyers Association Technology Committee. These papers are available online at https://www.lco-cdo.org/en/our-current-projects/crimai/.

103 For example, INTERPOL's "Principles for Responsible AI Innovation" states that
Accuracy corresponds to the degree to which an AI system can make correct predictions, recommendations, or decisions. It is important that agencies verify that any system…is highly accurate, as using inaccurate AI systems can result in various types of harm.
INTERPOL Responsible AI Principles at 12.

104 See, for example, INCLO Challenging FRT at 13 and 35-42 and The Markup, *Crime Prediction Software Promised to Be Free of Biases. New Data Shows it Perpetuates Them* (December 2, 2021), online: https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them and The Markup, *Predictive Policing Software Terrible at Predicting Crimes* (October 2, 2023), online: https://themarkup.org/prediction-bias/2023/10/02/predictive-policing-software-terrible-at-predicting-crimes.

105 See, for example, INCLO Challenging FRT at 14-15

106 INTERPOL Responsible AI Principles at 13.

107 See generally, LCO American Lessons.

108 For example, the NYU Policing Project states:
Although testing under laboratory conditions shows some improvement in the quality of many FRT algorithms, we have no information about how this technology operates under real-world conditions. The two are not comparable and one cannot assume the performance in the lab tells us much about performance under actual law enforcement conditions.
NYU Policing Project, *Law Enforcement Use of Facial Recognition Technology Must Be Regulated. Here's How*, online https://www.policingproject.org/policing-technology-model-statutes-and-legislative-resources/#facial at 2.

109 See generally, LCO American Lessons at 25-26.

110 The need for public engagement on criminal justice AI issues is acknowledged widely by civil society organizations, police services and governments, leading to extensive discussions about the principle and detail of criminal AI disclosure, public accountability, and oversight.

111 See generally Accountable AI at 36-37.

112 LCO American Lessons at 36-37. Footnotes omitted.

113 LCO American Lessons at 37.

114 LCO American Lessons.

115 The potential secondary consequences of criminal convictions in Canada could affect a person's employment, entry into certain professions, educational opportunities, volunteer opportunities, or even deportation. "Secondary" or "collateral" consequences are discussed extensively in a recent guide prepared by the Canadian Bar Association, *Collateral Consequences of Criminal Convictions*. Canadian Bar Association National Magazine, *The collateral consequences of criminal convictions* (December 4, 2023), online: https://nationalmagazine.ca/en-ca/articles/law/access-to-justice/2023/the-collateral-consequences-of-criminal-convictions.

116 There are many compendiums of "trustworthy AI" statutes and frameworks available on several websites, including: UNESCO, Global AI Ethics and Governance Observatory, *Global Hub*, online: https://www.unesco.org/ethics-ai/en/global-hub; IAPP, *Global AI Law and Policy Tracker*, online: https://iapp.org/resources/article/global-ai-legislation-tracker/; and Fairly AI, *Global AI Regulation Tracker*, online: https://www.fairly.ai/blog/map-of-global-ai-regulations, to name a few.

117 See generally, LCO Accountable AI.

118 European Union, *AI Act (Regulation (EU) 2024/1689 of the European Parliament and of the Council of Europe laying down harmonized rules on Artificial Intelligence* [EU AI Act] (2024), online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689. For a good summary of the EU AI Act, see the European Commission's EU AI Act webpage at https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

119 See generally, EU AI Act, Chapter II, Article 5 and Chapter III, Articles 6, 8-17, and Annex III.

120 EU AI Act, Chapter II, Article 5, s. 1(h).

121 EU AI Act, Chapter II, Article 5, s.2.(b).

122 EU AI Act, Chapter II, Article 5, s.3.

123 EU AI Act, Chapter II, Article 5, s.4.

124 EU AI Act, Chapter II, Article 5, s.1(d).

125 These systems are permitted if such a system is used to support a human assessment of the involvement of a crime that has actually occurred. In these circumstances, the AI system is considered an evaluation based on objective and verifiable facts rather than a prediction. EU AI Act, Chapter II, Article 5, s.1(d).

126 The list in Article III includes the following AI systems:
Law Enforcement
- *Used to assess an individual's risk of becoming a crime victim.*
- *Polygraphs.*
- *Evaluating evidence reliability during criminal investigations or prosecutions.*
- *Assessing risk of an individual offending or re-offending not solely based on profiling or assessing personality traits or past criminal behaviour.*

Administration of Justice
- *AI systems used in researching and interpreting facts and applying the law to concrete facts or used in alternative dispute resolution.*

EU AI Act, Chapter III, Annex III.

127 EU AI Act, Chapter III, Articles 8-17.

128 United States, Office of the President, Executive Order 14110 "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" [Executive Order 14110] (November 1 2023), online: https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

129 Office of Management and Budget, Executive Order M-24-10 "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence" [Executive Order M-24-10] (March 2023) at 2-4. Executive Order M-24-10 includes requirements to establish Chief AI Officers, AI governance bodies, compliance plans, use case inventories, responsible AI strategies (including plans for operational and governance processes to manage AI risks), to implement "initial baseline" AI risk management practices and "additional, context-specific risks that are associated with their use of AI as appropriate", among other requirements.

130 Executive Order M-24-10 at 21-24.

131 Executive Order M-24-10 at 31.

132 Executive Order M-24-10 at 32.

133 The White House, *Removing Barriers to American Leadership in Artificial Intelligence* (January 23, 2025), online: https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/.

134 For example, the first Trump Administration's December 2020 "Executive Order on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government" included a statement that
Sec. 3. Principles for Use of AI in Government. When designing, developing, acquiring, and using AI in the Federal Government, agencies shall adhere to the following Principles:
(a) Lawful and respectful of our Nation's values. Agencies shall design, develop, acquire, and use AI in a manner that exhibits due respect for our Nation's values and is consistent with the Constitution and all other applicable laws and policies, including those addressing privacy, civil rights, and civil liberties.
(b) Purposeful and performance-driven. Agencies shall seek opportunities for designing, developing, acquiring, and using AI, where the benefits of doing so significantly outweigh the risks, and the risks can be assessed and managed.
(c) Accurate, reliable, and effective. Agencies shall ensure that their application of AI is consistent with the use cases for which that AI was trained, and such use is accurate, reliable, and effective.
This section also included provisions stating that federal government AI had to be "Safe, secure, and resilient"; "Understandable"; "Responsible and traceable"; "Regularly monitored": "Transparent"; and "Accountable." United States, Executive Office of the President, December 2020 *Executive Order on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government* [December 2020), online: https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-promoting-use-trustworthy-artificial-intelligence-federal-government/.

135 There are compendiums of American AI statutes on several websites, including: National Conference of State Legislatures, *Artificial Intelligence 2024 Legislation*, online: https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation; IAPP, *Global AI Law and Policy Tracker*, online: https://iapp.org/resources/article/global-ai-legislation-tracker/; and the Brennan Centre, *Artificial Intelligence Legislation Tracker*, online: https://www.brennancenter.org/our-work/research-reports/artificial-intelligence-legislation-tracker. See also Nicole Turner Lee and Obioha Chijioke, Commentary, Brookings Institution, *Why states and localities are acting on AI* (December 15, 2023), online: https://www.brookings.edu/articles/why-states-and-localities-are-acting-on-ai/.

136 The LCO can provide a compendium upon request.

137 LCO Police AI Issue Paper.

138 A good summary of US FRT legislation is included in Mailyn Fidler and Justin Hurwitz, "An Overview of Facial Recognition Regulation in the United States" in *The Cambridge Handbook of Facial Recognition in the Modern State* (March 2024), online: https://www.cambridge.org/core/books/cambridge-handbook-of-facial-recognition-in-the-modern-state/an-overview-of-facial-recognition-technology-regulation-in-the-united-states/5D53D166AF623A44E1EA4E892C63727B.

139 Spivack, Jameson and Garvie, Clare, AINow Institute, "A Taxonomy of Legislative Approaches to Face Recognition in the United States" in *Regulating Biometrics: Global Approaches and Open Questions,* [AI Taxonomy] (Sept 2020), online: https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions at 86-95.

140 AI Taxonomy at 94.

141 AI Taxonomy at 89.

142 AI Taxonomy at 92-94.

143 Policing Project, New York University School of Law, *Regulating Police Use of Facial Recognition Technology – Resources for Legislators*, [NYU Policing Project FRT Resources] (accessed March 2025), online: https://www.policingproject.org/regulating-police-use-of-face-recognition-technology.

144 Policing Project, New York University School of Law, *Legislative Checklist for State Lawmakers*, [NYU Policing Project FRT Resources] (accessed March 2025), online: https://www.policingproject.org/regulating-police-use-of-face-recognition-technology.

145 New York Police Department, Facial Recognition Technology Policy, [NYPD FRT Policy] (Updated 2023), online: https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page.

146 Office of the Chief of Police, *Los Angeles Police Department, Use of Photo Comparison Technology Within Los Angeles County's Digital Mugshot System*, [LAPD Special Order 2-2021] included in Office of the Inspector General, Los Angeles Police Commission, *Review of the Department's Use of Photo Comparison Technology,* (2022), online: https://www.oig.lacity.org/significant-reports.

147 INTERPOL Responsible AI Principles. These principles are one component of nine part "AI Toolkit", that includes sections on AI risk assessments, organizational roadmaps, technical references, an organizational readiness questionnaire, and "innovation workbook." See generally, INTERPOL, *AI Toolkit* [INTERPOL AI Toolkit], (Revised 2024), online:https://www.interpol.int/en/How-we-work/Innovation/Artificial-Intelligence-Toolkit.

148 NYPD FRT Policy at 5.

149 NYPD FRT Policy at 1.

150 NYPD FRT Policy at 4-7.

151 See, for example, Ivey Dyson and Emile Ayoub, Brennan Center for Justice, *NYPD Continues to Dodge Surveillance Transparency Laws* (June 12, 2024), online: https://www.brennancenter.org/our-work/analysis-opinion/nypd-continues-dodge-surveillance-transparency-laws and Surveillance Technology Oversight Project (STOP), *Seeing Is Misbelieving: How Surveillance Technology Distorts Crime Statistics* (June 2024), online: https://www.stopspying.org/seeing-is-misbelieving.

152 INTERPOL AI Toolkit.

153 INTERPOL Responsible AI Principles at 6.

154 *Digital Charter Implementation Act*; *1st Sess. 44th Parliament, 2022, Part 3 "Artificial Intelligence and Data Act",* [*AIDA*], online: https://www.parl.ca/legisinfo/en/bill/44-1/c-27.

155 *AIDA*, s. 3.

156 As drafted, *AIDA* required persons responsible for AI systems to assess whether their systems were high-impact and to "establish measures to identify, assess and mitigate the risks of harm or biased output" in accordance with *AIDA* regulations. *AIDA*, sections 7 and 8. The wording of this section is broad enough that "mitigation" could include "cease operations".

157 *AIDA*, s. 5(1).

158 *AIDA*, sections 7 and 8.

159 AIDA s. 11(1) and (2).

160 For a discussion on AIDA as "risk-based" regulation, see Teresa Scassa's paper "Regulating AI in Canada: A Critical Look at the Proposed Artificial Intelligence and Data Act", *The Canadian Bar Review*, Vol. 101, 2023.

161 See, for example, a joint open letter from 45 civil society organizations, experts and academics criticizing *AIDA* on numerous grounds, online: https://bccla.org/policy-submission/joint-letter-of-concern-regarding-the-artificial-intelligence-and-data-act-aida/.

162 Canada. Innovation, Science and Economic Development Canada, "Letter to the Chair of the Standing Committee on Industry and Technology on Bill C-27" (November 28, 2023), online: https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12751351/12751351/MinisterOfInnovationScienceAndIndustry-2023-11-28-Combined-e.pdf.

163 A good summary of these criticisms is set out in Barry Sookman, *Analyzing AIDA 2.0: the problems with the proposed amendments to AIDA* (December 20, 2023), online: https://barrysookman.com/2023/12/20/analyzing-aida-2-0-the-problems-with-the-proposed-amendments-to-aida/.

164 Privacy and Access Council of Canada, "Key stakeholders call for withdrawal of controversial AI legislation," April 24, 2024, online: https://pacc-ccap.ca/aida-open-letter/.

165 Canada, *Directive on Automated Decision-Making* [Canada ADM Directive] (2019), online: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592; and Algorithmic Impact Assessment Tool [Canada AIA], online: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html.

166 Two LCO reports, Accountable AI and Regulating AI, include extensive analyses of the Canada ADM Directive and AIA.

167 See Accountable AI at 57-66 and Regulating AI at 17-49.

168 Canada ADM Directive, s. 5.1. Note that the Directive applies only to federal departments subject to Treasury Board Secretariat.

169 Canada ADM Directive, Appendix A and "Guide on the Scope of the Directive on Automated Decision-Making", online: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/guide-scope-directive-automated-decision-making.html.

170 This review is expected to be completed in 2025.

171 RCMP Communication with the Law Commission of Ontario, on file with the LCO.

172 RCMP Transparency Blueprint.

173 RCMP Transparency Blueprint at 6-7.

174 RCMP Communication with the Law Commission of Ontario, on file with the LCO.

175 RCMP Transparency Blueprint at 9.

176 *Enhancing Digital Security and Trust Act*, S.O. 2024, c. 24, [EDSTA], online: https://www.ontario.ca/laws/statute/24e24.

177 Government of Ontario, Ministry of Public and Business Service Delivery and Procurement, *Responsible Use of AI Directive*, December 1, 2024 [Ontario AI Directive].

178 Government of Ontario, *Consultation on proposed legislation: Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024 (2024),* online: https://www.ontariocanada.com/registry/view.do?postingId=47433&language=en.

179 Law Commission of Ontario, *Bill 194, Law Commission of Ontario Submission* [LCO Bill 194 Submission] (2024), online: https://www.lco-cdo.org/en/lco-releases-bill-194-submission/.

180 EDSTA s. 5(1) states that its provisions respecting AI systems "applies to such public sector entitles as may be prescribed if they use or intend to use an artificial intelligence system in prescribed circumstances." This section includes two important Bill 194 limitations. First, s. 1(1) identifies which "public sector entities" will be subject to EDSTA, including:
(a) an institution within the meaning of subsection 2 (1) of the Freedom of Information and Protection of Privacy Act,
(b) an institution within the meaning of subsection 2 (1) of the Municipal Freedom of Information and Protection of Privacy Act,
(c) a children's aid society,
(d) a school board; ("entité du secteur public").
[Emphasis added.] Second, s. 5(1) allows the province to prescribe AI "uses" or "circumstances" that are subject to Bill 194. Neither "use" nor "circumstances" is defined in the Act. Notably, neither s. 2(1) of *Freedom of Information and Protection of Privacy Act nor s.* 2(1) of the *Municipal Freedom of Information and Protection of Privacy Act include police services, courts, or tribunals. As a result, these institutions are not subject to Bill 194 governance or requirements.*

181 Ontario AI Directive.

182 Ontario AI Directive, s. 2.

183 The Ontario AI Directive requires the
…application of AI risk management by ministries and provincial agencies that are seeking to use AI systems, or use services that include AI functionality (including procured, ministry/provincial agency developed and publicly available tools), as part of the development of delivery of, or decision-making for, a Government of Ontario policy, program, or services."
Ontario AI Directive, s. 3.

184 More specifically, the principles in the Ontario AI Directive include:
- AI used to benefit the people of Ontario (5.1)
- AI use is justified and proportionate, systems are reliable and valid (5.2)
- AI is use in a safe, secure and privacy protected way (5.3)
- AI use is human rights affirming and non-discriminatory (5.4)
- AI use is transparent and meaningful explanations of decisions are made available (5.5)
- AI use is accountable and responsible (5.6)

185 Ontario AI Directive, s. 6.1 states that parties must explain the use of the AI system, identify and assess risks of the AI system, plan and implement methods to control those risks, and report and monitor the efforts to assess and control the risks.

186 Ontario AI Directive, sections 6.2 and 6.3 state that if the public interacts directly with an AI system (such as a chat bot), or if an AI system is involved in decision-making directly affecting a member of the public, ministries/agencies must publicly disclose the AI use as part of the process, service or program. Ministries and agencies must also provide an accessible avenue for the public to seek information about the use of AI in a process, service or program.

187 The Ontario AI Directive designates responsibility for AI risk management to each Ministry and designated agency executives. The Directive also:

- Requires the Associate Deputy Minister, Policy Archives and Data (PAD) is to conduct reviews of the Directive every two years at a minimum (s. 7.5).
- Assigns accountabilities and responsibilities for the Directive to designated officers across the provincial government (sections7.1 to 7.10). For example, Deputy Ministers are to ensure principles and requirements are implemented and monitored.

188 These agencies are not explicitly included in the Ontario AI Directive.

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

190 For example, the Ontario AI Directive does not include explicit provisions respecting:

- A public AI registry.
- Mitigation strategies.
- Impact assessments.
- Third party audits.
- Consultations.
- Explainability.

191 Section 3 of the Ontario AI Directive states that the Directive "requires the application of AI risk management" but does not include risk categories or guidance or metrics for how AI risks are to be identified or assessed. Most obviously, the Ontario AI Directive does not identify prohibited AI systems or criteria to determine if a system should be prohibited. Section 6 introduces "risk management obligations" where Ministries must "identify risks" and "assess risks" and "report and monitor risk assessments". However, it is unclear how and what risks are to be assessed/identified or what information needs to be reported.

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

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

194 The Ontario AI Directive states "The principles are meant to be applied in alignment with existing legislation..." (s.5).

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

196 The LCO participated in the consultation process for this policy. A copy of the LCO's 2021 submission is available at https://www.lco-cdo.org/en/publications-papers/.

197 TPS AI Policy, "Guiding Principles."

198 TPS AI Policy, "Guiding Principles."

199 TPS AI Policy, "Policy of the Board."

200 TPS AI Policy, "Definitions."

201 TPS AI Policy, "Continuous Review."

202 TPS AI Policy, "Policy of the Board", "Continuous Review."

203 TPS AI Policy, "Board Approval and Reporting Prior to Procurement, Utilization and Deployment."

204 TPS AI Policy, "Board Approval and Reporting Prior to Procurement, Utilization and Deployment."

205 TPS AI Policy, "Review and Assessment of New Technologies."

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

207 Durham Regional Police Services Board, *Use of Artificial Intelligence Policy,* October 2024 [Durham Police AI Policy], online at https://durhampoliceboard.ca/policies-and-bylaws/.

208 Durham Police AI Policy s. 2.

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

210 Privacy Commissioners Joint Clearview AI Investigation.

211 OPC Way Forward.

212 Privacy Commissioners Joint Police FRT Statement.

213 IPC Mugshot Guidance and IPC ALPR Guidance.

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

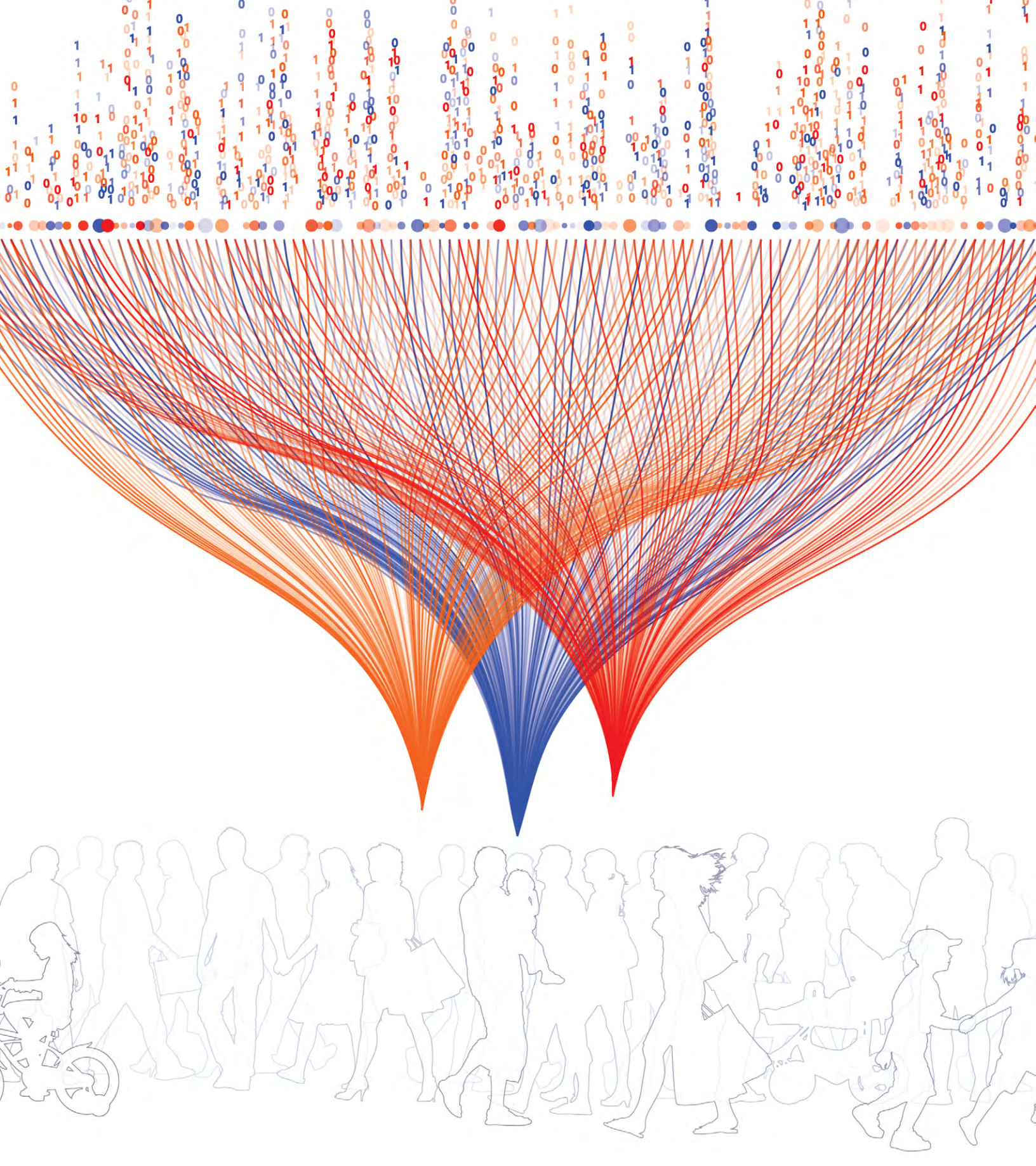
215 Alberta, "Notice to the Profession & Public- Ensuring the integrity of court submissions when using Large Language Models" (October 2023), online: https://www.albertacourts.ca/kb/resources/announcements/notice-to-the-profession-public---use-of-ai-in-citations-submissions; Manitoba, "Re: Use Of Artificial Intelligence In Court Submissions (June 2023), online: https://www.manitobacourts.mb.ca/site/assets/files/2045/practice_direction_-_use_of_artificial_intelligence_in_court_submissions.pdf; Québec, "Integrity of Court Submissions When Using Large Language Models" (October 2023) online: https://coursuperieureduquebec.ca/fileadmin/cour-superieure/Communiques_and_Directives/Montreal/Avis_a_la_Communite_juridique-Utilisation_intelligence_artificielle_EN.pdf.

216 Federal Court Practice Direction.

217 Canadian Judicial Council, *Guidelines for the Use of Artificial Intelligence in Canadian Courts* (Sept. 2024) [CJC Guidelines], online at https://cjc-ccm.ca/en/news/canadian-judicial-council-issues-guidelines-use-artificial-intelligence-canadian-courts.

218 CJC Guidelines at 6.

219 CJC Guidelines at 8-9.



LCO CDO
LAW COMMISSION OF ONTARIO
COMMISSION DU DROIT DE L'ONTARIO

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