



Law Commission of Ontario

AI IN CRIMINAL JUSTICE PROJECT

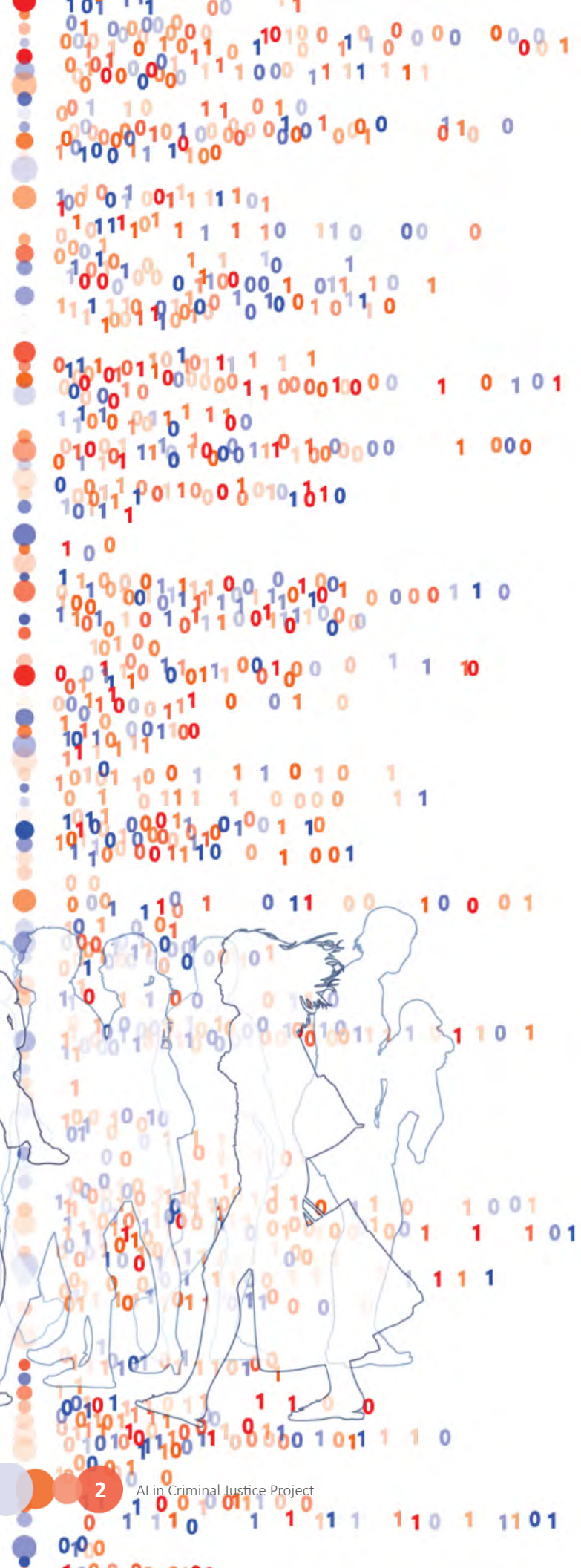
Final Report and Recommendations

October 2026



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.

A Board of Governors, representing a broad cross-section of leaders within Ontario's justice community, guides the LCO's work. Financial support is provided by the Law Foundation of Ontario, the Law Society of Ontario, and Osgoode Hall Law School.

Recent LCO reports and submissions addressing AI issues include:

- [Submission to the Ontario Court AI Subcommittee of the Civil Rules Committee](#) (2025)
- [Submission to the National Sprint on Canada's AI Strategy](#) (2025)
- [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)

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



Law Commission of
Ontario

Commission du droit
de l'Ontario

Authors

Ryan Fritsch, Counsel, Law Commission of Ontario
Nye Thomas, Executive Director, Law Commission of Ontario

Issue Papers Series Editors

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

Law Student Researchers & Contributors

Thurka Brabakaran
John Dief
Nouran Hamzeh
Shahmurad Lodhi
Maria Michouris
John Nyman
Rameiya Paramalingam
Ani Semanjaku
Shahroze Zafar

Citation

Law Commission of Ontario, *AI in Criminal Justice: Final Report and Recommendations* (2026), online at <https://lco-cdo.org/en/projects/ai-in-criminal-justice/>.

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. This paper was written without AI tools or assistance.

Contact

Law Commission of Ontario
2030 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](https://bsky.social/@lco-cdo)

YouTube: [@lawcommissionofontario8724](https://www.youtube.com/channel/UC8724)

Funders

The LCO is funded by the Law Foundation of Ontario, Law Society of Ontario, and Osgoode Hall Law School. The LCO gratefully acknowledges the funding from the Law Commission of Canada in support of the Vancouver and Toronto roundtable consultation events.



Table of Abbreviations – Entities

CACP	Canadian Association of Chiefs of Police
IGoP	Inspector General of Policing (Ontario)
IPC	Information and Privacy Commissioner of Ontario
LAPD	Los Angeles Police Department
LCO	Law Commission of Ontario
LECA	Law Enforcement Complaints Agency (Ontario)
MAG	Minister of the Attorney General (Ontario)
NTOP	RCMP National Technology Onboarding Program
OPC	Office of the Privacy Commissioner of Canada
RCMP	Royal Canadian Mounted Police
TPS	Toronto Police Services
UBC AI & Criminal Justice Project	University of British Columbia Artificial Intelligence and Criminal Justice Initiative, Peter A. Allard School of Law

Table of Abbreviations – Technologies

AI	Artificial Intelligence
ALPR	Automated License Plate Reader
CCTV	Closed-Circuit Television (Security Cameras)
CSAM	Child Sexual Abuse Material
FRT	Facial Recognition Technology
LFR	Live Facial Recognition Technology
LLM	Large Language Models
OIFR	Operator-Initiated Facial Recognition Technology
OSINT	Open-Source Intelligence
RFR	Retroactive Facial Recognition Technology
SOCINT	Social Media Intelligence

Table of Abbreviations – Legislation & Policies

ADM Directive	Automated Decision-making Directive (Canada)
AIA	Algorithmic Impact Assessment (Canada)
AIDA	<i>Artificial Intelligence and Data Act</i> (Canada)
CJA	<i>Courts of Justice Act</i>
EDSTA	<i>Enhancing Digital Security and Trust Act, 2024</i> (Ontario)
EU AI Act	<i>Artificial Intelligence Act</i> (EU)
NTOP	RCMP National Technology Onboarding Program
Ontario AI Directive	Responsible Use of Artificial Intelligence Directive (Ontario)
TPS AI Policy	Toronto Police Service “Use of Artificial Intelligence Technology” Policy

Contents

1. Introduction.....	7
1.1 Responsible Criminal AI in Canada	7
1.2 About the LCO.....	9
1.3 The AI in Criminal Justice Project.....	9
1.4 Project Lead and Funding	12
1.5 Next Steps and Contacts	12
2. Criminal AI Systems and Their Potential	14
2.1 Facial Recognition and Biometric Technology	16
2.2 ALPRs/Vehicle Surveillance Systems	20
2.3 Predictive Policing	22
2.4 Open Source Intelligence and Social Media Intelligence	23
2.5 Drones	23
2.6 AI-assisted Police Reports	24
2.7 Evidence Management	24
2.8 Gunshot Detection/Object Recognition	25
2.9 Bail and Sentencing Algorithms	25
2.10 Biometric Inferencing.....	25
2.11 Criminal Courts, Crowns and Defence Counsel.....	26
2.12 Other AI Systems Used in Criminal Justice	26
3. Criminal AI Harms and Risks.....	27
3.1 Legal Risks	27
3.2 Governance Risks	34
3.3 Administration of Justice and Access to Justice Risks	36
4. Responsible Criminal AI	38
4.1 International.....	38
4.2 Responsible Criminal AI in Canada	44
5. Gaps, Risks and Opportunities in the Canadian Criminal Justice System	51
5.1 Gaps in Responsible Criminal AI in Canada	51
5.2 What If We Do Not Regulate?.....	55
5.3 Responsible Criminal AI Consensus.....	55

6. LCO Recommendations: A Provincial Responsible Criminal AI Framework 58

Recommendations 1-3: Provincial Criminal AI Framework..... 62

Recommendation 4: Provincial Criminal Justice AI Legislation..... 64

 Provincial Legislation 65

 The Precautionary Principle 67

 The Principle of Judicial Independence 68

Recommendations 5-7: Provincial Reporting and Oversight 69

Recommendation 8: Digital Sovereignty and Procurement..... 74

Recommendation 9: Public Engagement 78

Recommendations 10-15: Criminal AI Risk Management 79

 Recommendations 10-11: Risk Categories and Public Consultations 80

 Recommendation 12: Prohibited AI Systems..... 83

 Recommendation 13: High Risk AI Systems..... 86

 Recommendation 14-15: Restricted Use / Medium Risk and Low Risk Technologies 89

Recommendation 16: Public Criminal AI Registry..... 92

Recommendation 17: Standard Risk Assessment 96

Recommendation 18: AI Pilots, Procurement and Digital Sovereignty 97

Recommendations 19-20: Oversight and Reporting Requirements 99

 Independent Supervisory Body for AI Systems in Criminal Justice..... 100

 Mandatory Reporting to LECA and IGoP 101

 What Should Be Reported? 101

 Crown Criminal AI Advisory Office 102

Recommendations 21-24: AI Evidence..... 103

 AI Evidence in Criminal Justice 104

 Establishing Procedural Rules Governing Criminal AI Evidence in Ontario 106

 AI Evidence in Bail Proceedings..... 107

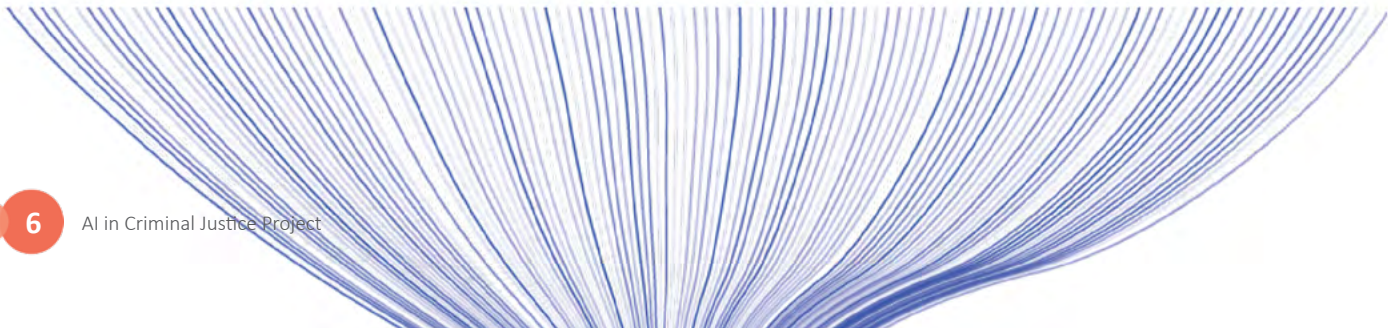
 Amending the Crown Prosecution Manual 109

Recommendations 25-29: Access to Justice and System Capacity..... 110

 Legal Aid Ontario 111

 Access to Experts and Forensic Tools..... 112

7. Endnotes..... 113





1. Introduction

1.1 Responsible Criminal AI in Canada

This is the *Final Report and Recommendations* of the Law Commission of Ontario's (LCO) **Artificial Intelligence in Criminal Justice Project** (the "Criminal AI project").¹ The Criminal AI Project is a groundbreaking survey and analysis of the opportunities, risks and law reform issues regarding artificial intelligence (AI) in Canada's criminal justice system.

The LCO believes this project is urgent. AI in the criminal justice system affects some of the most important issues and rights in Canadian society, including public safety, personal liberty, the Canadian *Charter of Rights and Freedoms*, procedural rights, and public trust in key institutions, including courts and law enforcement.

Fast-paced technological, legislative and policy developments in Canada and internationally have put pressure on Canadian governments, law enforcement services, courts, prosecutors, defence counsel and other stakeholders to respond quickly to AI in criminal justice.

AI is increasingly used in criminal justice systems in Canada and worldwide to aid investigations, analyze evidence, conduct risk assessments, support courts, research and prepare submissions and judgements, and better target resources. AI tools include biometric surveillance and facial recognition technology (FRT), predictive policing, automated license plate readers (ALPRs), social media monitoring, document and video analysis, bail and sentencing algorithms, drones, notetaking and many more.

Many AI technologies have the potential to improve public safety, improve police investigations, and improve the efficiency and fairness of criminal proceedings. At the same time, criminal AI systems such as predictive policing, FRT and generative AI systems have proven risks to human rights, criminal prosecutions, the reliability of evidence, privacy and access to justice. These risks affect racialized and low-income communities most acutely.

Criminal AI systems in many jurisdictions are widespread, expanding and controversial. In England and Wales, for example, more than 4.6 million faces were scanned by live facial recognition systems in 2024.² Criminal AI systems are also deployed widely in the United States, including a network of up to 140,000 ALPRs deployed across the country.³

American ALPR systems or “Flock” cameras (named after a company called Flock Safety, a leading US ALPR provider) have become an intense flashpoint for many of the issues discussed in this report. “Flock” cameras have been widely criticized for promoting mass surveillance and for being, in the words of the Governor of Florida, “out of control.”⁴ The pushback against this technology has been swift, bipartisan and decisive: DeFlock, an American ALPR mapping website, reports that 153 cities have cancelled or rejected ALPR contracts or deactivated cameras since 2021, including more than 50 in August 2026 alone.⁵

In these examples and many others, criminal AI systems are alternately praised for improving public safety and criticized for mass surveillance, racial and gender bias, violation of procedural rights, and errors and hallucinations. In response to these issues, many governments and other institutions have adopted “responsible AI” laws and policies to promote the benefits of criminal AI systems while controlling their limitations and foreseeable risks. Most recently, in June 2026, the UK government announced PoliceAI, “a new national centre dedicated to the responsible development, piloting and scaling of artificial intelligence in policing.”⁶

In comparison, AI deployment in the Canadian criminal justice system has been slower. However, reports suggest that many Canadian police services have piloted or deployed a range of AI systems including FRT, object recognition, predictive policing, ALPRs and drones. Canadian prosecutors, defence counsel, self-represented litigants and courts are also beginning to use AI systems.

Adoption of responsible criminal AI governance tools in Canada appears slower also. To date, no government in Canada has enacted dedicated laws or regulations governing the use of AI by law enforcement or criminal courts. Absent this guidance, many Canadian police services and other institutions have developed criminal AI self-governance policies.

Criminal AI systems introduce new and complex risks which could expose an unprecedented number of Ontarians to police surveillance, privacy violations, racial bias and other AI risks and harms. The LCO’s

research and consultations demonstrate that patchwork, uncoordinated responses are insufficient to govern these complex and widespread risks. Most notably, the LCO and many stakeholders are concerned that the combination of multiple laws, multiple institutions and complex technologies could result in ad hoc, inconsistent or improper governance of criminal AI systems. As a result, the LCO and others believe the provincial response to these risks must be coordinated and systemic to ensure criminal AI systems are legal, beneficial and have public trust.

This project is the first in Canada to analyze AI systems and issues across the entire “lifecycle” of criminal justice. This is also the first project in Canada to engage with stakeholders and institutions across the criminal justice system to collaboratively develop recommendations for law, regulatory and policy reform. The result is a comprehensive agenda and strategy that would embed responsible AI principles and policies throughout the criminal justice system. An important finding of this project is the near-universal desire amongst criminal justice stakeholders to work together to address criminal AI issues constructively.

The LCO’s 29 recommendations are principled, practical, balanced and proven. Indeed, almost all our recommendations are based on precedents, practices and strategies already in place in Canada, other jurisdictions or currently under development by Canadian law enforcement, governments and other justice institutions.

An **Executive Summary** and **List of Recommendations** are also available on the project [website](#). Readers should note that while LCO’s *Final Report and Recommendations* are largely focussed on Ontario, we believe they can be adapted to other Canadian jurisdictions.

1.2 About the LCO

The 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 law reform and public debate. LCO reports are a practical and principled long-term resource for policymakers, stakeholders, academics and the public. LCO reports have led to legislative amendments and changes in policy and practice. They are also frequently cited in judicial decisions, academic articles, government reports and the media.

A Board of Governors, representing a broad cross-section of leaders within Ontario's justice community, guides the LCO's work. Financial support is provided by the Law Foundation of Ontario, the Law Society of Ontario, and Osgoode Hall Law School.

This project is part of the LCO's multiyear AI in the Justice System project. This project analyzes AI regulation and governance issues from the perspective of the *Charter*, human rights, privacy, procedural fairness and access to justice. Recent LCO reports and submissions addressing AI issues include:

- [Submission to the Ontario Court AI Subcommittee of the Civil Rules Committee](#) (2025)
- [Submission to the National Sprint on Canada's AI Strategy](#) (2025)
- [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)

The LCO is located at Osgoode Hall Law School in Toronto.

More information about the LCO and its projects is available at www.lco-cdo.org.

1.3 The AI in Criminal Justice Project

The LCO's [AI in Criminal Justice Project](#) is the first comprehensive survey and analysis of the opportunities, risks and law reform issues regarding AI in the Canadian criminal justice system. The project combined extensive research, consultations and collaborations to address four key themes or topics.

First, the project considers important practical and legal questions confronting Canadian police, courts, policymakers, Crowns, defence counsel and accused, including:

- What AI tools could be used at each important stage of Canadian criminal justice?
- What legal issues are likely to arise at each stage?
- What is the state of Canadian law to address these issues?

Second, the project considers solutions at the specific and systemic level, including:

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

Third, the project asks what institutions, agencies, organizations or individuals will be affected by AI in the criminal justice system? What supports or policies are needed to promote the successful adoption of AI in the criminal justice system?

Finally, the project predicts what is likely to happen in Canadian criminal justice if action is not taken.

Issue Papers

In April 2025, the LCO released a project introduction/summary and four Issue Papers. Each Issue Paper considered AI in a distinct phase of the criminal justice process:

- [Paper 1: Introduction and Summary](#)
- [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](#)⁷

Together, the Issue Papers presented a “lifecycle” analysis of AI throughout Canadian criminal justice.

Project Roundtables

In addition to the project Issue Papers, the LCO convened two half-day roundtable events to consider key criminal justice AI issues.

The first event was our June 2025 [Vancouver Roundtable on the Use of Facial Recognition Technology by Law Enforcement](#). This event was followed in August 2025 with our [Toronto Roundtable on AI Evidence in Criminal Justice](#). Event reports are available for both roundtables.⁸

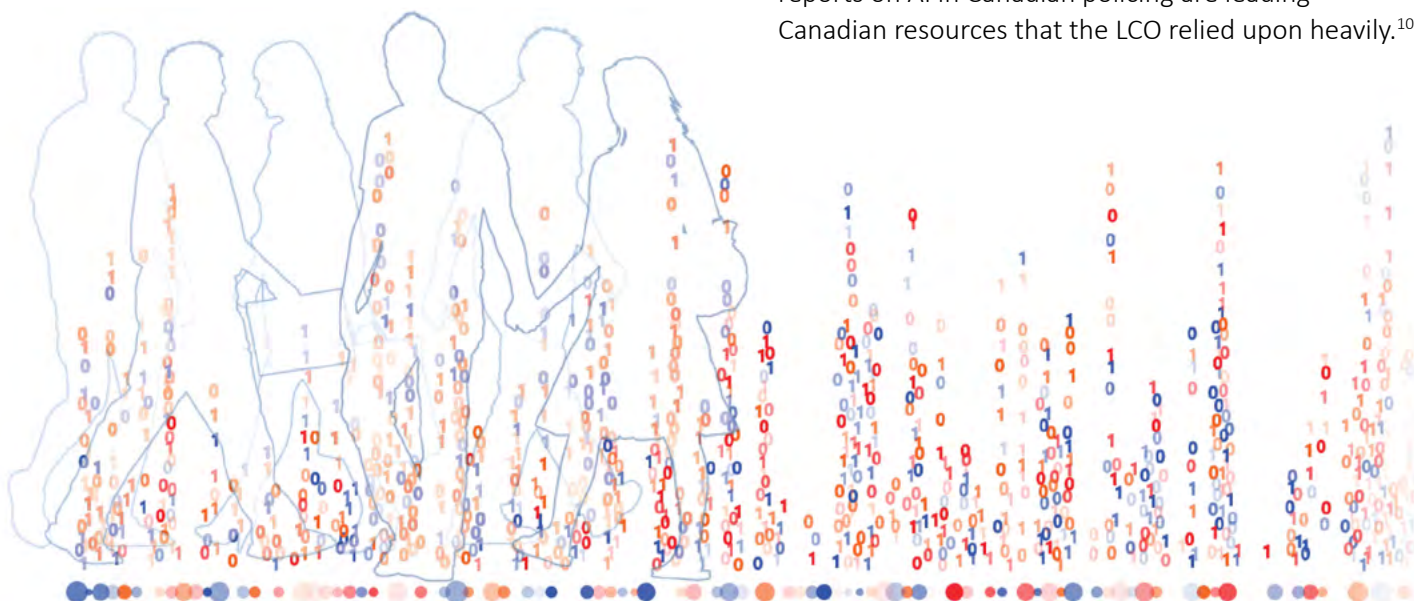
Project Consultations, Collaborators and Partnerships

After the Issue Papers were released, the LCO began extensive consultations and engagements that concluded in early 2026.

During this period, the LCO worked closely with law enforcement, Crown prosecutors, criminal defence lawyers, judges, governments, legal aid agencies, oversight agencies, privacy commissions, human rights commissions, professional associations, NGOs, community advocates, technology developers and academics.

In total, more than 1,400 people participated in more than 30 public discussions, workshops, conferences, and public lectures across Canada.⁹ Consultations included participants from British Columbia, Alberta, Saskatchewan, Nova Scotia, New Brunswick and Ontario as well as Canadian federal institutions. The LCO also met with hundreds of stakeholders across the country for frank and thoughtful private discussions. The LCO is deeply indebted to every person and institution who participated in this process.

Finally, the LCO benefitted from a strong research and consultation partnership with the UBC Artificial Intelligence and Criminal Justice Initiative, led by Professor Benjamin Perrin of the Peter A. Allard School of Law, University of British Columbia. Professor Perrin’s comprehensive research and roundtable reports on AI in Canadian policing are leading Canadian resources that the LCO relied upon heavily.¹⁰



WE LISTENED

1400+

participants in

27

consultation,
roundtable, conference
and education events

7

Published Issue
Papers and
Roundtable Reports

7

Issue Paper
authors

12

Advisory
Committee
members

3

Roundtable
events

29

Final
Recommendations

WE FOUND COMMON GROUND

Judiciary

Courts and judges

Government & regulators

Federal/provincial ministries, privacy and human-rights bodies

Law enforcement

Police, police governance & oversight bodies

Civil society

Civil liberties, equality and advocacy organizations

Legal profession

Crown, defence, Legal Aid & law societies

Academia

Law, criminology, sociology, technology & AI researchers

Advisory Committee and Project Authors

The LCO's project Advisory Committee provided invaluable guidance and support to the LCO over the course of the project. Members included:

- Alpha Chan, Chief Information Security Officer, Toronto Police Services
- Rosanna Giancristiano, Director, Court Operations, Ministry of the Attorney General
- Megan Howatt, Counsel, Office of the Chief Justice of the Superior Court of Justice
- Tamir Israel, Director of Privacy, Surveillance & Technology, Canadian Civil Liberties Association
- Alan Jaffee, Senior Policy Advisor, Policing Standards Section, Solicitor General
- Daniel Konikoff, Associate Professor, Department of Sociology, University of Alberta
- Elena Middelkamp, Crown Law Office Criminal, Ministry of the Attorney General
- Savio Pereira, Team Lead, Policing Standards Section, Ministry of the Solicitor General
- Ben Perrin, Professor, Faculty of Law, University of British Columbia
- Shakir Rahim, Director, Criminal Justice Program, Canadian Civil Liberties Association
- David Murakami Wood, Professor, Department of Criminology, University of Ottawa
- Dina Zalkind – Policy Counsel, Legal Aid Ontario

The LCO also partnered with institutional and subject matter experts who authored our project Issue Papers and often participated in consultation events. Issue Paper authors included:

- Gideon Christian, Professor, Faculty of Law, University of Calgary
- Armando D'Andrea, (then) Staff Lawyer, Provincial Office, Legal Aid Ontario
- Ryan Fritsch, Policy 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, Chair, 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

The LCO worked closely with our Advisory Committee and Issue Paper authors on every aspect of the project. The LCO is deeply indebted to these individuals and their institutions for their advice, time and support.

1.4 Project Lead and Funding

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

This project was funded by the LCO with additional project funding from the Law Commission of Canada and support from the UBC Artificial Intelligence and Criminal Justice Initiative.

1.5 Next Steps and Contacts

The LCO believes that successful law reform depends on broad and accessible consultations with individuals, communities, and organizations across Ontario. The LCO can be contacted at:

Law Commission of Ontario
Osgoode Hall Law School, York University
2030 Ignat Kaneff Building
4700 Keele Street Toronto
ON M3J 1P3

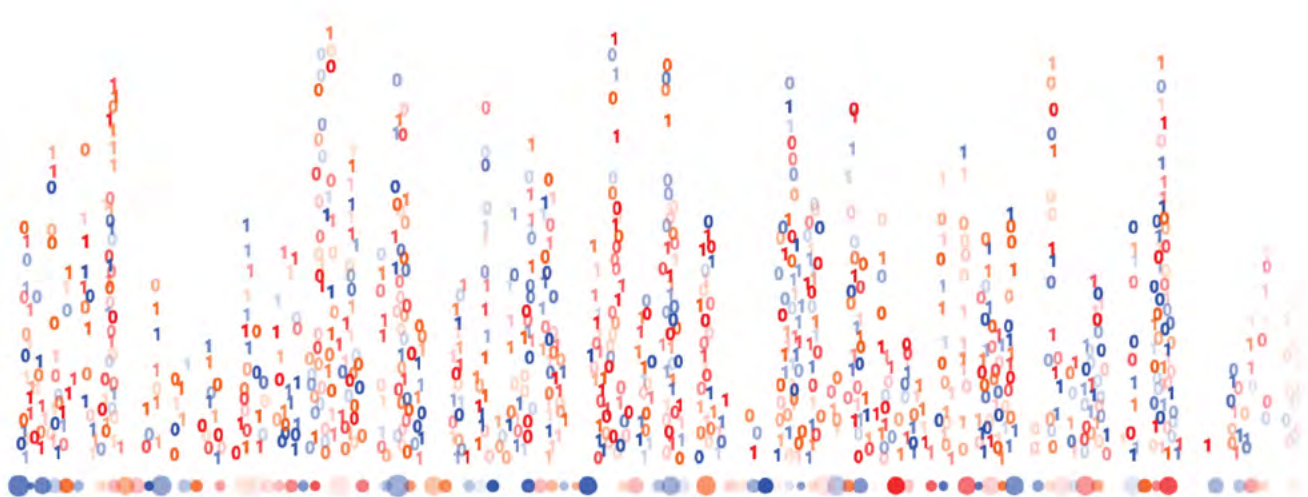
Telephone: (416) 650-8406

Email: lawcommission@lco-cdo.org

Web page: www.lco-cdo.org

LinkedIn: <https://linkedin.com/company/lco-cdo>

Bluesky: [@lco-cdo.bsky.social](https://bsky.social/lco-cdo)



Criminal AI in Canada

The extent of AI use by police agencies and other criminal justice institutions in Canada is not known. This is because there is no consistent rule or obligation for police or governments to disclose these technologies. The LCO's research and consultations suggest that the criminal justice system in Canada has been more cautious in adopting AI technology than other jurisdictions. There is also evidence that AI adoption in Canada is accelerating.

Fortunately, some prominent Canadian police services have committed to disclose at least some of their AI systems. For example, as of August 2026, the Royal Canadian Mounted Police (RCMP) had disclosed the use of 14 AI systems on the Government of Canada AI Register, including tools to:

- Assist child trafficking and exploitation investigations.
- Identify child sexual exploitation images.
- Assist transcribing, reviewing and categorizing video and audio files.
- Help officers generate draft reports using audio from body worn cameras.¹¹

The Toronto Police Service (TPS) also discloses AI systems pursuant to the Toronto Police Service Board's "Use of AI Policy." As of September 2026, the TPS disclosure lists six technologies, including:

- NeoFace, FRT technology that compares images to booking photographs.
- Automated Fingerprinting Identification System, biometric technology that compares fingerprints located at a crime scene with a database of known offenders.
- Axon ALPR, an automated licence plate recognition system that compares licence plates to those associated with stolen vehicles, missing persons and AMBER alerts.
- Briefcam, an object recognition system which assists investigators review large video files for specific objects and licence plates.¹²

The March 2026 UBC AI & Criminal Justice Project paper *AI and Policing: Research Report on the Governance and Use of Artificial Intelligence by Police in Canada* (UBC Police AI Report) represents the most

comprehensive survey of police AI use in Canada.¹³ The UBC Police AI Report, other research reports,¹⁴ police service disclosures and media reports suggest that the following Canadian police services have considered, used or are using the following AI systems:

Facial Recognition Technology

- Calgary Police Service
- Edmonton Police Service
- Halton Region Police Service
- Ottawa Police Service
- Peel Region Police Service
- RCMP
- Thunder Bay Police Service
- Toronto Police Service
- York Region Police Service

Object Recognition and Video Analytics

- RCMP
- Thunder Bay Police Service
- Toronto Police Service
- Winnipeg Police Service

Location-Based Predictive Policing

- Calgary Police Service
- Vancouver Police Service

Person-Based Predictive Policing

- Saskatoon Police Service

Automated Licence Plate Readers

- Ottawa Police Service
- RCMP
- Toronto Police Service
- Victoria Police Department

Autonomous Robots, Drones and Vehicles

- Up to 17 police services in Ontario
- RCMP
- Vancouver Police Service
- Winnipeg Police Department

Gunshot Detection

- Toronto Police Service

OSINT and Social Media Monitoring

- Calgary Police Service
- RCMP

AI-Assisted Police Reports

- Fredericton Police Service
- Ottawa Police Service
- Peel Police Service



2. Criminal AI Systems and Their Potential

Across the world, criminal justice systems are at the forefront of the adoption of AI.

AI technology is seen as particularly beneficial in policing, where many commentators see AI as transformative. For example, a 2024 EUROPOL report, *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement*, stated that:

*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.*¹⁵

This section discusses several of the most common criminal justice AI systems used in the United States, the United Kingdom and Canada.

Readers should note that this is not a definitive survey of criminal justice AI systems. It is, rather, a survey of common systems and a discussion of their purposes, potential benefits and variations. This survey incorporates the LCO's extensive international and Canadian research and the advice of many

contributors to the LCO's consultations. Most of the systems discussed in this section are police AI systems, however, AI is also being used by prosecutors, courts and others in the criminal justice system.

One preliminary observation about this survey is the incredible variety of AI systems already used in criminal justice today, with more certain to come. A second is the evident potential of the technology – under the right circumstances – to improve police investigations and increase the efficiency of police, prosecutions and criminal proceedings.

The most extensive analysis of AI deployed in the Canadian criminal justice system are reports by a team of researchers led by Professor Benjamin Perrin of the Peter A. Allard School of Law, University of British Columbia. Their main report, *AI and Policing: Research Report on the Governance and Use of Artificial Intelligence by Police in Canada* (UBC Police AI Report) was released in 2026 and is summarized in the text box “**Criminal AI in Canada**” following Section 1.5.¹⁶

In Section 3, we discuss the risks and potential harms of criminal AI systems.

Criminal AI Systems and Their Potential

Summary of Findings and Themes

- **There is a wide and growing number of AI systems being used in criminal justice. The pace of innovation and deployment is quickening.** Some technologies, such as FRT, predictive policing, and ALPRs have been deployed in many jurisdictions for many years. Other technologies, such as biometric inferencing, are emerging and could be used in criminal justice in the future. Courts are using AI to prepare judgements and may rely on AI-generated risk and assessments. Prosecutors, defence counsel and self-represented parties may use AI to draft submissions, conduct legal research, transcribe conversations, translate materials, and summarize documents.
- **The adoption of AI in the Canadian criminal justice system is slower than in many jurisdictions but is growing.** Reports suggest that several Canadian police services have piloted or deployed a range of AI systems including FRT, object recognition, location- and person-based predictive policing, automated license plate readers, drones, gunshot detection and social media monitoring.
- **The variations between and within criminal AI systems have important public safety, governance and legal consequences.** Criminal AI systems are not monolithic. For example, live facial recognition of a public street has much different investigative and legal implications than a retroactive system used to identify specific individuals.
- **Depending on how they are deployed, AI systems have significant potential to improve public safety and improve police investigations and operations.** AI systems are being used across an incredible range of police and criminal justice investigations, operations and functions. Perhaps most commonly, police AI systems are being used to:
 - Identify unknown individuals or verify their identity.
 - Track people's locations and movements.
 - Manage and analyze evidence.
 - Predict the location of future crimes or perpetrators.
 - Prepare police reports, transcribe or translate recordings.
- **AI can exponentially increase the speed, scale and number of people affected by police investigations and surveillance.** Between September 2024 and Sept 2025, the London Metropolitan Police reported scanning more than 3.1 million faces with live FRT. Similarly, the Toronto Police Service reports that its automated license plate readers can result in over 1.25 million scanned license plates every day in Toronto.¹⁷
- **The use and applications of the technology is evolving and adapting.** Many early predictive policing systems “have come and gone” in the face of experience, legal challenges or public controversies. In some cases, early systems have been superseded by more sophisticated and potentially powerful systems.

2.1 Facial Recognition and Biometric Technology

The best known AI technology in criminal justice is facial recognition technology (FRT). FRT is a form of biometrics.¹⁸ FRT compares a “faceprint” or probe image against a reference image in a database and makes a prediction about whether the images match. FRT is used to rapidly identify suspects, victims, missing persons and others.¹⁹

Many police services and governments believe FRT and biometrics have significant potential to improve public safety, police investigations and efficiency. As summarized by INTERPOL:

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... [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.²⁰

There are many types and variations of FRT. Some of the better known applications include:

- Suspect identification, where police use FRT to match photos of suspects against mugshot databases or other sources to generate leads.
- Missing person or human trafficking investigations can use FRT to scan police databases or other sources to locate missing persons or victims of human trafficking.
- Child sexual abuse investigations, where FRT is used to identify child victims within large image databases.
- Document review, where FRT is used to assist investigators review large collections of photo or video files.
- Crowd surveillance or monitoring, in which fixed or mobile cameras scan specific locations, protests, sporting events or public streets to identify suspects or persons of interest.
- Identity verification, where FRT is used to identify uncooperative or unidentified individuals.

From a public safety, legal and operational perspective, there are important issues and distinctions between FRT systems.

First, there is an important distinction between live FRT and retroactive FRT. Live FRT, or LFR, scans images from live camera feeds to identify or track individuals in real time. In contrast, retroactive FRT, or RFR, is used to identify individuals from previously recorded images or videos.

Operator-initiated facial recognition (OIFR) is a newer form of FRT. OIFR is a mobile tool where an officer takes a photograph of a person’s face using a handheld device or mobile phone to identify the person in real-time or subsequently. An early and leading case on the legality of police use of OIFR in Canada is currently before the Ontario Court of Appeal.²¹



Second, there are many types of FRT cameras. FRT probe images can be collected from:

- Closed circuit security cameras (CCTV) mounted on street furniture, lampposts or buildings.
- Drones.
- Mobile FRT vans.
- Police body cameras.
- Open internet sources.
- Images or video collected by third parties, such as private security cameras or ATMs.

Third, there are many different types of FRT reference databases, including dedicated investigative databases, mugshot databases, driver's license databases, private photo or video collections, or even images scraped off the internet.

Fourth, FRT can be used for many kinds of police work including:

- Major criminal investigations, such as terrorist threats, missing person investigations and investigations for human trafficking or child sexual abuse.
- To identify persons wanted on serious criminal warrants or persons flagged as safety risks.
- To identify persons in less serious criminal investigations or persons wanted on warrants.
- General surveillance in public, private or secure spaces.

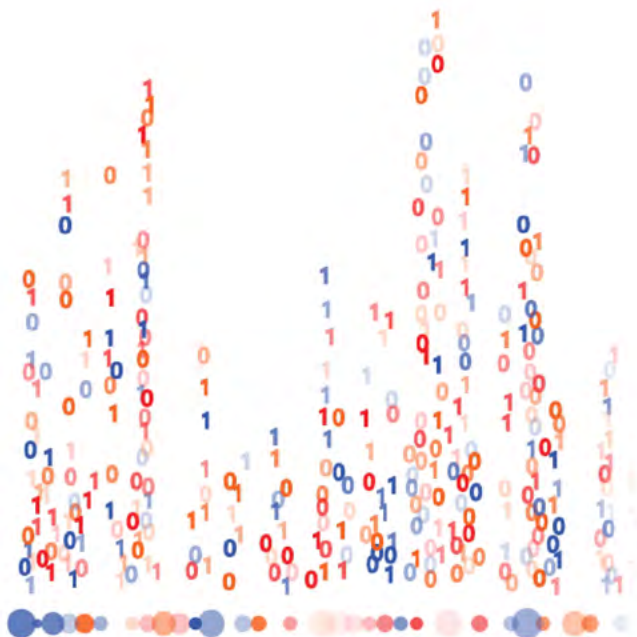
Finally, FRT can be used in a wide variety of locations, including:

- Critical infrastructure, such as courts, government buildings, airports or train stations.
- Preidentified criminal or missing person "hotspots".
- Public streets.
- Public events such as protests, parades, music festivals, and sporting events.
- Private sector locations such as banks, offices, stores or shopping malls.²²

There is an extraordinary range of FRT applications being used today in the United States, the United Kingdom and Canada. The most extensive FRT deployment may be in the UK, where a large-scale, national live FRT system is currently being implemented. (See the text box below "**How FRT is Used in the UK**" for more information). FRT is also reported to be used in some form by hundreds of law enforcement agencies in the United States.²³

The best-known example of FRT in Canada is the use of Clearview AI by the RCMP and other Canadian police services. The RCMP's use of Clearview AI became a public controversy in 2020 and was the subject of several investigations by Canadian privacy commissioners.²⁴ The RCMP has confirmed that it has stopped using Clearview AI.

Beyond the Clearview AI example, it is difficult to know police are using FRT in Canada due to the lack of mandatory disclosure of policing AI systems across Canada. The Toronto Police Service has disclosed that it uses 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)."²⁵ The UBC Police AI Report states that FRT has been used by at least five Ontario police services including Thunder Bay, York Region, Peel Region, Halton Region and Toronto.²⁶ (See the text box "**Criminal AI in Canada**" following Section 1.5 for more examples of Canadian police services use of FRT and AI generally.)



The use of FRT systems by Canadian police services is expanding. For example, both the Ottawa and Edmonton Police Services have recently announced or operationalized new FRT systems.²⁷ In 2026, the Ottawa Police Service Board approved a plan to use FRT to match police bodycam images and videos using the IDEMIA FRT and image database used by police in York, Peel, and Halton.²⁸ The Chief of Police of the Ottawa Police Service states that FRT

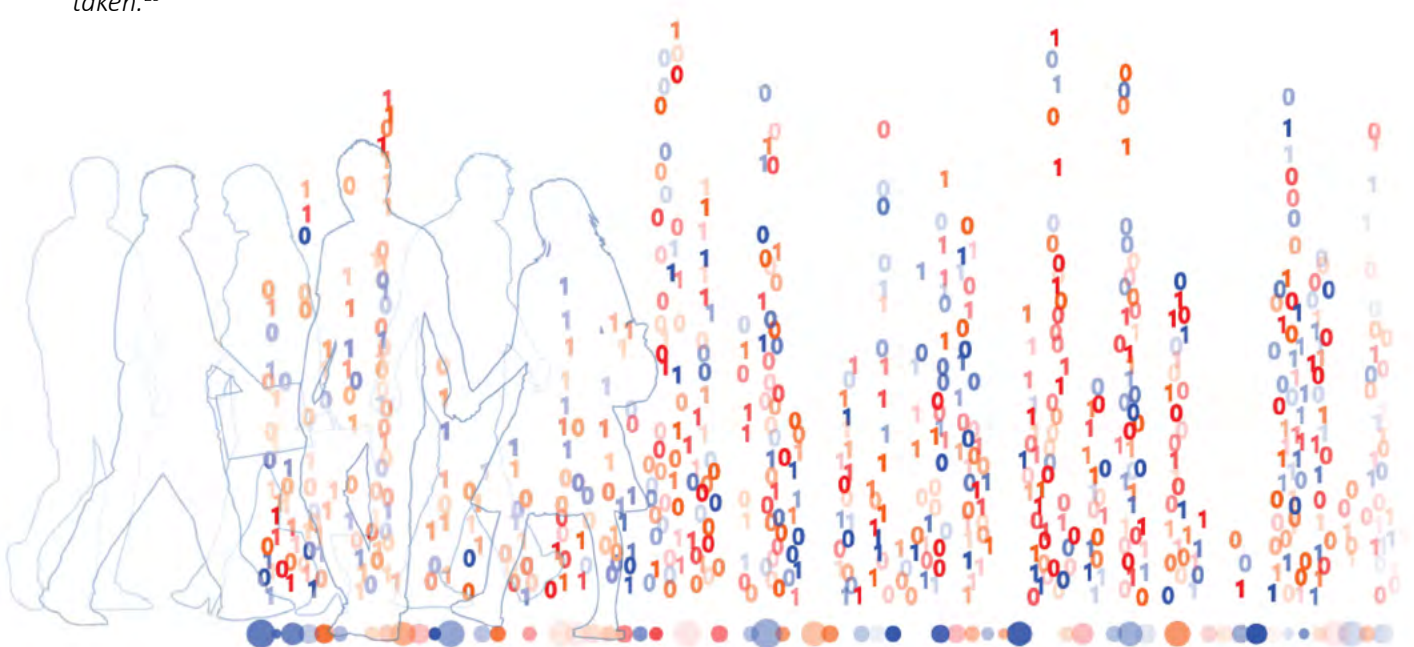
*...is an increasingly common biometric tool investigative tool by police services to help generate more investigative leads from images connected to criminal investigations, contributing to increased case solvency and enhancing public safety through more timely identification of suspects and persons of interest. FRT uses software to compare an image of an unknown person with lawfully obtained images of known individuals, such as booking photographs. Its value lies in its ability to assist investigators where traditional methods may be limited, time-consuming or unavailable. A facial recognition result does not confirm identity on its own and is not evidence by itself. Any possible match must be reviewed by trained analysts and corroborated through additional investigative steps before any enforcement action is taken.*²⁹

In Edmonton, police have begun testing body cameras equipped with FRT trained to detect the faces of about 7,000 people on a watchlist, based on mugshots of people police say have serious criminal warrants or who are flagged as potential safety risks.³⁰ The service states that

*NEC's NeoFace Reveal facial recognition solution is used by hundreds of law enforcement agencies across the world. It delivers prompt and reliable facial recognition results and works in conjunction with EPS' and Calgary Police Service's mugshot database, enabling both police services to share data securely.*³¹

According to the Edmonton Police, they “will be the first police service in the world to test Axon’s body-worn video camera recognition technology.”³²

In addition to facial recognition, other forms of biometric identification include iris recognition, automated fingerprint identification, palm-print identification, ear biometrics, gait recognition, voice recognition, and DNA analysis.³³



How FRT Is Used in the UK

The United Kingdom is an example of a widespread, national deployment of FRT. According to the UK government, police in England and Wales use three types of FRT:

- Live Facial Recognition (LFR): As of March 2026, LFR is used by 13 of the 43 police forces in England and Wales. LFR uses mounted cameras in public spaces to capture live images of passers-by. The UK also deploys LFR vans. LFR vans are mobile police units equipped with rooftop CCTV cameras that scan crowds and match faces against a specific police watchlist in real time.
- Retrospective Facial Recognition (RFR): RFR is used across UK police forces to identify suspects after a police incident. Images of a suspect are collected from sources such as CCTV, mobile phones and social media. These images are compared with reference images of known individuals in the Police National Database.
- Operator-Initiated Facial Recognition (OIFR): OIFR is a near real-time method currently used or piloted by several UK police forces. OIFR is a mobile policing tool where an officer takes a photograph of a person's face using a handheld device or mobile phone to identify them in real-time against a predetermined database or watchlist.³⁴

FRT, including LFR, is also used by several other UK government agencies. For example, LFR is currently deployed in many UK ports to support immigration enforcement. LFR is also deployed in many UK train stations³⁵ and several stations of the London Underground.³⁶

In 2025 and 2026, the UK government announced plans to expand the use of FRT nationally, including

*...a new national centre for AI in policing...which will enable the rapid and responsible adoption of AI across policing, national rollout of live facial recognition, and investment to strengthen the use of data across policing.*³⁷

In furtherance of this plan, in January 2026, the Home Office announced plans to expand FRT to every regional police force in England and Wales by purchasing 40 new LFR vans.³⁸

According to the UK government, LFR scanned 4.6 million faces across England and Wales in 2024. During the same period, RFR was used 252,798 times.³⁹ Plans to expand FRT across the UK will increase these numbers.

LFR appears to be used most extensively by the London Metropolitan Police. Between September 2025 and Sept 2025, the London Metropolitan Police reported scanning more than 3.1 million faces with live facial recognition technology.⁴⁰

The Commissioner of the Metropolitan Police Service, Sir Mark Rowley, recently stated:

*Facial recognition is one of the most revolutionary technology advances in policing in recent years. Public confidence in this is clear - around 80 per cent of Londoners support its use. That backing reflects a simple truth: it works.*⁴¹

At present, LFR in London is largely implemented through LFR camera vans deployed in pre-identified crime or missing person “hotspots.” The Metropolitan Police also use “static LFR” i.e. permanently mounted LFR-enabled CCTV cameras, located in high street areas such as Soho and the West End.⁴²



The Metropolitan Police have announced plans to expand the use of permanent cameras, LFR vans and OIFR in 2026 and 2027. In June 2026, for example, Sir Mark Rowley announced a major expansion of policing technology, including a significant expansion of AI video analytics, drones, data analytics, and live facial recognition. He stated the Metropolitan Police were “rolling out static LFR making it mainstream in central London...Next year our intention is to continue the rollout across London.”⁴³

The expansion of FRT in the UK has been rapid and controversial. Facial recognition has been described as “spiralling out of control.”⁴⁴ Many critics, including the UK’s Equality and Human Rights Commissioner, have noted the risks of privacy violations, racial bias, police harassment and the speed of FRT deployment across the UK.⁴⁵ Critics have also stated that rapid FRT deployment is proceeding in the absence of a statutory and policy framework to govern the technology.⁴⁶

The UK government concluded a consultation on police use of FRT in early 2026. In May 2026, the UK government announced plans to “Establish a new legal framework” to

... underpin law enforcement use of facial recognition and similar technologies, making it clear when use of these technologies can be justified, including creation of a single, expert regulatory body to provide independent advice and oversight. This will be world-leading and is essential for boosting public and policing confidence in the use of these innovative technologies, which has the potential to transform crime outcomes while also generating major efficiencies.”⁴⁷

Further discussion of these issues is found in Section 3.1.

2.2 ALPRs/Vehicle Surveillance Systems

Other common criminal AI systems are automated licence plate readers (ALPRs), vehicle surveillance systems and tracking algorithms.⁴⁸

ALPRs and vehicle surveillance systems use mobile or fixed cameras to detect information about vehicles, potentially including a vehicle’s license plate number and other information.⁴⁹ ALPRs have been described as “vehicle fingerprints.”⁵⁰

ALPRs can scan thousands of license plates per hour and operate significantly faster than manually inputting license plates. ALPRs are designed to assist police to quickly find stolen vehicles and unlicensed, prohibited, suspended and/or uninsured drivers. ALPRs and vehicle surveillance systems can also be used to track individuals, provide evidence, locate missing persons, or analyze patterns in criminal activity.⁵¹ Finally, ALPRs can also be used to increase security at events or facilities, and improve traffic flows.⁵²

ALPRs are deployed extensively in the US, where there are a reported 140,000 ALPRs across the country.⁵³ The text box below “**ALPRs in Los Angeles**” summarizes how ALPRs are deployed in Los Angeles where more than 210 million license plates were scanned by a network of almost 2,000 cameras in two months in 2025.⁵⁴



The widespread deployment of ALPRs in the US is very controversial and is currently the subject of a national debate about the technology. Many of these criticisms have centred on a company called Flock Safety, a leading US ALPR provider.⁵⁵ Flock Safety describes the benefits of ALPRs as follows:

Individuals planning to commit a crime also know that license plates are identifiable data points, so what happens if they steal a car or a license plate tag to commit a crime? Flock is a step ahead. Using patented Vehicle Fingerprint™ technology, the camera captures the vehicle make, color, type, license plate, state of the license plate, missing plate, covered plate, paper plate, and over 20 unique vehicle details like roof racks and bumper stickers.

So if a traditional security camera or an eyewitness saw a yellow SUV with a roof rack, a detective would use Flock to turn thousands of hours of video into the one suspect vehicle that happens to be a yellow SUV with a roof rack. Narrowing the focus to the pertinent evidence saves a tremendous amount of time and leads to a faster case clearance.

Flock Safety technology integrates with the National Crime Information Center (NCIC), to provide alerts to dispatch and patrol officers on vehicle license plates associated with outstanding warrants, missing persons, and stolen vehicles. Since stolen vehicles are often used to perpetuate more crime, and the inhabitants of those vehicles are more likely to have been involved in violent crime, a stop of a stolen vehicle as a result of a Flock alert disrupts the crime cycle by removing criminal transportation and arresting suspects.⁵⁶

It is not clear how widely ALPRs are deployed in Ontario or Canada. The Toronto Police Service states 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.”⁵⁷ The Toronto Police Service reports that its ALPRs can scan more than 1.25 million licence plates every day.⁵⁸ In 2025, the TPS reported this resulted in an 83% increase in enforcement for unattached plates and suspended drivers and located 30 missing persons.⁵⁹

The Ottawa Police Service began using ALPRs in 2016 and reports that

[ALPRs have] been an enormous help in identifying drivers who should not be on the road.

An ALPR can identify:

- Stolen licence plates
- Misuse of plates
- Driving whilst disqualified (CC)
- Driving whilst suspended (HTA)
- Unlicensed driver
- Expired validation
- Persons wanted on warrant

It can also alert officers of the presence of vehicles involved in serious crimes or wanted in instances of Amber Alerts.⁶⁰

ALPRs in Los Angeles

A July 2026 report by the Office of the Inspector General of the Los Angeles Police Commission highlighted how the Los Angeles Police Department (LAPD) uses ALPRs.⁶¹ The ALPR system in Los Angeles is extensive, including at least:

- 248 pole-mounted cameras.
- 140 cameras mounted on police vehicle roofs.
- Approximately 1,500 cameras installed inside police vehicles.
- Seven mobile trailer cameras.

The Inspector General reported the LAPD's ALPR cameras generated 210,568,103 license plate reads between August 1 and September 30, 2025, a period of just two months.

The Inspector General reported the following outcomes from in-car ALPR alerts during that period:

- 337 alerts resulting in the recovery of stolen vehicles.
- 161 alerts where subsequent investigations determined that the vehicles had not been stolen.
- 68 alerts resulting in 74 arrests.
- Nine alerts resulting in pursuits.

The Inspector General's report was very critical of the LAPD ALPR program, citing concerns about program and vendor security practices, data sharing, privacy controls, access controls, retention policies, terms of service, digital sovereignty, and auditing practices.

One of the program's three vendors was Flock Safety. Following the Inspector General's report, the LAPD announced it would not renew its contract with Flock Safety due to concerns about data sharing with federal officials, including immigration authorities.⁶²

The LAPD Inspector General report is discussed further in Section 3.1 and Section 6 at Recommendation 8, below.

2.3 Predictive Policing

Predictive policing is a generic name for police AI systems that processes and analyses large and complex datasets much more quickly than humans.⁶³ EUROPOL 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.*⁶⁴

The use of predictive policing technology has been characterized as a “technological promise” aimed at “revolutionizing law enforcement.”⁶⁵ 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.*⁶⁶

Predictive policing has many applications but is commonly understood as AI systems that try to predict or ‘forecast’ future crime. In its 2020 report, *To Surveil and Protect*, The Citizen Lab at the University of Toronto states 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.⁶⁷ Location-based systems have been used to manage police patrols, identify times and locations where specific crimes are likely to occur (“hot spots”), and identify areas where community interventions could be helpful to reduce crime.⁶⁸
- 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.⁶⁹ Person-based predictive policing has been used to predict which individuals are more likely to be involved with crime (“targeted offender lists”), to promote officer safety when responding to 911 calls, and to promote “focussed deterrence.”⁷⁰

Predictive policing has been deployed extensively across the US.⁷¹ 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.⁷²

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).⁷³

2.4 Open Source Intelligence and Social Media Intelligence

Police services can use open source intelligence (OSINT) and social media intelligence (SOCINT) “to predict crimes, track criminal networks, locate missing persons, investigate, and discover criminal activities”.⁷⁴

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.*⁷⁵

The technology has been used to:

*...seek potential evidence for a wide range of criminal activity, including white collar crime, child sexual abuse material (CSAM), drug and firearm offences, human trafficking, money laundering, and terrorism. [OSINT and social media intelligence] can help police secure public events, uncover criminal networks, and identify individuals who are becoming radicalized.*⁷⁶

2.5 Drones

According to the UBC Police AI Report,

*Use of drones for surveillance can improve officer, civilian, and suspect safety by using high-resolution cameras to monitor a situation before police arrive at a scene – allowing police to determine the presence of weapons, the behaviour of the suspect, and the safety of civilians...Response times can be much faster with drones versus humans.*⁷⁷

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

*...are used for aerial surveillance activities... 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.*⁷⁸

The RCMP also states that drones reduce the risk to police officers in certain situations by sending the technology into high risk environments.⁷⁹

Drones are reported to be used by over 1,400 US police departments.⁸⁰

A recent research report commissioned by the Information and Privacy Commissioner of Ontario estimated that 17 Ontario police services were using some form of remotely piloted aircraft systems (RPASs) or drones as of September 2024.⁸¹

2.6 AI-assisted Police Reports

AI-assisted police reports use police body-worn camera footage and dictation to provide transcripts and generate reports with the use of large language models (LLM) such as ChatGPT with additional filters, inserts and prompts. Police can fill in blanks within the report to add missing facts and edit the report before submitting a final version to police databases for recordkeeping and prosecution purposes.⁸²

According to the UBC Police AI Report,

*Writing reports and submitting narratives after police incidents and encounters are administrative tasks that take up large portions of police officers' time. Companies have claimed that AI-generated police reports can help streamline such activities allowing officers to focus on responding to calls-for-service, investigating crimes, and supporting communities.*⁸³

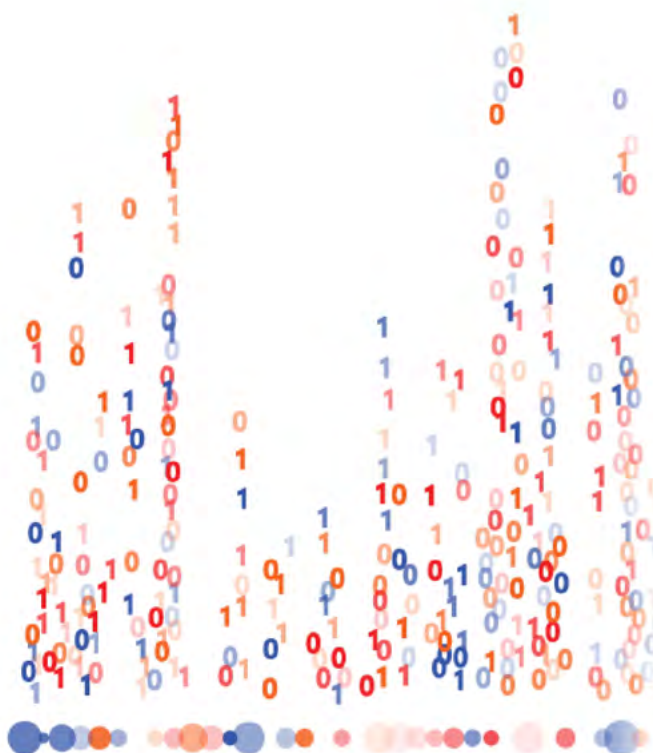
In Canada, it is not clear how many police services have used AI to assist in generating police reports. In Ontario, the Ottawa Police Service has contracted with Axon to provide automated transcription, translation and court-ready redaction.⁸⁴

2.7 Evidence Management

Police use AI to investigate complex cases with voluminous disclosure, such as mapping relationships in complex fraud and organized crime cases.

An important application of this technology relates to child sexual abuse material (CSAM). AI can detect and flag CSAM on devices or large datasets, helping police investigate crimes and locate victims quickly.⁸⁵

In Canada, the RCMP uses Griffeye, specialized software designed to assist in the categorization and classification of CSAM.⁸⁶ The RCMP states that Griffeye ingests media from seized exhibits and partner submissions, using AI-driven classifiers to identify and group potential CSAM for human review. This function is crucial for managing the immense volume of data investigators face. The RCMP states that a "single case can contain in excess of 3 million media items to review."⁸⁷



2.8 Gunshot Detection/Object Recognition

Gunshot detection systems use a network of outdoor acoustic sensors to detect and locate gunfire and alert police so they may respond faster.

ShotSpotter is the best-known gunshot detection technology. According to the company's website, more than 180 American cities use the technology as of September 2026.⁸⁸ The technology relies on thousands of microphones installed across cities to automatically detect gunshot sounds and to dispatch police.⁸⁹

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 public concerns.⁹⁰

Other AI detection systems include weapons detection systems that analyze images to detect objects that appear to be weapons, and drug detection systems that can be used to detect drugs faster.⁹¹

2.9 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.

The use of bail and sentencing algorithms expanded rapidly across the United States in the 2010s.⁹² The growth was driven largely by the American bail reform movement, the purpose of which is "end of wealth-based [bail] system and move pretrial justice systems to a risk-based model."⁹³ Algorithmic pretrial risk assessments quickly emerged as the "favored reform" towards advance these initiatives.⁹⁴

Bail and sentencing algorithms do not appear to be used in Canada.

2.10 Biometric Inferencing

The New York University Policing Project reports that U.S. policing agencies are experimenting with AI systems that analyze an individual's sentiments or emotions. Biometric inferencing are systems that "seek to categorize people and infer sensitive internal states."⁹⁵ These systems can include:

- Lie detection systems: These are systems that track eye movements and analyze micro-expressions to determine whether an individual is engaged in deception. Some systems are designed specifically for law enforcement use.
- Sentiment analysis: A natural language processing technique designed to classify individuals' sentiment as positive, negative, or neutral.
- Affective computing: This is AI that goes beyond sentiment analysis and seeks to understand and interpret specific emotions based on facial expressions, voice intonations, text, and physiological signals.

Biometric inferencing systems do not appear to be used in Canada.



2.11 Criminal Courts, Crowns and Defence Counsel

There is no comprehensive picture of how Canadian criminal courts, prosecutors or defence counsel are using AI. Nevertheless, there are several indicators suggesting AI use is accelerating among litigators in Canada's civil and criminal justice systems. For instance, the annual number of AI-related case decisions has tripled between 2021 and 2025.⁹⁶ Court decisions about the misuse of AI tools have also jumped from fewer than 10 in 2024 to 144 between January 2025 and May 2026.⁹⁷

LCO research and consultations have identified several ways in which AI is being used by courts, litigators and other justice system participants in Canada and internationally. For example:

- **Prosecutors.** According to the NYU Policing Project, prosecutors can use AI to help manage digital evidence, automate redactions, streamline document generation and analyze forensic evidence.⁹⁸ In Canada, Crown prosecutors may use a library of pre-approved Co-Pilot AI prompts to assist with drafting,⁹⁹ use AI tools to summarize and analyze voluminous disclosure materials,¹⁰⁰ or use AI to research and draft materials based on a pre-approved library of legal memos, practice directions, templates, precedents, and research.¹⁰¹
- **Courts.** Courts have used AI to aid in writing judgements;¹⁰² to assist legal research, drafting, and translation;¹⁰³ to generate transcripts;¹⁰⁴ and to help litigants complete and file forms with AI guided pathways and natural language chats.¹⁰⁵
- **Legal practice.** Lawyers and unrepresented litigants may use AI systems for legal research and writing;¹⁰⁶ to draft pleadings and submissions;¹⁰⁷ to evaluate evidence;¹⁰⁸ to test testimony;¹⁰⁹ or to summarize transcripts, analyze expert reports, prepare cross-examination, and review the status of cases.¹¹⁰
- **Risk assessment.** Risk assessments can incorporate AI-generated or AI-aided evidence such as biometric identification and “enhanced” images and video.¹¹¹ Risk assessments may also rely on medical and social services reports transcribed or summarized by AI.¹¹²

There are many other examples of AI use in criminal justice. In some US states, AI-powered legal services help people expunge their criminal records by using generative AI to draft personal statements.¹¹³ AI systems have also been used in other jurisdictions to support victims of crime.¹¹⁴ AI can also be used to improve transparency and accountability in the administration of criminal justice. For instance, researchers in the US 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.”¹¹⁵ Finally, the LCO has learned that AI tools appear to be increasing the number and sophistication of issues referred to independent police oversight agencies in Ontario.¹¹⁶

2.12 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. Other systems being used in criminal justice include emergency responses¹¹⁷, real time crime analysis¹¹⁸, post-conviction analysis¹¹⁹, digital forensics¹²⁰, police services strategic planning¹²¹, criminal record expungement¹²², victim support¹²³ and to monitor police conduct.¹²⁴



3. Criminal AI Harms and Risks

Section 2 discussed the uses and potential benefits of AI technology in the criminal justice system. This section discusses criminal AI's risks and potential harms.

The risks and potential harms of criminal AI systems were discussed at length in the LCO's Criminal AI project Issue Papers, the LCO Vancouver and Toronto Roundtable Reports, the UBC Police AI Report,¹²⁵ and several earlier LCO reports.¹²⁶ These reports and others document how AI systems present serious risks to constitutional rights, human rights, privacy, procedural protections and access to justice. These reports emphasize how criminal AI risks fall disproportionately on low-income, Indigenous, racialized, or otherwise vulnerable communities and individuals.

Over the last two years, the LCO has talked to hundreds of stakeholders and organizations across Canada and internationally about criminal AI risks and harms. We have also learned about risks from new research and the practical experience of jurisdictions, police services and other institutions that have deployed criminal AI systems. Finally, we have learned about the important and emerging governance, operational and legal risks that arise when AI systems are deployed at scale in many locations across a large jurisdiction.

We have categorized these risks into three areas:

- Legal risks.
- Governance risks.
- Administration of justice/Access to justice risks.

3.1 Legal Risks

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 procedure, criminal common law and evidence law work together to check state power, protect individual rights and promote public safety. LCO consultations confirmed broad support across criminal justice institutions on the need to develop a "made in Canada" approach to address these risks. This is the baseline for the LCO's analysis of criminal AI legal risks.

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.¹²⁷ For example, issues respecting the quality and potential bias of AI training sets ("bias in, bias out") are well-known.¹²⁸ AI bias can also intersect multiple grounds.

Criminal AI: Harms and Risks

Summary of Findings and Themes

- **Criminal AI systems such as FRT, predictive policing and ALPRs have demonstrable and serious legal risks, including human rights, privacy and procedural risks. Many of these risks are new and complex.** Notable legal risks include discrimination, surveillance, disclosure, explainability and data reliability risks. Specific systems can often present multiple risks. Due to the sheer variety of AI applications and the scale on which AI operates, these risks potentially affect far more people than traditional police investigative techniques.
- **When assessing criminal AI legal risks, it is important to account for the variations within and between criminal AI systems.** Not all criminal AI systems present the same risks. For example, surveillance risks are present in all FRT systems, but their scope and impact depend on how the system is deployed. Mitigating criminal AI risks depends on a complex series of technical, operational, policy, governance and legal choices.
- **Criminal AI systems create important access to justice and administration of justice risks.** Criminal defendants will not have the resources to challenge AI in criminal proceedings. The result could be worsening the over-representation of low-income and racialized communities in the criminal justice system. Nor will courts have the resources or mandate to address many of the systemic legal issues raised by criminal AI evidence.
- **Risks will compound and grow as more institutions adopt criminal AI systems across Ontario.** The risks of inconsistent and fragmented AI deployments, governance standards and legal protections will grow as more criminal justice institutions adopt AI. Many police services, courts, Crowns, legal aid services, and regulators will be challenged to develop responsible AI policies and coordinate systems across dozens of jurisdictions.
- **There is a risk that existing criminal AI systems or emerging technologies will outpace regulation.** Criminal AI systems may be widely deployed before a comprehensive responsible AI framework is established. If so, systemic harms may become commonplace.
- **The potential consequences and harms of criminal AI risks are serious and far-reaching.** Potential consequences include:
 - o Insufficient or inadequate protection of rights.
 - o Increased risks of false arrests, surveillance violations and worsening over-representation of low-income and racialized communities in criminal justice.
 - o A fragmented legal and regulatory landscape.
 - o Inconsistent deployment of technology.
 - o Financial and administrative inefficiencies.
 - o Hampering innovation.
 - o Reduced legal and public accountability.
 - o Undermining public trust in criminal justice AI systems.

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.*¹²⁹

Concerns about FRT bias are the foundation for many proposals to strictly regulate police FRT systems.¹³⁰ Many advocates believe that FRT bias is conclusive proof that FRT systems should be banned in whole or in part.¹³¹ Others believe that FRT bias is a diminishing issue and that better training data or systems can mitigate errors.¹³²

This debate is currently occurring in the UK. In a recent report, the London Metropolitan Police stated that the UK National Physical Laboratories has found the Met's live FRT systems to be "accurate and balanced with regard to ethnicity and gender."¹³³ This view has been challenged by many, including by researchers from PROBABLE Futures, a UK AI research organization, who state that NPL testing has many "omissions."¹³⁴ Notably, the UK National Physical Laboratory study was relied upon by the Ottawa police service to support its recent Facial Recognition Initiative.¹³⁵

Many predictive policing systems have also been proven to be biased and discriminatory.¹³⁶ The Ontario Human Rights Commission (OHRC) has stated that 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."¹³⁷ However, "the opposite can happen when predictive policing is used improperly."¹³⁸

Concerns about biased predictive policing have led to the withdrawal of many systems in the face of legal challenges and public outcry.¹³⁹ There have also been significant bias concerns raised about several other criminal AI systems, especially bail/sentencing algorithms.¹⁴⁰

Privacy and Surveillance

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

*Should a policing FRT system enable members 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.*¹⁴¹

Two recent reports by Canadian Privacy Commissioners, *Police use of Facial Recognition Technology in Canada and the Way Forward*¹⁴² and *Facial Recognition and Mugshot Databases: Guidance for Police in Ontario*,¹⁴³ describe the privacy risks of police FRT comprehensively. The use and risks of FRT were also discussed extensively at the LCO's Vancouver Roundtable.¹⁴⁴

Privacy and surveillance risks can vary widely depending on how FRT systems are used. For example, surveillance risks are present in all FRT systems, but the scope of that risk largely depends on how and where FRT images are collected and what database they are compared to. A live FRT system monitoring a public protest has more serious constitutional and privacy risks than a retrospective FRT system comparing a suspect to a mugshot database.

The deployment of FRT in the UK example is an important illustration of the privacy risks of FRT deployed at scale. In the UK, police services have used a combination of live FRT vans and static LFR to surveil millions of people, including more than 3M in London in a single year.¹⁴⁵ LFR cameras and mobile FRT vans have surveilled people in criminal "hot spots", in major shopping districts, on trains and subways, at sporting events and music festivals, and more.¹⁴⁶

The UK police are also piloting Operator Initiated Facial Recognition (OIFR), in which police officers use handheld devices or mobile phones to identify individuals in real-time against a predetermined database or watchlist. A civil liberties advocate in the UK has stated:

Placing a tool in the hand of officers which can lift the veil of anonymity in public in a matter of seconds by simply pointing a phone at a face is a disaster for civil liberties...[the technology could be used to]...unlock a vast array of personal records.¹⁴⁷

Canadian criminal AI systems are not immune from privacy and surveillance criticisms. The RCMP's use of Clearview AI and the Toronto Police Service's AI have both been criticized on these grounds.¹⁴⁸ More recently, there has been strong criticism of the Edmonton Police Service's piloting of body cameras equipped with FRT trained to detect the faces of about 7,000 people who police say have serious criminal warrants or have been flagged as potential safety risks.¹⁴⁹ Kate Robertson, a senior research associate with Citizen's Lab, has stated:

As someone who has been studying algorithmic policing technologies for nearly a decade, and [previously] a lawyer in Canada's justice system, I have to say that this is likely the most high risk algorithmic surveillance program that I have observed to date in Canada.¹⁵⁰

In Canada, the Office of the Privacy Commissioner of Canada (OPC) and Information and Privacy Commissioner of Ontario (IPC) have issued multiple comprehensive reports on the privacy and surveillance risks of FRT, licence plate readers, and drones.¹⁵¹

R. v. Bykovets

Courts in Canada are showing sensitivity to the surveillance power of online information in the hands of law enforcement. The 2024 Supreme Court of Canada decision *R. v. Bykovets* confirmed that, in an increasingly digital age, even routine IP internet addresses can create "the crucial link between an Internet user and their online activity... [and] ultimately, their identity..."¹⁵² The Court concluded the power of this technology is sufficient to attract *Charter of Rights* s. 8 protections to a reasonable expectation of privacy and against unreasonable search and seizure.¹⁵³

FRT is not the only criminal AI system raising privacy and surveillance concerns. ALPRs in particular have been the source of major privacy and data sharing controversies in the United States.

The use of ALPRs in the United States is widespread. As noted earlier, DeFlock reports that more than 140,000 licence plate readers have been mapped in the US.¹⁵⁴ ALPRs have been heavily criticized for privacy violations, for promoting mass surveillance, for ineffectiveness, for promoting systemic racism in policing and for unauthorized data sharing with federal officials, including immigration authorities.¹⁵⁵

The 2026 LAPD Inspector General audit report also identified several other criticisms of the LAPD's use of ALPRs, including concerns about program and vendor security practices, data sharing, privacy controls, access controls, retention policies, terms of service, digital sovereignty, and auditing practices.¹⁵⁶

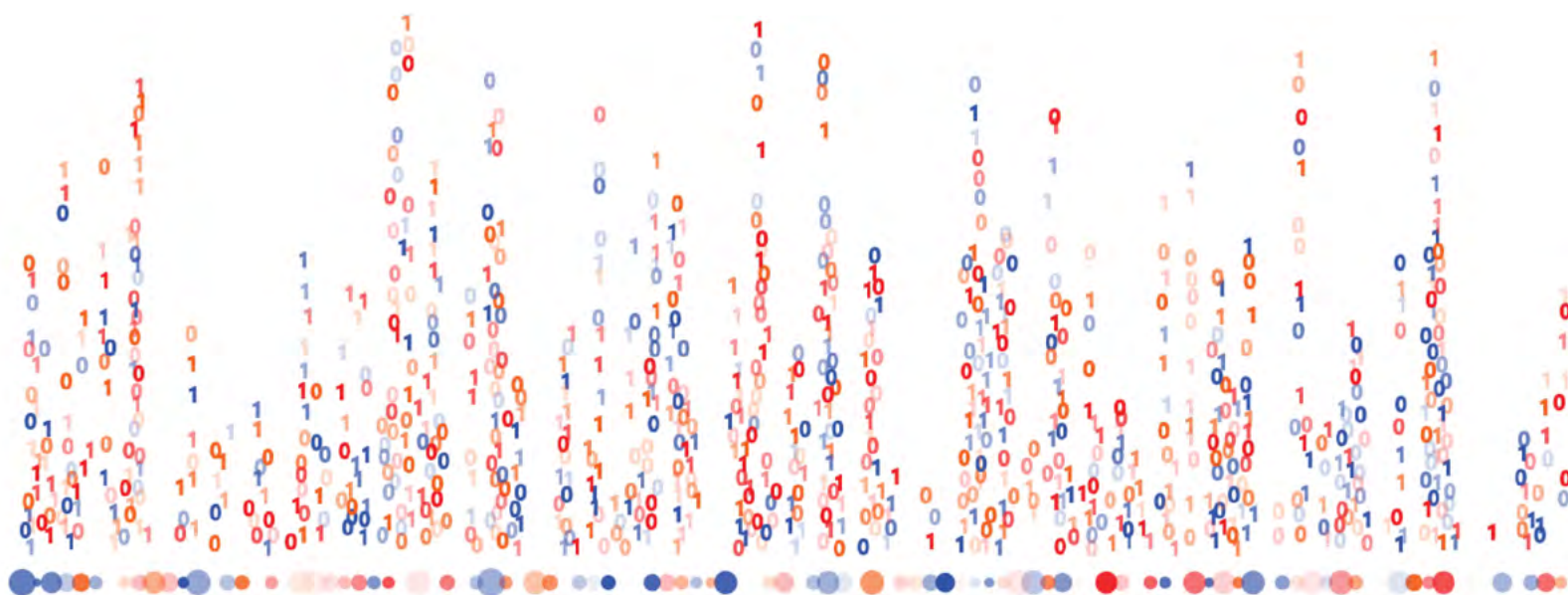
The American Flock camera debate is discussed in more detail in Section 4.1.

Police use of drones also raises important privacy and surveillance issues. The Information and Privacy Commissioner of Ontario released a report in August 2026, *Guidance on Police Use of Remotely Piloted Aircraft Systems (Drones) in Ontario*, which noted:

*The use of drones by police can raise significant legal, privacy, and ethical challenges for a range of reasons, including their ability to operate unnoticed by individuals, cover larger distances, and stream or record imagery from mobile overhead vantage points with increasing accuracy. These enhanced capabilities can amplify public surveillance risks and the potential overcollection of personal information. Related concerns include lack of sufficient notice to the public about the operation of drones, the ability of drones to record individuals in locations that are considered private venues (e.g., on private property) and their ability to capture a large number of people when intending to monitor a single individual amongst a crowd. Individuals have a diminished, but nonetheless, reasonable expectation of privacy in public spaces, and these risks can impose a chilling effect on public behaviour if individuals feel constrained from exercising their rights or participating in public life due to the possibility of aerial police surveillance.*¹⁵⁷

FRT, ALPRs and drones have been the most prominent AI technologies criticized on privacy and surveillance grounds, but not the only ones. The UBC Police AI Report, the NYU Policing Project and the Brennan Center for Justice, a US law and policy institute, describe the privacy risks of other technologies as follows:

Video Analytics	Video analytics allow for persistent surveillance as individuals move throughout a jurisdiction, 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. ¹⁵⁸



How AI Can Supercharge Mass Surveillance: Examples from the US

A recent US study has concluded that AI systems can “supercharge mass surveillance” by linking together otherwise obscure pieces of personal data together.¹⁵⁹ The study concluded that while judicial authorization may be required to search location data on a personal phone, US law enforcement has the ability to buy bulk data from brokers and circumvent the need for warrants and other authorizations. Even ostensibly anonymized data is easily deanonymized by AI.¹⁶⁰

Other studies have “shown that LLMs [Large Language Models] can match pseudonymous forum accounts to LinkedIn profiles; identify writers’ native languages; isolate potentially identifying information from a user’s online post history; and infer social media users’ psychological traits, locations, incomes, sexes, and ages, among other attributes.”¹⁶¹

American studies have shown how AI can mesh different surveillance technologies together. A recent US investigation showed how “Biometric trackers, cellphone location databases and drones are among the surveillance technologies that federal [ICE] agents are tapping in their deportation campaign.”¹⁶² Similarly, drones equipped with “a “Gorgon Stare” system of hundreds of cameras that can track everything that moves across 40 square miles in high definition.”¹⁶³

Finally, lawful individuals may not escape detection and the fear that comes with a risk of prosecution. For instance, it was recently revealed that a police officer in Texas – where almost all abortions are illegal – tapped into a live national ALPR network to track the movements of a woman who drove out of state and correlated her location to a known facility specializing in women’s health care in a state where abortion is legal.¹⁶⁴ Civil rights advocates note the chilling effect this has on rights, given how the “invasion of privacy increases people’s fear.”¹⁶⁵

Disclosure and Transparency

An enduring criticism of AI systems, including criminal AI systems, has been their lack of disclosure and transparency.¹⁶⁶ Disclosure and transparency are fundamental elements of legal and public accountability, especially in the context of criminal prosecutions.¹⁶⁷

AI disclosure and transparency concerns can arise in two ways. Criminal AI systems have been criticized on both grounds.¹⁶⁸

- 1) *Lack of transparency or public disclosure about the existence of an AI system, including lack of disclosure about key elements of the system and how the system makes decisions.*

There have been many public controversies about the lack of public disclosure of FRT and predictive policing systems, leading to accusations in many jurisdictions of secret surveillance or lack of consent. For example, the International Network of Civil Rights Organizations has stated that:

*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. This is a point of critical importance when we consider the use of FRT by police, as some uses of FRT could amount to covert and/or sustained mass surveillance.*¹⁶⁹

2) *Lack of disclosure to an accused during an investigation or prosecution.*

There have been criticisms of police services and other institutions for their failure to disclose their use of AI in individual investigations. A recent Washington Post investigation concluded that “police seldom disclose use of facial recognition despite false arrests... [while] and many defendants were unaware of the technology’s role in linking them to crimes”.¹⁷⁰ The investigation described the scope of the problem:

Hundreds of Americans have been arrested after being connected to a crime by facial recognition software... but many never know it because police seldom disclose their use of the controversial technology.

Police departments in 15 states provided The Post with rarely seen records documenting their use of facial recognition in more than 1,000 criminal investigations over the past four years. According to the arrest reports in those cases and interviews with people who were arrested, authorities routinely failed to inform defendants about their use of the software — denying them the opportunity to contest the results of an emerging technology that is prone to error, especially when identifying people of color.

*In fact, the records show that officers often obscured their reliance on the software in public-facing reports, saying that they identified suspects “through investigative means” or that a human source such as a witness or police officer made the initial identification.*¹⁷¹

Transparency and disclosure criticisms are widely acknowledged across the criminal justice system. As a result, governments and criminal justice institutions in the US, UK and Canada have prioritized AI disclosure and transparency as fundamental governance principles.

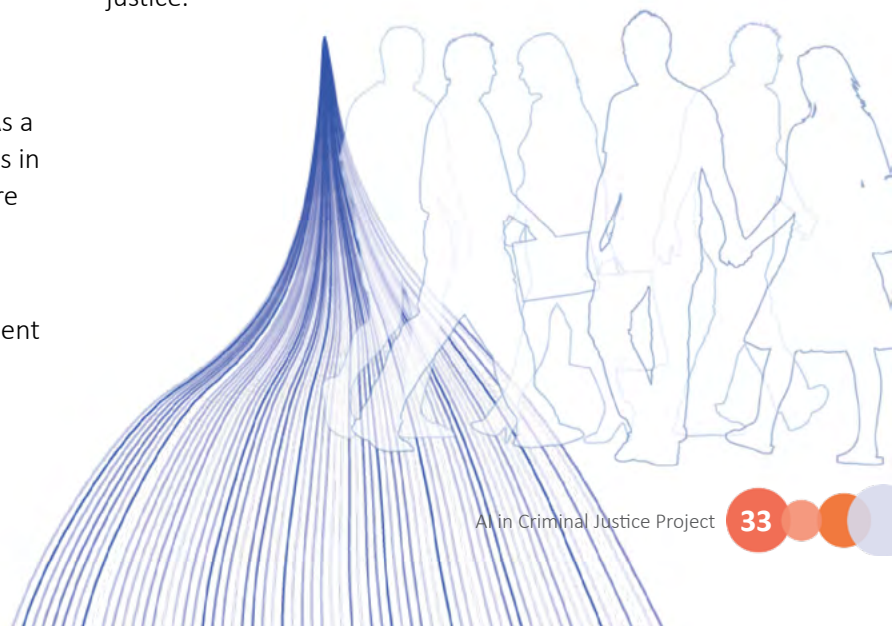
The RCMP’s use of Clearview AI is the most prominent Canadian criminal AI transparency controversy.¹⁷²

In Canada, there is limited disclosure of criminal AI justice systems. Notably, both the RCMP and Toronto Police Service have committed to publicly disclosing at least some of their AI systems. As of August 2026, the Government of Canada AI Register includes 14 RCMP AI systems.¹⁷³ The RCMP also publishes an online *Transparency Blueprint: Snapshot of Operational Technologies* that includes descriptions and operational details of many AI technologies.¹⁷⁴ The Toronto Police Service’s AI systems are published pursuant to the Toronto Police Service Board’s “Use of AI Policy.”¹⁷⁵ As of August 2026, the disclosure listed six technologies.

The federal Office of the Privacy Commissioner of Canada’s (OPC) *Privacy guidance on facial recognition for police agencies* includes detailed recommendations for disclosing FRT systems to both the general public and individuals who may be affected.¹⁷⁶ The Information and Privacy Commissioner of Ontario’s *Facial Recognition and Mugshot Databases: Guidance for Police in Ontario* includes similar recommendations.¹⁷⁷

Explainability and 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.”¹⁷⁸ 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.¹⁷⁹



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.¹⁸⁰ FRT and predictive policing systems in particular have been subject to strident criticisms of their training data.¹⁸¹ These concerns have led to many proposals to continuously test and evaluate the data used to train criminal AI systems.¹⁸²

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.”¹⁸³ 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.¹⁸⁴

For many advocates, data accuracy, reliability and validity issues suggest the need for extensive testing and monitoring of criminal AI data, including the need to test AI technologies in real-life contexts. After reviewing the claims and evidence of police AI testing, the UBC AI & Criminal Justice Project conclude

*There is striking little independent evidence demonstrating that many police AI technologies are accurate, reliable, effective or necessary. Despite widespread claims of efficiency and objectivity, significant concerns remain over documented error rates, bias amplification, and false positives. However, there is some evidence that some AI tools have led to public safety and efficiency gains, and have demonstrated improvements under controlled conditions as technology improves. As a result, a high degree of skepticism and caution is needed in approaching any AI policing technology.*¹⁸⁵

3.2 Governance Risks

In addition to legal risks, the LCO’s research and consultations have revealed that criminal AI systems create important governance risks in Ontario.

Governance risks arise in two ways: First, there will be a multiplicity of laws, regulators and institutions governing or deploying AI criminal justice in Ontario, resulting in what the Ada Lovelace Institute in the UK has called the “diffused” risks of decentralized AI governance.¹⁸⁶ Second, there are AI governance risks within each criminal justice institution.

Decentralized Governance Risks

During our consultations, the LCO consistently heard about the risks of decentralized and fragmented criminal AI governance. These risks arise for two reasons.

First, there are an extraordinary number and range of laws and regulators governing AI systems in Ontario’s criminal justice system, including:

- The *Charter of Rights and Freedoms*.
- The *Criminal Code of Canada*.
- Human rights and privacy law.
- Evidence law, procedural rules, common law rules and related statutes.
- Federal and provincial AI regulations, directives or policies.
- Canadian law enforcement AI policies.
- Policies or guidance from police boards, the provincial Law Enforcement Complaints Agency and the Inspector General for Policing.
- AI decisions, policies or guidance from courts, privacy commissions, human rights commissions, law societies and others.

Second, there is a 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.

It is easy to see how the combination of multiple laws, multiple actors/institutions and complex technologies could result in ad hoc, inconsistent or improper governance of criminal AI systems.

The Edmonton Police Service example demonstrates the risk of decentralized governance. As noted, the Edmonton Police Service has begun testing body cameras equipped with FRT trained to detect the faces of about 7,000 people on a dedicated watchlist.¹⁸⁷ This has been described as the highest risk algorithmic surveillance program in Canada.¹⁸⁸ In comparison, the RCMP, Canada's national police service, "specifically forbids the use of body-worn video for any biometric analysis, including facial recognition." The RCMP policy also forbids the use of body-worn camera for surveillance purposes or covert recording.¹⁸⁹ The contrast between the Edmonton Police Service's FRT-enabled body cameras and the RCMP is stark and consequential.

The Edmonton Police Service/RCMP contrast is actually a comparatively simple example of the "diffusion" risks of FRT deployment and governance. Consider the many complex and far-reaching issues and choices involved in criminal FRT systems, including but not limited to:

- Live, retroactive or "officer-based" FRT?
- Mass surveillance, criminal "hotspot" surveillance or targeted surveillance?
- FRT to support suspect identification for "serious" criminals, CSAM investigations or outstanding warrants?
- Static FRT cameras, mobile FRT cameras, body cameras, third party cameras or internet images?
- Dedicated investigative databases, mugshot databases, driver's license or other government databases, private photo or video collections, or internet images?
- How and what to disclose and publicly report?
- What "guardrails" to impose?
- FRT training and oversight standards?
- Privacy and bias standards?
- Evidential disclosure, onus and admissibility rules?

Each of these choices has important implications for public safety, legal rights and public trust. Absent a comprehensive approach, the LCO and project stakeholders are concerned that AI risks and harms will be compounded and pervasive in the wide, diverse and decentralized network of institutions and actors who will be deploying, litigating or overseeing AI in Canada's and Ontario's criminal justice system.

Institutional Governance Risks

In addition to the legal and decentralized governance risks described above, the LCO frequently heard about the risks and challenges of deploying or governing AI within police services and other criminal justice institutions. For example, police services often described the comprehensive efforts needed to embed responsible AI practices in their organizations, including but not limited to internal policies and resources dedicated to:

- Legal compliance.
- Procurement.
- AI assessments.
- Training.
- Human oversight.
- Data reliability and validity.
- Digital and data sovereignty, security and retention.
- Evidence management.
- Evaluation.
- Pilot projects and regulatory sandboxes.
- Internal governance and reporting.
- Public engagement and reporting.

Needless to say, these are complicated and expensive tasks, potentially out of reach for all but the largest and best resourced criminal justice institutions.

LCO consultations and research revealed sophisticated efforts within and between many Canadian police organizations to address these institutional issues proactively, including impressive initiatives by the RCMP, TPS and Canadian Association of Chiefs of Police (CACP).

This approach, while commendable, also brings many risks and inefficiencies. For example, we frequently heard of the need to develop common, or at least consistent, criminal AI impact assessment, compliance and procurement policies. Many consultees noted that it felt like many institutions were trying to solve the same problem at the same time. The LCO often heard it would be helpful if police services could purchase AI systems that were “certified” or pre-tested by a centralized authority to meet requirements for legal compliance, reliability and validity, human rights, bias and privacy.

3.3 Administration of Justice and Access to Justice Risks

The legal and governance risks described above can create complex new administration of justice and access to justice risks.

These risks are demonstrated by the well-known 2016 Wisconsin state court decision, *State v. Loomis*.¹⁹⁰

In *Loomis*, a defendant from La Crosse County, Wisconsin challenged the use of a risk assessment tool called COMPAS. COMPAS had been used by Wisconsin since 2006 and was not subject to any legislative provisions, regulations or dedicated rules of practice. After Loomis pled guilty, the court requested a pre-sentence investigation report, which included a risk score calculated using COMPAS. COMPAS identified Loomis as high risk for three types of recidivism.

Loomis ultimately received a six-year prison sentence. The sentencing judge told Loomis, “The risk assessment tools that have been utilized suggest that you’re extremely high risk to reoffend.” Loomis challenged his sentence on due process grounds, arguing that the judge’s use of the risk assessment score violated his constitutional right to a fair trial.¹⁹¹ The decision in *Loomis* has been both complimented and criticized.

Loomis demonstrates how “regulation by litigation” can create important administration of justice and access to justice risks.

First, it is not clear that courts alone have the capacity or tools to address the *systemic* statistical, technical, policy and legal issues that arise in cases like *Loomis*. This is for several reasons:

- Courts’ potential inability to assess complex technical and statistical evidence.
- Courts’ potential inability to assess AI “black box” decision-making.
- The legal issues and implications of AI systems can vary significantly even within the same class of technology, such as FRT or ALPRs.
- An AI system may change dynamically as the system is updated with new data or code. This situation may limit the precedential value of a court decision if the AI system is significantly different at the time a decision is released.
- Courts might be required to develop legal standards for each technology or application on a case-by-case basis, resulting in inconsistent judgements, judicial inefficiencies and harm to criminal defendants.

Second, *Loomis* demonstrates the difficulty of *defending* a prosecution that includes AI evidence. This issue was discussed in the LCO’s American Lessons Paper extensively, where we emphasized the enormous practical burden placed on courts and individual defendants wishing to challenge bail or sentencing decisions based in part on AI or algorithmic tools.¹⁹²

It is inconceivable that *Loomis* or any other criminal defendant (particularly one represented legal aid-funded counsel or self-represented) would be in a position to mount an effective challenge to the complex statistical, technical and legal issues raised by a tool like COMPAS, especially in the context of a bail or sentencing hearing.

The legal and social implications of administration of justice and access to justice risks are worrisome. It is possible that only the best-resourced litigants will be able to challenge criminal AI systems. As a result, criminal AI systems could add significant new barriers to low-income, marginalized, Indigenous and racialized communities, thus compounding the over-representation of these communities in Ontario’s justice system.

The LCO is not diminishing the role or importance of litigation in holding criminal AI systems to account and protecting defendant’s rights. Many issues will always be best addressed in open court with the benefit of an evidential record and high-quality and experienced counsel. Our conclusion, rather, is that legal accountability in criminal proceedings depend on both general regulation of AI *systems* and a dedicated procedural and evidential rules and supports that will allow defendants to effectively protect their rights in *individual cases* or prosecutions.



4. Responsible Criminal AI

Section 4 reviews legal and policy approaches to responsible criminal AI internationally and in Canada. Section 4.1 is a survey of important initiatives in Europe, the United States and the United Kingdom. Section 4.2 reviews Canadian responsible criminal AI initiatives. Section 5 summarizes the strengths, gaps and opportunities to develop a comprehensive responsible AI framework in Canada.

4.1 International

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.¹⁹³ This acknowledgement has led to an extraordinary range of “trustworthy” or “responsible” criminal AI laws, policies, frameworks and related initiatives based on the principle that criminal AI’s benefits depend on dedicated and sophisticated rules to minimize risks and harms.¹⁹⁴

The substance and form of these initiatives vary significantly. Their overarching theme, however, is that consistent and comprehensive criminal AI governance is needed, potentially including:

- Mandatory public disclosure of criminal AI systems including public “AI registers.”
- Prohibitions on highest risk criminal AI systems.
- Criteria to identify prohibited, high risk and limited-risk systems.
- Purpose and use limitations.
- Mandatory and transparent AI risk and impact assessments.
- Mitigation requirements.
- Mandatory obligations to measure, correct and audit bias.
- Procedural and evidential protections.
- Mandatory “human in the loop” requirements and training.
- Mandatory auditing and evaluation requirements.
- Defined pilot project and “sandboxing” evaluation procedures.
- Independent oversight of individual systems and criminal AI systems.

This section reviews major responsible AI initiatives in Europe, the US and the UK. These initiatives include framework legislation, technology specific laws and policies, police policies and model statutes. The LCO believes Canadian policymakers can learn valuable lessons from these jurisdictions.

Readers will note there are often important differences between the governance frameworks in these jurisdictions. Most obviously, live facial recognition is permitted in the United Kingdom,

while it is largely prohibited in Europe and other jurisdictions. These distinctions are significant. Nevertheless, there are more common features than differences, including a consistent acknowledgement of the importance of AI system disclosure, risk management, impact assessments, human oversight, auditing and legal and public accountability. Many of these jurisdictions have also deployed criminal AI systems widely and have encountered many of the issues that will likely arise in Ontario and Canada.

Responsible Criminal AI – International Summary of Findings and Themes

- **The potential benefits, risks, and harms of AI in criminal justice are widely documented and acknowledged in Europe, the United States and the United Kingdom.**
- **There are an extraordinary range of “trustworthy” or “responsible” criminal AI laws, policies, frameworks and other initiatives based on the principle that promoting criminal AI’s benefits depends on dedicated and sophisticated rules to minimize risks and harms.**
- **The substance and form of these initiatives vary significantly but there are consistent themes and principles.** Depending on the jurisdiction or system, responsible AI governance can include:
 - o Mandatory public disclosure of criminal AI systems.
 - o Risk assessment criteria and impact assessments.
 - o Purpose and use limitations.
 - o Bias mitigation and procedural requirements.
 - o Mandatory obligations to measure, correct and audit bias.
 - o Mandatory “human in the loop”.
 - o Mandatory auditing and evaluation requirements.
 - o Independent oversight of individual systems and government AI generally.
- **The most important international AI governance statute is the European Union’s *Artificial Intelligence Act (EU AI Act)*.** The EU AI Act establishes a comprehensive risk management and governance regime for criminal AI systems, including prohibitions for live police FRT and predictive policing. The Act also creates procedural and oversight requirements for other systems.
- **The United States has seen the broadest range of criminal AI deployments, controversies and governance initiatives.** Statutes governing police use of FRT are common, with more than 30 state or local statutes prohibiting or limiting its use. There are also many state and local statutes and policies governing bail and sentencing algorithms, predictive policing, drones, ALPRs and gunshot detection.
- **There is a currently a national controversy across the US regarding ALPRs.** ALPRs are deployed widely across the US. “Flock” cameras have been heavily criticized for privacy violations, for promoting mass surveillance, for promoting systemic racism, and for unauthorized data sharing. In response, reports suggest that more than 150 cities have cancelled ALPR contracts or deactivated cameras.
- **The UK government has announced a national strategy to implement and govern police AI systems, including a national AI policing agency and national governance legislation.**

The European Union Artificial Intelligence Act

The most important international AI governance statute is the European Union's *Artificial Intelligence Act* (EU AI Act).¹⁹⁵ The EU AI Act is sweeping, framework legislation governing the development and use of AI systems across the EU, including systems used in both the private and public sector. The EU AI Act is the most sophisticated legislative responsible criminal AI regime in the world today.

Chapter II, Article 5 of the EU AI Act sets out several “unacceptable risks” and prohibitions on specified AI systems, including two systems 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.¹⁹⁶ This prohibition is subject to several exceptions. For example, the EU AI Act allows real time remote biometric surveillance if law enforcement agencies are:

- Searching for missing persons, victims of abductions, human trafficking or sexual exploitation.
- Preventing a substantial and imminent threat to life, or foreseeable terrorist attack.
- Identifying suspects in serious crimes.

In these circumstances, the EU AI Act explicitly requires completing a fundamental rights impact assessment;¹⁹⁷ judicial or administrative authorization;¹⁹⁸ and registration in an EU database.¹⁹⁹

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.²⁰⁰ This prohibition also has exceptions.²⁰¹

Article III of the EU AI Act also pre-emptively defines several criminal AI systems as “high risk”, including bail and sentencing algorithms and AI-generated evidence in criminal trials.²⁰² In the event police or governments deploy these systems, the EU AI Act requires:

- 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.²⁰³

United States

Unlike the EU, there is no single statute or framework governing criminal AI systems in the United States. That said, the United States has seen the broadest range of criminal AI deployments, controversies and governance initiatives.

US Federal Government

The US federal government has seen dramatic shifts in responsible criminal AI rules and policies.

In October 2023, the Biden Administration issued Executive Order 14110 on “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.”²⁰⁴ This lengthy policy sets out detailed requirements for US federal departments and agencies using AI. This Order was followed in March 2024 with an Office of Management and Budget guidance (Memorandum M-24-10) on the management of AI systems and applications used by federal agencies. This guidance included detailed responsible AI requirements for “rights-impacting”

AI systems used by U.S. departments and agencies covered by the Executive Order²⁰⁵, including obligations 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.²⁰⁶

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],²⁰⁷ including no fewer than 18 systems potentially used in criminal justice, including biometric identification, predictive policing, ALPRs, gunshot detection, social media monitoring, and others.²⁰⁸ Executive Order 14110 and Memorandum M-24-10 established a comprehensive responsible AI framework.

In January 2025, both Executive Order 14110 and Memorandum M-24-10 were rescinded by the Trump administration.²⁰⁹

State and Local Initiatives

There have been dozens of U.S. state and local statutes and policies governing AI systems, including AI used in law enforcement. The website AI Law by State reports that more than 240 bills or statutes governing police FRT, body cameras, video analytics, predictive policing and drones have been introduced since 2020.²¹⁰

Statutes governing police use of FRT in the United States are common, with more than 30 state or municipal statutes prohibiting or limiting the use of FRT as of August 2026.²¹¹ There are also state and local statutes and policies governing predictive policing,²¹² gunshot detection,²¹³ drones and license plate readers.²¹⁴

The range of FRT statutes and laws is very wide.

Many US states, cities and counties limit FRT use to specific use cases and require extensive accountability mechanisms. Approaches include:

- Outright bans.
- Warrant, probable cause or court order requirements.
- Serious crime limits.
- Bans on the use of FRT with body cameras.
- Requirements to provide defendants with notice of FRT use by law enforcement.
- Reporting requirements.
- “No sole basis” rules i.e. FRT cannot be the sole basis for an arrest.²¹⁵

Drone regulation is also common. Some research suggests as many as 18 US states have passed legislation requiring law enforcement agencies to obtain a search warrant to use drones for surveillance or to conduct a search.²¹⁶ Ohio Bill 251 is a recent example. This law comes into effect in October 2026 and specifies when agencies need warrants, circumstances allowing warrantless surveillance and the documentation required for surveillance flights.²¹⁷ The City of Cleveland has actually gone further. The Cleveland Community Police Commission has approved a policy that bans the use of police drones “for conducting surveillance of individuals or groups within large gatherings or for crowd control”, subject to limited exceptions.²¹⁸ This policy also states that drones “shall not be equipped” with “facial recognition or gait analysis.”²¹⁹

There are also many American criminal AI police policies and helpful American models for proposed criminal AI legislation.²²⁰ Interesting examples include the New York City Police Department FRT policy²²¹, the LAPD FRT policy,²²² and the New York University (NYU) Policing Project’s model statutes for FRT²²³, police disclosure²²⁴ and ALPRs.²²⁵

FRT Regulation in the United States

The AINow Institute, an American research organization, published an overview of U.S. facial recognition legislation in 2020.²²⁶ The report states that “[In the US, there] 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.”²²⁷

AINow states there are three approaches to regulating FRT in the U.S., including bans, temporary or directive moratoria and regulatory bills.²²⁸ Common elements of regulatory bills include:

- Establishing a Task Force or Working Group.
- Requirements on companies, including bias testing and data access.
- Accountability and transparency reports.
- Process regulations, including officer training, reviews and 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.²²⁹



The Flock Controversy

There is currently a national controversy in the United States regarding ALPRs.

ALPRs are deployed widely in the United States. DeFlock, an open-source mapping project, reports that more than 140,000 licence plate readers have been mapped in the US.²³⁰ The pushback against “Flock” cameras (named after a company called Flock Safety, a leading US ALPR provider) has been swift, bipartisan and decisive.

ALPRs have been heavily criticized for privacy violations, for promoting mass surveillance, for ineffectiveness, for promoting systemic racism in policing and for unauthorized data sharing with federal officials, including immigration authorities.²³¹

The American Civil Liberties Union, in a report titled “You Are Being Tracked” stated:

*The information captured by the readers – including the license plate number, and the date, time, and location of every scan – is being collected and sometimes pooled into regional sharing systems. As a result, enormous databases of innocent motorists’ location information are growing rapidly. This information is often retained for years or even indefinitely, with few or no restrictions to protect privacy rights.*²³²

These criticisms and public controversies have had an impact. DeFlock reports that 153 cities have cancelled or rejected ALPR contracts or deactivated cameras since 2021, including more than 50 in August 2026 alone.²³³ The New York Times recently reported that state and local lawmakers in Texas, Florida, Indiana, Tennessee and Ohio have also decided to remove or pause their ALPR programs.²³⁴ The Republican Governor of Florida, Ron DeSantis, has called the use of ALPRs in Florida “out of control”²³⁵ and ordered the removal of ALPR cameras from state roads, stating that

*What we don’t want in the state of Florida is to have a digital A.I. surveillance state where everything we’re doing is being tracked at all times.*²³⁶

United Kingdom

As discussed above, the United Kingdom uses FRT extensively. In 2025 and 2026, the UK government announced plans to expand the use of FRT nationally, including 40 more live FRT units, which would triple the previous capacity.

The expansion of FRT in the UK has been rapid and controversial. Facial recognition has been described as “spiralling out of control.”²³⁷ Many critics, including the UK’s Equality and Human Rights Commissioner, have noted the risks of privacy violations, racial bias, police harassment and the speed of FRT deployment across the UK.²³⁸ Critics have also stated that rapid FRT deployment is proceeding in the absence of a statutory and policy framework to govern the technology.²³⁹

The UK government conducted a consultation on police use of FRT that concluded in early 2026.²⁴⁰

In May 2026, the UK government announced plans to “establish a new legal framework” to

...underpin law enforcement use of facial recognition and similar technologies, making it clear when use of these technologies can be justified, including creation of a single, expert regulatory body to provide

*independent advice and oversight. This will be world-leading and is essential for boosting public and policing confidence in the use of these innovative technologies, which has the potential to transform crime outcomes while also generating major efficiencies.*²⁴¹

The UK government has also moved quickly to institutionalize many of the responsible AI practices discussed in this report. In June 2026, the UK government announced PoliceAI, “a new national centre dedicated to the responsible development, piloting and scaling of artificial intelligence in policing.”²⁴² UK Policing Minister Sarah Jones stated:

AI is already helping police catch dangerous offenders, speed up investigations and keep our communities safe – and we are only just getting started.

PoliceAI will transform how every force in England and Wales works, improving police access to data and intelligence, generating new evidential leads and ultimately freeing up the equivalent of 3,000 extra officers and putting more police back where they belong: in our communities.

*But we will only realise that potential if we do this responsibly, with public consent at every step. That is exactly what PoliceAI is designed to deliver.*²⁴³

PoliceAI will become part of the planned UK National Policing Service and will publish a registry of AI tools used in policing.

Finally, the UK government also states that

*AI models will be independently tested for accuracy and bias, building on the government-funded rigorous approach already established for live facial recognition algorithms. This is vital in areas like evidence translation where documents must be translated accurately to stand up in court.*²⁴⁴

4.2 Responsible Criminal AI in Canada

Section 4.1 analyzed responsible criminal AI legislation and policies in Europe, the United States and the UK. This section surveys responsible criminal AI in Canada and Ontario.

Federal Government

There is no dedicated federal responsible criminal AI framework or policy in Canada.

Legislation

The proposed federal *Artificial Intelligence and Data Act (AIDA)* would have included several responsible AI principles and established a limited risk-based governance framework for private sector AI systems in Canada.²⁴⁵ Unlike the EU *AI Act*, however, *AIDA* would not have directly regulated the use of AI in the public sector or criminal justice system. *AIDA* was heavily criticized on many grounds, including its failure to effectively regulate high risk AI systems, including criminal AI systems. Even if *AIDA* had been enacted, it would have not established trustworthy criminal AI in federal law enforcement or the criminal justice system.²⁴⁶ Nor have there been AI-specific amendments to the *Criminal Code of Canada* or other relevant federal legislation.

Canada National AI Strategy

In May 2026, the federal government also introduced *Canada's National Artificial Intelligence Strategy: AI for All*.²⁴⁷ Notably, the strategy acknowledges that:

*The risks of AI are real. Adoption means that AI systems will make consequential decisions about Canadians' lives in hiring, lending, healthcare, and public services. [...] Trust is not a brake on [AI] innovation; it is the foundation that makes broad, confident adoption possible.*²⁴⁸

However, the *Strategy* introduces no explicit commitments to establish trustworthy AI in criminal justice. Nor does the *Strategy* appear to promote responsible AI through the regulation of private sector firms providing criminal AI systems as *AIDA* might have. That said, the *Strategy* includes some elements which could, over time, support responsible AI in Canadian criminal justice, including commitments to:

- Develop “legal tools to combat deepfakes.”
- Safeguard privacy and sensitive information by promoting “digital sovereignty.”
- Expand the Canadian AI Safety Institute “to conduct transparent evaluations of AI models.”
- Create a “create a Canada Trusted AI Certification program” to identify trustworthy AI products in the marketplace.
- Expand the Standards Council of Canada’s AI Program to “enable standards-based AI testing, certification, [and] interoperability.”²⁴⁹



Responsible Criminal AI in Canada

Summary of Findings and Themes

- **Neither the federal government nor Government of Ontario have adopted a comprehensive responsible criminal AI strategy.** Responsible criminal AI governance in Canada has been led by police services, privacy commissioners and others.
- **There is no dedicated federal responsible criminal AI law or policy in Canada.** The federal *Artificial Intelligence and Data Act (AIDA)* would have established rules for private sector AI systems, potentially including high risk criminal AI systems. *AIDA* did not pass, nor has there been AI-specific amendments to the *Criminal Code* or other federal criminal legislation.
- **The federal Automated Decision-making Directive and Algorithmic Impact Assessment are leading examples of public sector responsible AI policies, but their impact is limited.** Neither explicitly apply to federal law enforcement agencies, nor are they dedicated criminal law risk assessments.
- **Ontario does not have a framework establishing responsible criminal AI in the province.** Neither *Enhancing Digital Security and Trust Act* nor the provincial *Responsible Use of Artificial Intelligence Directive* apply to AI in Ontario's criminal justice system.
- **Canadian police services have taken important steps to develop responsible criminal AI.** The RCMP's National Technology Onboarding Program and Transparency Blueprint are sophisticated responsible AI initiatives. Many municipal police services have adopted AI policies as well. The Toronto Police Service Use of AI Policy is the most significant criminal AI governance policy in Canada. The Canadian Association of Chiefs of Police has also taken an important leadership role.
- **Canadian Privacy Commissioners have issued detailed reports, but other initiatives are limited.** The federal and Ontario Privacy Commissioners have released detailed guidance and reports considering criminal AI issues. Many other institutions in Ontario are studying or discussing responsible criminal AI issues, but few reports or formal policies have been released.
- **Several Canadian courts have established detailed responsible AI policies.** These policies will have some impact on criminal proceedings. An important development is the proposed new Rule of Civil Procedure governing the use of AI evidence in civil proceedings in Ontario. This could be an important precedent for criminal proceedings.



Research Report on the Governance & Use Of Artificial Intelligence by Police in Canada

Professor Ben Perrin and a team of researchers from the Peter A. Allard School of Law at the University of British Columbia have prepared a comprehensive analysis of 13 distinct applications of AI in policing that have been adopted in Canada or other jurisdictions. Most of most applications are included in the “Criminal AI in Canada” text box following Section 1.5.²⁵⁰

The report describes each technology and provides real-world examples of their use. The report also considers the evidence supporting their benefits and risks.

The reports major conclusions include:

- There is limited independent peer-reviewed empirical validation of police AI tools.
- The risks of police AI tools are widely documented.
- Police self-governance of AI varies widely.
- There is an important, but limited, role for existing impact assessment tools and oversight bodies.
- There is a consensus on core AI governance principles.
- Existing laws of general application should be rigorously applied to police AI tools.
- There is a need for principles and guidance on the use of AI by police in Canada.
- Public engagement and multi-stakeholder discussions are needed.
- There is a need for AI-specific policing legislation and regulations.

Since the *Strategy* was announced, the federal government has introduced two new AI-related bills: Bill C-34 (the *Safe Social Media Act*), which proposes to regulate social media, AI chatbots and online services.²⁵¹

Bill C-36 (the *Protecting Privacy and Consumer Data Act*) which updates private sector privacy laws.²⁵²

Neither Bill would establish responsible criminal AI governance in Canada.

Federal Automated Decision-making Directive

The most important federal responsible AI initiative to date is the 2021 enactment of the federal Automated Decision-making Directive (federal ADM Directive) and Algorithmic Impact Assessment (AIA).²⁵³

The LCO has written at length about federal ADM Directive and AIA.²⁵⁴ In general, we have praised both as leading examples of tools and strategies that incorporate procedural fairness protections into federal government AI and algorithmic systems.²⁵⁵ The Federal Directive and AIA do not explicitly apply to federal law enforcement agencies but the RCMP has voluntarily complied, posting 14 reports to the Government of Canada AI Register.²⁵⁶

The federal government’s inaction on establishing responsible criminal AI legislation, regulations or policies is disappointing. It has been 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.



Government of Ontario

The Government of Ontario has taken important steps to establish responsible AI governance in Ontario's public sector but these initiatives do not include the provincial criminal justice sector. As a result, there is no responsible criminal AI governance framework in Ontario.

The *Enhancing Digital Security and Trust Act*

The Government of Ontario passed the *Enhancing Digital Security and Trust Act, 2024 (EDSTA)* in November 2024.²⁵⁷ The purpose of *EDSTA* is to "...[s]et a definition of artificial intelligence (AI) to create consistency across the public sector and establish protections to ensure responsible use of AI systems."²⁵⁸ *EDSTA* creates the power to prescribe a wide range of AI governance instruments in regulation, including AI prohibitions, risk management schemes, public disclosure obligations, technical standards and designated individuals with oversight responsibility.²⁵⁹ *EDSTA* does not apply to AI used in Ontario's criminal justice system.²⁶⁰

The LCO has written about *EDSTA* and Bill 194, the Bill that introduced the legislation.²⁶¹ We concluded the legislation did not establish comprehensive responsible AI for public sector AI systems in Ontario due to its lack of protections for human rights, disclosure requirements, risk categories and other provisions.

As of August 2026, the province has not introduced comprehensive *EDSTA* regulations. Thoughtful regulations could address many of the LCO's concerns.

Ontario's Responsible Use of AI Directive

The provincial government followed *EDSTA* with its "Responsible Use of Artificial Intelligence Directive" ("the Ontario AI Directive") in December 2024.²⁶² The Ontario AI Directive is more comprehensive than *EDSTA* and addresses several of the LCO's ongoing concerns about provincial AI policy.

Notwithstanding its strengths, the LCO has concluded that the Ontario AI Directive has several significant gaps or uncertainties.²⁶³ For example, the Ontario AI Directive:

- Does not explicitly apply to any law enforcement agency or police service in Ontario.
- Does not establish a consistent or transparent AI risk criteria or prohibitions.
- Does not establish consistent or comprehensive disclosure obligations.
- Does not establish a remedial regime and lacks access to justice provisions.

Neither the *EDSTA* nor the *Ontario AI Directive* apply to AI systems used in Ontario's criminal justice system, including AI systems used in policing or by courts. As a result, the province of Ontario does not have a legal framework establishing trustworthy criminal AI in Ontario.

Canadian Police Services

In contrast to the federal and provincial governments, several Canadian police services have taken important steps to develop comprehensive responsible criminal AI frameworks.

Federally, the RCMP's National Technology Onboarding Program (NTO) and Transparency Blueprint are sophisticated initiatives that incorporate many responsible criminal AI principles. NTO was "established to ensure the responsible use of operational technologies by the RCMP and encourage more public transparency of those technologies."²⁶⁴ Similarly, the RCMP Transparency Blueprint includes important details about how the RCMP assesses technology and its potential use within the RCMP.²⁶⁵ The LCO is aware of several other important RCMP initiatives, including FRT policies and emerging procedures regarding AI evidence.

Many municipal police services have also taken important steps. Most significantly, in 2022 the Toronto Police Services adopted a “Use of AI Technology Policy” (“TPS AI Policy”) following public consultations.²⁶⁶ (See text box below, “**Toronto Police Services Use of AI Policy**”).

Several other provincial police services have adopted limited, technology-specific criminal AI policies, including services in Peel, Durham, York and Ottawa.²⁶⁷

LCO consultations confirm that many other Canadian police services and police service boards

are considering general or technology-specific responsible AI policies. The LCO was impressed by the commitment and sophistication of these efforts. In particular, the LCO wants to highlight the leadership efforts of the Canadian Association of Chiefs of Police (CACP). In 2025-2026, the CACP sought to develop an AI guidance framework and AI risk assessment tool suited to the Canadian context. A draft of the CACP model was approved in August 2026 (this is further discussed in Section 6, Recommendation 4, below).²⁶⁸

Toronto Police Services Use of AI Policy

The TPS Use of 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 comprehensive trustworthy AI principles to govern AI technologies in use or proposed for use by the TPS.

The TPS AI Policy is a sophisticated document that incorporates many responsible criminal AI principles identified by the LCO and other jurisdictions. 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].”²⁶⁹ The TPS AI Policy also requires that all use of technology, including AI technology, must adhere to the important guiding principles, including legality, fairness, reliability, and transparency.

The TPS AI Policy includes explicit risk criteria, including “Extreme Risk Technologies which may not be considered for adoption.”²⁷⁰ 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.”

Finally, the TPS AI Policy includes:

- An obligation to identify operational needs and how the technology will improve operations.
- Detailed data requirements.
- Public disclosure requirements.
- Risk mitigation, audit and ongoing evaluation requirements.
- Detailed approval and reporting procedures.
- Public engagement requirements.



Privacy Commissioners

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 six investigations, reports or guidance documents on FRT in Canadian policing, including:

- A Joint Investigation of Clearview AI by the Privacy Commissioners of Canada, Quebec, British Columbia and Alberta (February 2021).²⁷¹
- A federal Privacy Commissioner report on the use of FRT by the RCMP, *Police use of Facial Recognition Technology in Canada and the Way Forward* (June 2021).²⁷²
- A joint statement by the Privacy Commissioners of Canada on police FRT (May 2022).²⁷³
- Two guidance reports from the Privacy Commissioner of Ontario addressing mugshot databases and automatic license plate readers.²⁷⁴
- A Privacy Commissioner of Ontario report, *Guidance on Police Use of Remotely Piloted Aircraft Systems (Drones) in Ontario* (August 2026).²⁷⁵

These reports include important recommendations addressing how police services can and should use criminal AI technology.

Other Criminal Justice Institutions

As noted in Section 3.2 above, several other institutions have a role in governing police services and criminal justice organizations in Ontario, including:

- The provincial Inspector General for Policing.
- The provincial Law Enforcement Complaints Agency.
- The provincial Ministry of the Solicitor General.
- The provincial Ministry of the Attorney General.
- The Ontario Court of Justice.
- The Superior Court of Ontario.
- Provincial and federal privacy commissions.
- Provincial and federal human rights commissions.
- Legal Aid Ontario.

The LCO is aware that many of these organizations are actively considering criminal AI issues in some fashion. As of August 2026, however, the number of public reports or policies addressing criminal AI issues from these institutions is very limited.

Court Rules

Several Canadian courts have established responsible AI policies to govern their work and proceedings. For example, the Federal Court has adopted a policy to guide the use of AI by the court and to direct the use of AI by parties and professionals appearing before the court.²⁷⁶ Courts in other provinces have adopted similar AI policies include Alberta, Manitoba and Quebec.²⁷⁷

The Federal Court's December 2023 *Interim Principles and Guidelines on the Court's Use of Artificial Intelligence* is an interesting and important statement of intent regarding that court's potential use of AI systems.²⁷⁸

The Canadian Judicial Council has also produced a thoughtful set of *Guidelines for the Use of Artificial Intelligence in Canadian Courts* in October 2024.²⁷⁹ 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."²⁸⁰ The Guidelines also note 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.²⁸¹

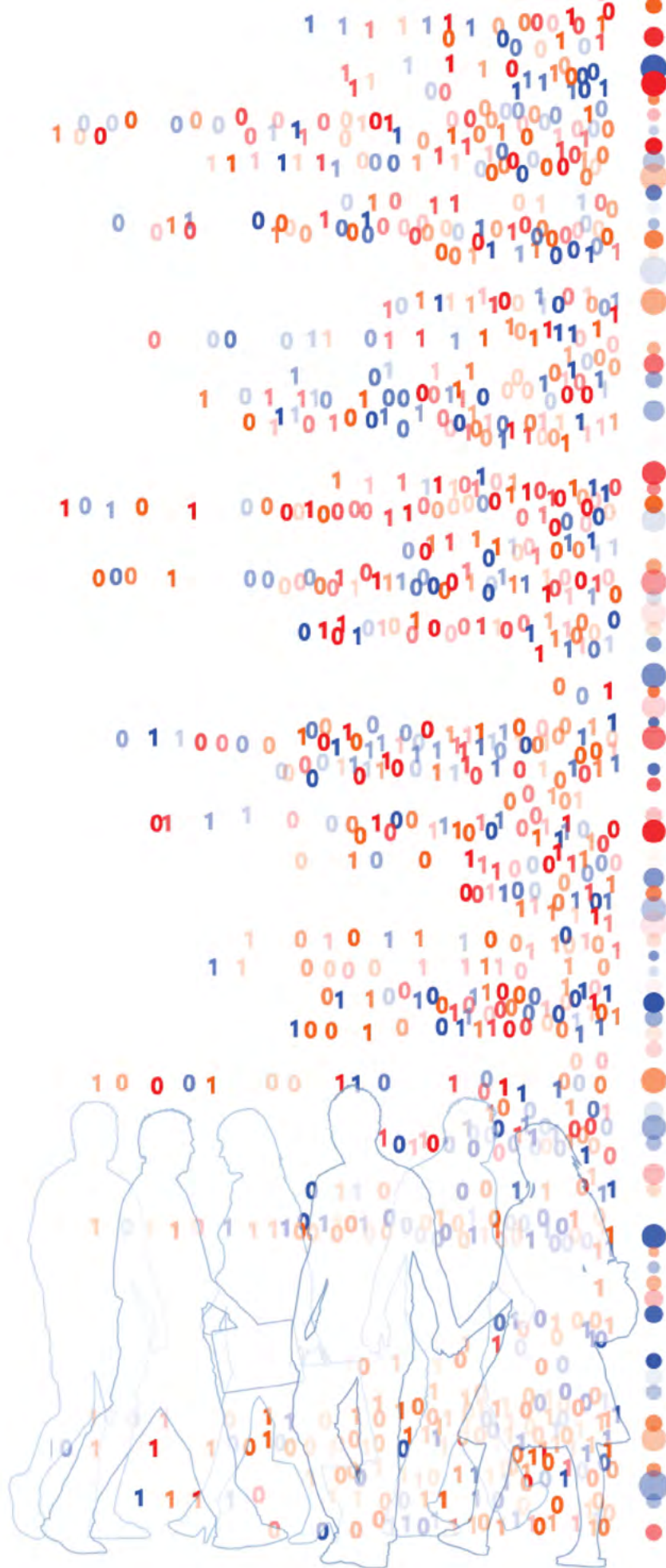
Ontario Civil Rules Committee Artificial Intelligence Sub-Committee

The most significant development in court-based responsible AI policy in Canada may be a proposed new Rule of Civil Procedure in Ontario. In 2025 and 2026, the Ontario Civil Rules Committee Artificial Intelligence Sub-Committee (“the Sub-Committee”) proposed a new Rule relating to both deep fakes and AI evidence. The proposal was approved by the full Civil Rules Committee in early 2026 and is under review by MAG.

The Sub-Committee’s four main proposals would:

- Establish a definition of “artificial intelligence” to subject its many different forms and uses to a common set of evidentiary and procedural rules.
- Establish a disclosure and evidentiary onus rule on parties who put forth AI evidence. This would require parties to identify the AI software used, the data used to train it, and create an onus to show the system produces valid and reliable results.
- Establish a rule that where AI evidence is challenged for fabrication it is presumptively inadmissible. To be admitted, the proponent would be required to demonstrate on the balance of probabilities that the evidence’s probative value exceeds its prejudicial effect.
- Establish a rule that would admit expert AI evidence (such as where a witness relies in whole or in part on material generated by AI) only where it can be shown that the evidence is based on sufficiently valid and reliable facts or data; is the product of valid and reliable principles and methods; and reflects a valid and reliable application of the principles and methods to the facts of the case.²⁸²

These rules could be an important precedent for equivalent rules in the criminal justice system.





5. Gaps, Risks and Opportunities in the Canadian Criminal Justice System

This section summarizes the LCO’s analysis of the legal and governance landscape governing Canadian and provincial criminal AI systems.

As noted in Section 4, there have been many developments in responsible AI governance at the federal level and in Ontario. Both governments have begun to establish responsible AI in many areas of the public sector and elsewhere. In criminal justice, however, neither government has taken action to establish responsible criminal AI legislation or policies.

In contrast, many police services, privacy commissions and other organizations have taken important steps to institute responsible criminal AI policies and address criminal AI risks. The support for, and sophistication of, these efforts is increasing.

5.1 Gaps in Responsible Criminal AI in Canada

It is helpful to compare Canadian initiatives with responsible criminal AI governance other jurisdictions. As summarized in Section 4.1, there are many responsible criminal AI regimes in Europe, the United States and the United Kingdom. The form and substance of these regimes differ but our peer jurisdictions have enacted or proposed complex frameworks governing:

- Mandatory disclosure of criminal AI systems, including public “AI registers”.
- Prohibitions on the highest risk criminal AI systems
- Criteria to identify prohibited or high risk systems.
- 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 systems.

Broadly speaking, these reforms set out the constituent elements of comprehensive responsible criminal AI governance.

Gaps, Risks and Opportunities in Canadian Criminal Justice Summary and Findings and Themes

- **Canadian jurisdictions are far behind jurisdictions in Europe, the United States and the United Kingdom in establishing responsible criminal AI.**
- **There are wide and consequential gaps in the legislative, regulatory and policy framework governing criminal AI systems in Canada and Ontario.** Major gaps include:
 - o No national or provincial criminal justice AI strategy.
 - o Missing or inconsistent disclosure requirements.
 - o Missing or inconsistent criminal AI prohibitions, “guardrails”, and risk criteria.
 - o No dedicated criminal AI impact assessment.
 - o Missing, inconsistent or unclear criminal procedural protections.
 - o No obligation to test, audit, or evaluate criminal AI systems.
 - o No obligation to undertake public consultations.
- **Absent effective regulation, the potential harm to criminal defendants, criminal courts, and public trust is foreseeable and significant.** Failure to regulate could mean predictive policing, FRT, and other technologies could be introduced in Ontario without appropriate “guardrails” or accountability requirements.
- **There is a significant opportunity to promote responsible criminal AI in Ontario and across the country.** There is a near-universal desire amongst criminal justice system stakeholders for a proactive and collaborative strategy to address criminal AI governance issues in Canada. There is also a significant responsible criminal AI “community of practice” in Canada.
- **The LCO and its collaborators have developed comprehensive and detailed recommendations for law, regulatory and policy reform.** The result is a comprehensive agenda and framework that would embed responsible AI principles and policies throughout Ontario’s criminal justice system.

Our research and consultations confirm that, despite many important efforts, there are still wide and consequential gaps in the legislative, regulatory and policy framework governing criminal AI systems in Canada and Ontario. More specifically, the LCO has identified several important gaps in responsible criminal AI governance in Canada and Ontario, including:

- No national or provincial criminal justice AI strategy.
- Missing or inconsistent disclosure requirements.
- Missing or inconsistent criminal AI prohibitions, “guardrails” or risk criteria.

- No dedicated criminal AI impact assessment.
- Missing, inconsistent or unclear criminal procedural protections.
- No consistent obligation to test, audit, or evaluate criminal AI systems.
- No consistent obligation to undertake public consultations.

The legal and governance risks discussed in this report will be exacerbated by these gaps, resulting in unacceptable legal risks, inefficiencies, barriers to responsible AI adoption and missed opportunities to improve public safety. The chart below summarizes the risks and potential impact of these gaps in Ontario.

Summary Analysis of Gaps in Ontario’s Responsible Framework and Potential Risks and Impacts

Gap	Potential Risk and Impact
1. No provincial responsible criminal AI strategy.	Potential Risk No provincial coordination or leadership on criminal AI issues. Provincial criminal justice institutions and courts respond on institution-by-institution or case-by-case basis. Potential Impact • Systemic breaches of <i>Charter</i> or other legal rights. • Inconsistent deployment of provincial criminal AI systems. • Unclear rules to promote responsible criminal AI deployment. • Inconsistent or inadequate legal and public oversight. • Increased litigation/reduced access to justice. • Loss of public accountability and public trust.
2. Missing or inconsistent provincial disclosure requirements.	Potential Risk The majority of police services in Ontario could implement FRT, predictive policing or other AI systems without public disclosure. Potential Impact • Public concerns about “secret” surveillance or racial profiling. • Systemic breaches of <i>Charter</i> or other legal rights • Inconsistent or inadequate legal and public oversight. • Loss of public accountability and trust.

Gap	Potential Risk and Impact
3. Missing or inconsistent provincial criminal AI prohibitions, “guardrails” and risk criteria.	Potential Risk Police services or other institutions in Ontario could deploy the highest risk criminal AI systems without “guardrails” or provincial criteria. Potential Impact • Systemic breaches of <i>Charter</i> or other legal rights. • Inconsistent deployment of provincial criminal AI systems. • Unclear rules to promote responsible criminal AI deployment. • Inconsistent or inadequate legal and public oversight. • Increased litigation/reduced access to justice. • Loss of public accountability and public trust.
4. No dedicated provincial criminal AI impact assessment.	Potential Risk AI systems could be deployed in Ontario without adequate assessment of their impact on <i>Charter</i> rights, human rights, privacy, evidence, procedure, etc. Potential Impact • No assurance of compliance with Canadian law. • Systemic breaches of <i>Charter</i> or other legal rights. • Inconsistent deployment of provincial criminal AI systems. • Unclear rules to promote responsible deployment. • Duplication or inefficiencies as organizations develop their own assessments. • Increased litigation/reduced access to justice.
5. Missing, inconsistent or unclear provincial criminal procedural protections.	Potential Risk Criminal courts need to develop AI legal standards on case-by-case basis. Potential Impact • Unclear/inconsistent decisions re disclosure, warrants or evidence. • Increased litigation. • Significant new barriers to low-income, Indigenous and racialized communities. • Reduced access to justice. • Inconsistent or inadequate legal accountability.
6. No provincial obligation to test, audit, or evaluate criminal AI systems.	Potential Risk Criminal AI systems could be deployed in Ontario without a duty to audit or evaluate their accuracy, bias or effectiveness. Potential Impact • Systemic breaches of <i>Charter</i> or other legal rights. • Worsening over-representation of racialized and Indigenous communities. • Inconsistent or inadequate legal and public oversight. • Increased litigation/reduced access to justice. • Loss of public accountability and public trust.

Gap	Potential Risk and Impact
7. No obligation to undertake public consultations.	Potential Risk Police services and other criminal justice institutions in Ontario could implement FRT, predictive policing or other AI systems without public consultations. Potential Impact • Public concerns about “secret” surveillance or racial profiling. • Inadequate review/assessment of criminal justice AI systems. • Loss of public accountability and public trust.

5.2 What If We Do Not Regulate?

In these circumstances, it is fair to ask what could happen if governments and other institutions do not take proactive steps to establish responsible criminal AI in Ontario. 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.
- Worsening overrepresentation of low-income, racialized and Indigenous communities.

These risks and consequences are foreseeable in a province that lacks consistent criminal AI disclosure requirements, risk criteria, reliability and bias testing, evidential rules and other measures.

Failure to regulate criminal justice AI systems could mean predictive policing, FRT, and other 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 is foreseeable and significant.

The lack of provincial responsible criminal AI standards is particularly important considering the wide, diverse and decentralized network of institutions and actors involved in developing, operating, litigating or overseeing AI in Ontario’s criminal justice system.

5.3 Responsible Criminal AI Consensus

Notwithstanding this analysis, there are many reasons to be optimistic.

An important finding of this project is the near-universal desire amongst criminal justice system stakeholders for a proactive and collaborative strategy to address criminal AI governance issues in Canada.

Another important finding is the breadth and depth of organizations and individuals already collaborating on criminal AI issues. The Canadian “community of practice” in this area is growing in numbers and sophistication as more institutions, researchers and advocates begin to consider and discuss these important issues.

Two recent examples demonstrate these efforts.

- **UBC/LCO Principles on Governance and Use of AI by Police in Canada**

On May 26, 2026, over 65 criminal justice sector professionals attended the *AI & Policing Symposium* co-hosted by the UBC AI & Criminal Justice Initiative and the LCO.

Participants included representatives from across the Canadian criminal justice system, including police, defence counsel, Crowns, oversight bodies, NGOs, academics and legal aid organizations.

The Symposium discussed draft *Principles on the Governance & Use of AI by Police in Canada*, developed by the UBC AI Criminal Justice Initiative and the LCO. The *Principles* followed a series of reports and consultation events held in 2025. The *Principles* are a voluntary, consensus-based framework to better achieve “trustworthy AI” among law enforcement agencies. The *Principles* promote consistent police AI governance policies and encourage law and policy reform. The principles include:

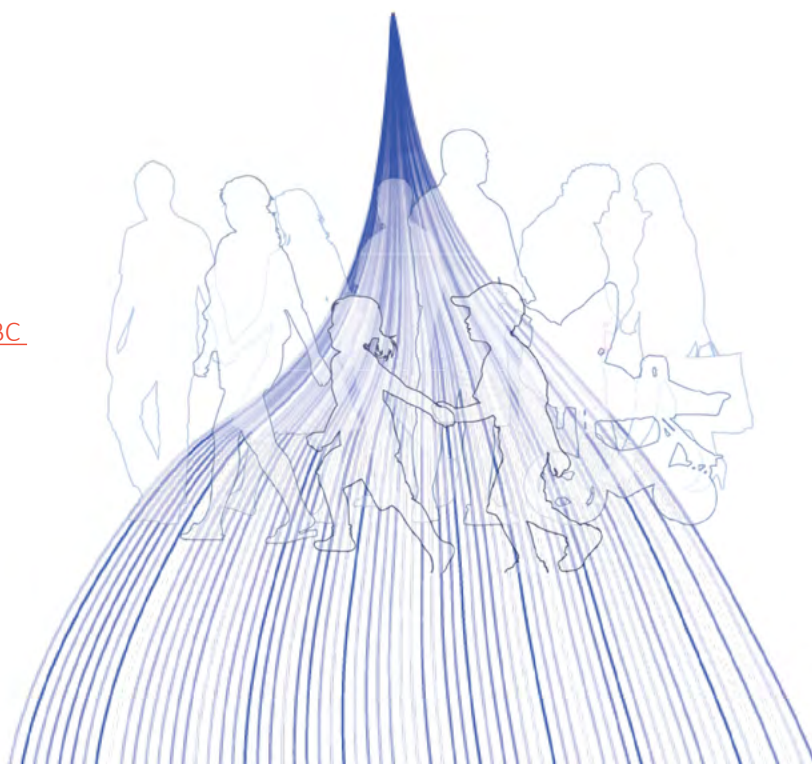
- 1) Good Governance and Accountability
- 2) Lawfulness
- 3) Respect for Human Rights
- 4) Privacy by Design
- 5) Accuracy, Reliability, Validity, and Robustness
- 6) Notice and Transparency
- 7) Human Control & Accountability
- 8) Security, Safety & Digital Sovereignty
- 9) Explainability & Interpretability
- 10) Independent Third-Party Oversight & Public Engagement

The *Principles* and an accompanying report were released in September 2026 and are available on [UBC AI & Criminal Justice Initiative](#) website.

- **The LCO Vancouver Roundtable on the Use of FRT by Law Enforcement**

A second important collaboration occurred in June 2025 at the LCO’s Vancouver Roundtable on the Use of FRT by Law Enforcement. The Vancouver Roundtable was the first of two LCO roundtables on criminal justice AI issues. A second roundtable on AI Evidence in Criminal Proceedings was held in Toronto in August 2025.

The Vancouver Roundtable brought together a broad range of stakeholders for a frank and collaborative roundtable discussion about FRT benefits, risks, deployment, legal issues and governance. The Roundtable was participatory, constructive and solution-oriented. Participants included representatives from federal and municipal law enforcement, private bar and legal aid defence counsel, provincial human rights and privacy agencies, academics and public interest advocates. The Roundtable’s findings and themes are summarized in the text box on the following page.



Vancouver Roundtable Theme	Insight or Finding
1. FRT adoption is uneven.	FRT has not been widely adopted by Canadian police services. There are wide variations in interest, capacity and use of FRT across the country. Larger services may have the resources to support FRT adoption; smaller services will likely need help.
2. There are many forms of FRT governance. Police policies are a good place to start.	Police services agree that successful FRT adoption depends on robust, transparent and participatory governance. FRT governance can take many forms. Police services should not wait for FRT legislation. Several police services have developed AI or FRT policies and procedures. These policies are important first steps. Model AI or FRT policies could promote consistent and thoughtful police practices across Canada.
3. FRT governance must reflect Canadian law.	FRT governance must reflect and proactively apply Canadian law. This will better ensure FRT use is legal, reflects Canadian and local values, and is more likely to be accepted in court.
4. FRT governance must be risk-based.	Not all FRT applications are the same. A “one size fits all” FRT governance model is unlikely to be effective or reflect Canadian law. Risk-based governance is needed to differentiate FRT applications, tailor governance requirements, and align with baseline requirements for all AI systems.
5. Canadian privacy and evidence law should be updated to address FRT issues.	Canadian privacy law must be updated to reflect the legal and operational complexities of FRT, including updated expectations of privacy and the rules for storing images. Similarly, Canadian criminal evidence law could adopt dedicated thresholds for FRT admissibility and updated tests for evidentiary reliability and validity.
6. Presumptive AI “red lines” and authorized uses are important regulatory standards.	A thoughtful list of presumptive AI “red lines” or prohibitions could prevent overbroad use of FRT. Similarly, it would be helpful to list the applications or criteria to authorize lawful FRT, including when FRT could be used legally in exceptional circumstances. Any such list must reflect differences in police service mandates and responsibilities.
7. Thoughtful policies can foster responsible FRT adoption.	Governance and procurement policies can promote responsible and consistent police FRT deployment. For example, it would be helpful if police services could purchase FRT systems that were “certified” or pre-tested to meet requirements for reliability and validity, human rights, bias and privacy.
8. Public accountability is essential for FRT adoption and public trust.	Successful police FRT adoption depends on public understanding and credibility. Public reporting and transparency are necessary to ensure public trust. At present, there is little public awareness of the “footprint” or impact of law enforcement FRT systems in Canada.
9. Oversight of police FRT systems could be coordinated more effectively.	Several factors currently limit the effectiveness of police FRT oversight, including the need for dedicated police AI and FRT impact assessments, the need for skilled “humans-in-the-loop” to evaluate FRT outputs and systems, and the need for provincial policing standards to support model police AI and FRT-related practices and policies.



6. LCO Recommendations: A Provincial Responsible Criminal AI Framework

Criminal AI systems introduce new and complex risks which could expose an unprecedented number of Ontarians to police surveillance, rights and privacy violations, racial bias and other AI risks and harms.

The LCO's research and consultations demonstrate that patchwork, uncoordinated responses are insufficient to govern these complex and widespread risks. Most notably, the LCO and many stakeholders are concerned that the combination of multiple laws, multiple institutions and complex technologies could result in ad hoc, inconsistent or improper governance of criminal AI systems. As a result, the LCO and others believe the provincial response to these risks must be coordinated and systemic to ensure criminal AI systems are legal, beneficial and build public trust.

This project is the first in Canada to analyze AI systems and issues across the entire "lifecycle" of criminal justice. This is also the first project in Canada to engage with stakeholders and institutions across the criminal justice system to collaboratively develop recommendations for law, regulatory and policy reform. The result is a comprehensive agenda and framework that would embed responsible AI principles and policies throughout the criminal justice system. An important finding of this project is the near-universal desire amongst criminal justice stakeholders to work together to address criminal AI issues constructively.

The LCO's 29 recommendations are principled, practical, balanced and proven. Indeed, almost all our recommendations are based on precedents, practices and strategies already in place in Canada, other jurisdictions or currently under development by Canadian law enforcement, governments and other justice institutions.

Summary of LCO Recommendations

Recommendations 1-3: Provincial Criminal AI Framework

LCO Recommendations 1-3 commit Ontario to comprehensive responsible criminal AI governance and confirm the key elements necessary to achieve it.

The LCO and stakeholders agreed that a provincial commitment is necessary to ensure AI systems in criminal justice promote public safety, protect legal rights and build public trust. Specific recommendations would:

- Establish the commitment and objectives of a responsible criminal AI framework in Ontario.
- Confirm the institutions and actors subject to the framework.
- Confirm the necessary elements of the framework.

These recommendations are consistent with well-established, existing responsible criminal AI frameworks in many jurisdictions and sectors, including many Canadian precedents.

Recommendation 4: Provincial Criminal Justice AI Legislation

LCO Recommendation 4 amends the provincial [*Enhancing Digital Security and Trust Act, 2024*](#) or creates complementary legislation to establish significant responsible criminal AI principles and requirements in Ontario, including:

- A precautionary principle.
- Duties to comply with fundamental Canadian rights, law and values.
- Mandatory risk categories.
- Public disclosure, risk assessment, legal safeguards and auditing.

Provincial legislation is needed to establish a foundational governance framework for criminal AI systems. Legislation would also provide consistent direction and accountability requirements to the actors, departments and/or agencies within its scope. Finally, legislation would establish a level of public and legal accountability commensurate with the issues and rights at stake.

Recommendations 5-7: Provincial Reporting and Oversight

LCO recommendations 5-7 establish an effective provincial responsible criminal AI reporting and oversight regime. Recommendations include legislative provisions establishing:

- Comprehensive public reporting requirements for provincial law enforcement agencies.
- A dedicated provincial supervisory authority for AI systems.
- A requirement for agencies to develop related AI governance and operational policies.

These recommendations promote evidence-based criminal AI governance. They also support responsible AI adoption and public trust and accountability.

Recommendation 8: Digital Sovereignty and Procurement

LCO Recommendation 8 protects digital sovereignty in Ontario's criminal AI systems. It also establishes a legislative power to regulate standard terms for third party AI vendor service contracts.

This recommendation is needed to ensure AI systems used by provincial criminal justice institutions have consistent and enforceable standards; ensure data is managed properly; and respect Canadian privacy and other laws.

Recommendation 9: Public Engagement

Recommendation 9 establishes legislative authority to define a series of public engagement and transparency measures, including public participation in any AI assessment process, annual reporting on how AI systems are being used, public participation in the provincial supervisory authority, and mandatory legislative reviews.

Recommendations 10-15: Criminal AI Risk Management

LCO Recommendations 10-15 establish a comprehensive risk management framework and strategy to govern AI systems in Ontario's criminal justice system.

Recommendation 10 identifies four risk categories (Prohibited, High Risk, Restricted and Low Risk) that should be established in legislation.

Recommendation 11 directs the provincial government to conduct public consultations on risk management issues.

Recommendations 12, 13, 14 and 15 identify potential criteria and use cases for each risk category.

Together, these recommendations match criminal AI governance obligations to a system's uses, benefits and risks; support responsible AI adoption; promote public trust; and uphold the principles and requirements of Canadian law.

Recommendation 16: Public Criminal AI Registry

Recommendation 16 establishes a comprehensive public registry of AI systems used in Ontario's criminal justice system. The Recommendation identifies key details to be included and mandates regular reporting obligations.

Recommendations 17-18: Risk Assessments

Recommendation 17 commits the Government of Ontario to engage criminal justice sector institutions in developing a standard risk assessment framework. Common risk assessment criteria, categories and mitigation measures would ensure a consistent approach to reliable AI across Ontario's criminal justice institutions.

Recommendation 18 establishes legislative authority to set standards for AI pilot projects and real-world performance evaluations; a set of procurement standards and standard terms for vendor contracts; and protections for digital sovereignty.

Recommendations 19-20: Oversight and Reporting

LCO Recommendations 19-20 establish detailed oversight and reporting obligations. These recommendations have two parts: First, they commit the province to establishing a dedicated supervisory body for AI systems in criminal justice. In the interim, the recommendations add reporting, oversight and advisory functions to Ontario's Inspector General of Policing, Law Enforcement Complaints Agency, and others.

Recommendations 21-24: AI Evidence

LCO Recommendations 21 – 24 address AI-created or AI-enhanced evidence that might be used in criminal proceedings or during a criminal investigation. These recommendations account for the shared jurisdiction in these matters between the provincial government, federal government and various Rules committees, and the need to develop dedicated evidentiary rules for different stages of the criminal justice process.

Recommendations 25-29: Access to Justice and System Capacity

Recommendations 25-29 address the need to ensure criminal accused and defence counsel have meaningful access to justice in criminal proceedings involving AI systems. These recommendations also address the need to increase capacity within provincial criminal justice institutions to effectively respond to the foreseeable challenges of AI systems.

Recommendations 1-3: Provincial Criminal AI Framework

LCO Recommendations 1-3 commit Ontario to developing a comprehensive framework to govern criminal AI systems in the province.

The LCO and stakeholders agreed that a provincial framework is necessary to ensure consistent governance throughout the lifecycle of AI in Ontario's

criminal justice system. This framework will promote public safety, protect legal rights and build public trust. Specific recommendations will:

- Commit Ontario to developing a responsible criminal AI framework.
- Confirm the institutions and actors subject to the framework.
- Confirm the necessary elements of the framework.

LCO Recommendations

1. The Province of Ontario should commit to developing a comprehensive governance framework for AI systems used in the criminal justice system in Ontario.
2. This framework should establish clear legal and policy guidance to governments, law enforcement agencies, courts, Crowns, defence counsel, legal aid and others to promote the responsible development and deployment of AI in Ontario's criminal justice sector.
3. The key elements of this framework should include:
 - a. Mandatory, public disclosure of AI systems in criminal justice.
 - b. Risk criteria identifying prohibited, high risk, restricted use and low risk uses of AI systems in criminal justice.
 - c. A dedicated and mandatory impact assessment for AI systems in criminal justice.
 - d. A duty to evaluate AI systems in criminal justice for reliability, validity, bias, and conformity with the *Charter*, human rights law, privacy law, and criminal procedural and evidentiary requirements; and for law enforcement services to additionally evaluate lawful authority and purpose.
 - e. Procedural protections, such as warrant requirements for high risk systems and dedicated rules governing AI generated or enhanced evidence in different proceedings.
 - f. Support for criminal justice AI pilots.
 - g. Mandatory and ongoing auditing and evaluation requirements.
 - h. Procurement standards and policies governing responsible software practices including software explainability, version control and archiving, training data disclosure and transparency, and reports on reliability, validity and bias of the system.
 - i. An independent supervisory body to support oversight of individual AI systems and provincial AI systems in criminal justice generally.
 - j. Guarantees for judicial independence and investigative privilege for law enforcement.
 - k. Commitments that will ensure access to justice and equitable access to AI legal tools.



A Provincial Framework

LCO Recommendations 1-3 commit Ontario to developing a comprehensive framework to govern criminal AI systems in the province. Recommendations 1 and 2 establish the broad obligation to establish this framework and who it applies to. Recommendation 3 establishes the key elements of the framework.

The LCO believes a provincial framework is necessary for four reasons:

First, absent coordination, institutions across the province will have to develop their own AI policies, which may or may not conform with existing legal rules, protect rights, be consistent with one another or incorporate responsible criminal AI principles.

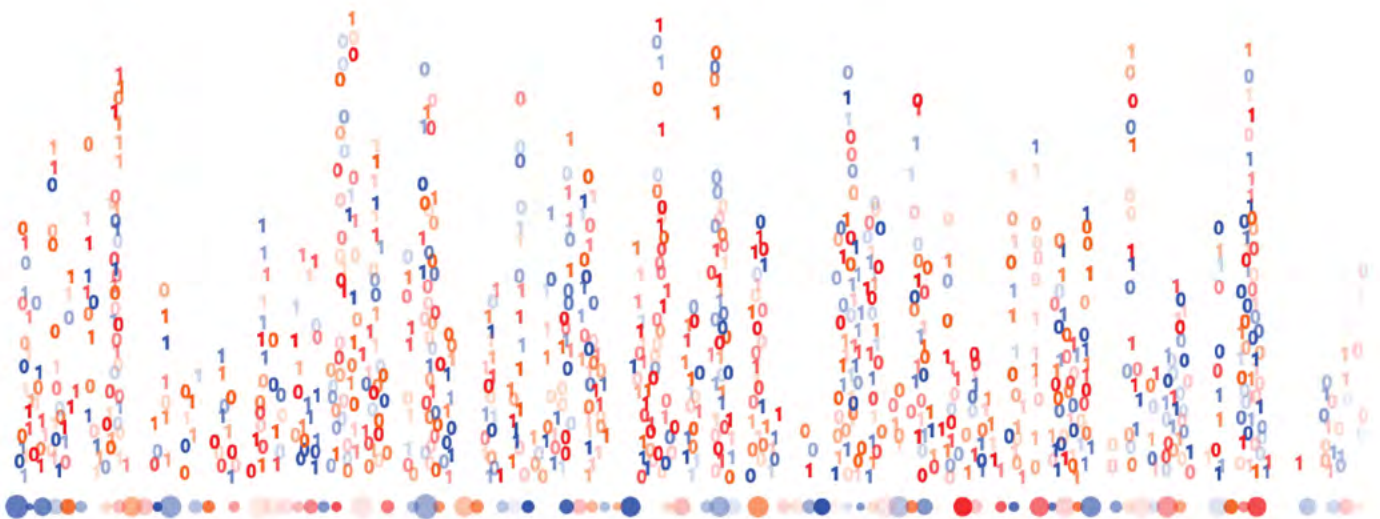
Second, experience demonstrates that patchwork AI rules self-determined by different institutions may put residents in some areas of the province at greater risk of AI discrimination, false arrest, privacy violations and more.

Third, a provincial framework will promote responsible criminal AI adoption across the province, reduce duplication, and improve the province's ability to promote, evaluate and oversee criminal AI systems.

Finally, a provincial framework will establish a transparent and comprehensive provincial agenda.

LCO research and consultations indicate broad support for this approach. For example,

- Consultees consistently told us that criminal AI systems have considerable potential but that AI risks create serious barriers to responsible AI adoption.
- Consultees frequently complemented the many initiatives across the province and country to promote responsible criminal AI. At the same time, many stakeholders were worried about the “Governance Risks” summarized in Section 3.2 above.
- Consultees consistently discussed the need for guidance. The LCO frequently heard that institutions are uncertain about their legal obligations, need assistance on AI risk assessment, and are concerned that existing AI tools and governance instruments may not reflect Canadian law and values.
- Consultees note that criminal AI systems are not discrete or limited to one institution or proceeding. The use of FRT to identify a suspect by the police, for example, is just the first step in a long process that may include an investigation, warrants, charging, disclosure, bail, trial, expert evidence, sentencing, and appeals. We were told there is a strong need for consistency across this “lifecycle” to ensure it meets constitutional, statutory, evidential and procedural requirements at every step of the process.



Recommendation 4: Provincial Criminal Justice AI Legislation

LCO Recommendation 4 would amend the provincial [*Enhancing Digital Security and Trust Act, 2024*](#) or create complementary legislation to establish significant responsible criminal AI principles and requirements in Ontario, including:

- A precautionary principle.
- Duties to comply with fundamental Canadian rights, law and values.
- Mandatory risk assessment categories.
- Public disclosure, risk assessment, legal safeguards and auditing.

Provincial legislation is needed to establish the foundational governance framework for criminal AI systems in Ontario. Legislation would also provide consistent direction and accountability requirements to the actors, institutions, departments and/or agencies within its scope. Finally, legislation would establish a level of public and legal accountability commensurate with the issues and rights at stake.

LCO Recommendations

4. The Government of Ontario should amend the [*Enhancing Digital Security and Trust Act, 2024*](#), or create complementary legislation, to enshrine significant governance principles and requirements in provincial legislation for AI systems in criminal justice. This legislation (or accompanying regulations) should:
 - a. Include a preamble specifying that AI systems in criminal justice are subject to a precautionary principle, and must comply with the *Charter*, principles of criminal procedural fairness, privacy law, human rights law, criminal common law, and the principle of judicial independence.
 - b. Establish mandatory risk categories for AI systems in criminal justice, including:
 - i. Prohibited systems.
 - ii. High risk systems.
 - iii. Restricted use systems.
 - iv. Low risk systems.
 - c. Require AI systems in criminal justice to:
 - i. Be disclosed on a public AI registry.
 - ii. Be subject to a dedicated and mandatory impact assessment.
 - iii. Comply with procedural and evidence standards.
 - iv. Be audited and evaluated on an ongoing basis.



Provincial Legislation

The LCO has concluded that provincial legislation is needed to establish significant governance principles and requirements in Ontario's criminal AI systems. This view was widely shared in the multidisciplinary and multi-institutional consultations and roundtables convened by the LCO and are included in the UBC/LCO Principles on Governance and Use of AI by Police AI discussed in Section 5 above.

This recommendation is consistent with responsible criminal AI governance established in the EU, the United States and the United Kingdom. It is also consistent with Ontario's own *EDSTA*.

In our view, Recommendation 4 is justified by many of the themes and issues that have been discussed in this report, including:

- **Need for Provincial Consistency and Baseline Requirements**

The LCO's research and consultations have consistently affirmed the key principles and elements of responsible criminal AI. They have also consistently warned against the risks of institutional self-regulation; uncoordinated decentralization; missing, inconsistent or unclear governance standards; and gaps in legal and public accountability. LCO consultees agree that discrete or institution-by-institution AI policies and practices are insufficient to mitigate the harms caused by AI and related systems due to their risk of inconsistency, lack of specificity and reliance on voluntary compliance. Provincial legislation would bring coherence and coordination to this decentralized and disorganized network.

Importantly, the need for provincial consistency and baseline requirements is growing. Unless action is taken, criminal AI legal and governance risks will *worsen* as more police services and other criminal justice institutions begin to use AI.

- **Need to Establish Governing Rules Commensurate with Legal Rights and Risks**

AI in the criminal justice system affects some of most important issues and rights in Canadian society, including public safety; personal liberty; *Charter* rights; procedural rights; and public trust in key institutions, including courts and law enforcement. Provincial legislation would establish governing rules that are commensurate with the rights and risks at issue.

The LCO emphasizes that AI in criminal justice needs to be comprehensively regulated not just because of the range and severity of potential legal risks, but also because of the potential scale of legal risks. Simply stated, the number of people whose rights could be affected by criminal AI systems dwarfs the scale and impact of traditional police investigative techniques. AI adopted by other provincial criminal justice institutions will also operate at scale, triggering systemic impacts and risks that must be identified, mitigated and monitored.

- **Risk of AI Deployment Outpacing Governance and the Risk of Emerging Technology**

It would compromise the purpose and credibility of responsible AI governance in Ontario if provincial police services or other criminal justice institutions widely deployed high risk systems *before* consistent governance standards were established. Yet this is exactly what could happen if criminal AI governance remained the responsibility of individual institutions. Provincial legislation minimizes this risk and will ensure all relevant criminal justice institutions in Ontario are bound by common and coordinated principles and expectations.

Provincial legislation also addresses a related risk: Powerful new technology and criminal justice applications are emerging all the time. For example, FRT vans, handheld FRT devices and biometric inferencing are new and potentially very risky tools. Provincial legislation would establish broad principles of governance and ensure new or emerging technologies or applications did not avoid responsible AI governance.

- **Existing Laws and Litigation are Not Sufficient**

The LCO's analysis and consultations repeatedly show that responsible criminal AI governance cannot rely on existing laws or litigation alone. For example, our research and consultations consistently demonstrated that there are many gaps and unanswered questions regarding FRT or AI-generated evidence that need legislative clarification.²⁸³

This is not to say that existing law does not apply or is not helpful. Indeed, criminal procedure and evidence law is flexible and accustomed to dealing with new investigative technologies. The LCO repeatedly heard confidence in the ability of courts to test the reliability and validity of investigative technologies; examine the context and lawful purpose under which such technology is used; and ground their analysis in facts and technology specific to the case.

At the same time, the LCO heard serious concerns about relying exclusively on litigation and courts as a de facto regulator for AI. This is for several practical reasons discussed in LCO's fourth and fifth Issue Papers and confirmed in consultations where the LCO was told that:

- Most charges never go to trial, meaning most AI cases will not be tested in a full hearing.
- Litigation is adversarial, expensive, and precedents are narrowed to the facts, technology and specific use case at trial.
- Litigation necessarily entails a degree of "law lag" in which judicial hearings and decisions trail months or years behind the use of an AI system.
- The uses, capabilities and performance characteristics of AI technology are certain to change over time, likely distinguishing new cases from established precedent.
- Proceedings like bail, diversion, sentencing and warrants each come with significant consequences but are decided on varying burdens of proof, procedures of varying rigor, and may not be easily adapted to testing complex AI evidence without new rules in place.

- Access to justice is not always equitable, with significant differences in resources between law enforcement, prosecutors, and defence of an accused.²⁸⁴

Provincial legislation is needed to address these gaps.

- **EDSTA is an Established Precedent**

Ontario has already established the precedent of framework AI legislation. In 2024 Ontario became the first province in Canada to enact broad public sector AI governance legislation. The *Enhancing Digital Security and Trust Act, 2024 (EDSTA)* establishes provincial authority to regulate the AI use across most of the Ontario public sector while leaving specific details to regulations. In this manner, *EDSTA* explicitly acknowledges it is appropriate and effective to legislate broad AI governance standards and operational regulations across institutions and use cases.

As presently written, however, *EDSTA* cannot be the framework criminal AI legislation we recommend. This is because *EDSTA* excludes courts, tribunals and law enforcement agencies from its jurisdiction, as noted in Section 4.2 above.²⁸⁵

The AI governance approach in *EDSTA* is mirrored in several federal initiatives, including statutes, strategies, and assessment instruments.²⁸⁶

EDSTA and the federal initiatives are important examples of Canadian AI governance legislation. Recommendation 4 would establish AI governance legislation in criminal justice. At the very least, it would be puzzling if AI in most of Ontario's public sector was subject to AI governance legislation but the highest risk AI systems used in criminal justice were not.

To address these issues, Recommendation 4 directs the province to amend *EDSTA* to include the criminal justice sector or develop complementary legislation.

There are many international precedents for establishing framework legislation to govern AI systems, including the EU *AI Act*, multiple American examples and the recent announcement of PoliceAI and national AI legislation in the UK.²⁸⁷

The Precautionary Principle

Recommendation 4 suggests a legislative preamble with three important provisions: the precautionary principle, the priority for Canadian law, and the principle of judicial independence.

As discussed throughout this report, most jurisdictions and LCO consultations confirm the widely held view that criminal justice is among the highest risk use cases for AI. The use of AI in criminal justice comes with direct impacts on fundamental rights and freedoms guaranteed under the *Charter of Rights*, human rights, privacy and the rule of law. The Canadian federal government has acknowledged that use of AI technology in criminal justice comes with potentially “severe consequences for individuals’ freedoms, rights, and social and economic circumstances... [and] important effects on the rule of law and access to justice.”²⁸⁸

To ensure the proposed criminal sector AI framework and legislation is interpreted and operationalized consistent with this level of risk, the LCO recommends preamble provisions to guide interpretation of the proposed legislation.

First, our recommended preamble includes a precautionary principle. A precautionary principle and priority assessment for conformity with Canadian criminal law are both important and practical. Together, they would ensure that no high risk AI or restricted use AI systems are deployed without first and foremost assessing the risks to individual rights and the systemic impacts that might flow from the failure to foresee guardrails inherent in basic procedural fairness and evidence law.

Second, our recommended preamble establishes Canadian criminal law as the primary standard for assessing criminal AI risks and impacts.

Almost all consultees agreed that established Canadian criminal law guardrails should remain the first standard against which criminal AI tools should be assessed. Indeed, several roundtable sessions with over 100 justice sector professionals concluded, with a high degree of consensus, that the two most important principles governing police AI systems should be 1) “good governance and accountability” and 2) “lawfulness.”²⁸⁹

Significantly, the Canadian Association of Chiefs of Police (CACP) sees these as fundamental commitments. Over 2025-2026, the Canadian Association of Chiefs of Police (CACP) sought to develop an AI guidance framework and AI risk assessment tool suited to the Canadian context. A draft of the CACP model was approved in August 2026. Importantly, the proposed draft echoes key LCO recommendations including:

- Committing to a precautionary principle.
- Assessing AI through four standard risk classifications (including AI prohibitions).
- Prioritizing lawfulness and fundamental rights as the primary criterion for AI assessment.²⁹⁰

Several other jurisdictions use a rights-based lens to analyze AI risks. For instance in February 2026 the EU’s Council of Europe Committee on Artificial Intelligence formally adopted the “human rights, democracy and rule of law” (HUDERIA) framework to assess AI.²⁹¹ The HUDERIA framework is designed “to support consistent and practical risk and impact assessment of AI systems from the perspective of human rights, democracy and the rule of law.”²⁹²

To their credit, many self-governance policies and assessment practices in Ontario include fundamental rights and protections among their assessment criteria.²⁹³ That said, these policies are not consistent, nor do they necessarily, proactively, or comprehensively assess a system’s compliance with Canadian criminal law.²⁹⁴

LCO consultations discussed several examples that demonstrate the need for rigorous assessment against Canadian law. For example, a FRT system with a high error rate may not satisfy evidentiary admissibility thresholds for validity or reliability under Canadian criminal evidence law.²⁹⁵ Similarly, FRT software may violate criminal procedural fairness if there is no policy on disclosure, an inability to describe checks and balances in how the software is operationalized or deployed, or the creation of a “human in the loop” process that identifies responsible officers to can verify, certify and testify to the match.

The Principle of Judicial Independence

Recommendation 4.a. also states that the new provincial criminal AI statute should explicitly state that judicial independence is a key governance requirement for AI systems.

Sections 71 and 72 of the *Courts of Justice Act (CJA)* states that the administration of the courts shall be carried on so as to “maintain the independence of the judiciary as a separate branch of government; recognize the respective roles and responsibilities of the Attorney General and the judiciary in the administration of Justice; [... and] promote the efficient use of public resources.”²⁹⁶ Section 72 of the *CJA* further provides that the Attorney General is “responsible for superintending the administration of the courts.”²⁹⁷ These obligations reflect the reaffirmation within the *Charter of Rights and Freedoms* section 11(d), guaranteeing that every person charged with an offence has the right to a fair trial before “an independent and impartial tribunal.”

As noted in Section 4.2, the principle of judicial independence is already reflected in many court AI rules.

Recommendations 5-7: Provincial Reporting and Oversight

LCO Recommendations 5-7 establish a provincial responsible criminal AI reporting and oversight regime. Recommendations include legislative provisions establishing:

- Comprehensive AI reporting requirements for provincial law enforcement agencies.
- A dedicated provincial supervisory authority for AI systems.
- A requirement for agencies to develop AI governance and operational policies.

These recommendations promote evidence-based criminal AI governance. They also support responsible AI adoption and public trust and accountability.

LCO Recommendations

5. The legislation should establish reporting requirements to Ontario's Inspector General of Policing and Law Enforcement Complaints Agency, who will provide an annual public report analyzing the use of AI by law enforcement services.
6. The legislation should establish the authority to create a dedicated provincial supervisory authority for AI systems in criminal justice.
7. The legislation should require law enforcement services to establish dedicated AI operational and governance policies and designate officials responsible for the policy's implementation.

Public Reporting and Oversight in Ontario's Criminal Justice System

There are many statutes, regulations and policies in Ontario ensuring public reporting and transparency in provincial law enforcement. These provisions are essential to good governance, effective oversight and public trust in law enforcement, especially in high risk contexts. For example, the *Community Safety and Policing Act, 2019* and other statutes and regulations establish provincial reporting requirements for:

- Annual reports from Chiefs of Police and the OPP Commissioner.
- Information collection in specified circumstances, such as street checks and carding checks.
- Annual reports on the use of force.
- Reports on missing persons investigations.
- Police discipline reports.²⁹⁸

Notably, the reporting requirements in these examples apply to all provincial law enforcement agencies.

Unlike use of force or street check reports, there is no provincial requirement to report on the use of AI in law enforcement or criminal justice generally. As a result, there is no comprehensive or publicly disclosed picture of how provincial criminal justice agencies are using AI, what the benefits and impacts of AI use may be, and whether the systems are cost-effective or meeting their objectives. To date, information about the use of criminal AI systems in Ontario and Canada has been voluntary, inconsistent or linked to specific controversies.²⁹⁹



Fortunately, there are some important Canadian precedents that commit to meaningful transparency and public disclosure. For example, both the TPS and RCMP make detailed reports on their AI systems publicly available.³⁰⁰ The TPS Use of AI policy also commits to a long list of transparency and reporting practices. (See the text box “**Toronto Police Service – Reporting Requirements**” below.)

Across Canada and in Ontario, the comprehensive TPS and RCMP policies are the exception, not the rule. Several other police forces, including Peel and Edmonton, have adopted narrower governance and disclosure policies centered on their deployment or piloting of specific AI technologies.

Regardless of the approach, both the IPC and OHRC note that existing reports from law enforcement agencies may fall short. For instance, the IPC raised several concerns with the format, timing, and extent of the first “AI inventory” report delivered internally to the Toronto Police Services Board in January, 2024.³⁰¹

The IPC and OHRC also raised concerns with the way AI assessment was conducted and conclusions about the appropriate risk-level assigned to technologies including automated license plate recognition systems.³⁰² It is unclear if the TPS investigated or responded to these concerns, and if any corresponding changes were made in policy or practice.³⁰³

This discussion highlights what is by now a familiar concern: Institution-by-institution reporting policies and practices could result in a patchwork of AI reporting obligations, uneven public disclosure of high risk criminal AI systems, higher legal risks in some areas of the province, operational inefficiencies, etc. The LCO believes these risks and concerns will worsen as AI spreads across more provincial police services and as other criminal justice institutions begin to deploy AI systems.

Patchwork reporting obligations also undermine responsible criminal AI adoption and public trust. Narrow or inconsistent AI reporting policies make it difficult for policymakers and the public to fully understand how AI is being used and what is, or is not, effective. Patchwork reporting obligations also undermine evidence-based policies and could lead to accusations of “secret policing.”³⁰⁴

The impact of patchwork reporting is already evident. Law enforcement agencies frequently told the LCO that they are often unfamiliar with what other agencies are doing.



Toronto Police Service – Reporting Requirements

The Toronto Police Service Use of AI Policy includes detailed reporting requirements to the Toronto Police Service Board.³⁰⁵ The Policy states that the Chief of Police:

1. Will not procure, utilize or deploy any new AI technology deemed to be of High or Moderate risk before reporting to the Board and obtaining its approval.
2. Will inform the Board, at the earliest possible opportunity, of the decision to procure, utilize or deploy a new AI technology deemed to be of low risk, and explain why the AI technology was ascribed this risk level;
3. When reporting to the Board in accordance with section 5, will describe, at a minimum:
 1. The operational need(s) the AI technology will address, including how use of the new AI technology will improve on current practices or operations;
 2. How the Service intends to use the AI technology;
 3. The risk level ascribed to the AI technology, why the AI technology was ascribed this risk level, and the rationale for continuing with the procurement, utilization or deployment requested despite the associated risk(s);
 4. The legislative authority for the collection of personal information;
 5. How the AI technology operates, including, where applicable, the source of the training data, what information will be collected, how and where information will be stored and how it will be disposed of, retention periods for the information collected, and evidence of the validity, accuracy and security of the AI technology under consideration, based on industry standards;
 6. The steps the Service will take or has taken to ensure the AI technology is used only in accordance with the *Police Services Act* and its regulations (as well as successor legislation), applicable privacy laws, Ontario's *Human Rights Code*, the *Charter of Rights and Freedoms* and other legislative and legal requirements, including training, and applicable governance;
 7. An evaluation of the AI technology's vendor, including its record with regard to data security and ethical practices;
 8. The results of any privacy impact and other assessment(s) that have been conducted;
 9. The feedback received from consultations with the Information and Privacy Commissioner of Ontario, the Ministry of the Attorney General, stakeholders and the general public, independent human rights experts, independent legal experts, independent technology experts, and affected communities;
 10. An analysis of possible unintended consequences of the proposed use of the AI technology from legal and human rights perspectives, including the potential for disproportionate impacts on *Human Rights Code*-protected groups, and steps the Service will take to mitigate these unintended consequences;

11. Where applicable, a legal analysis of potential challenges to the admissibility of evidence generated or impacted by the AI technology in criminal proceedings;
 12. The findings of any risk analyses carried out in accordance with section 1(d) above, and any additional analysis as appropriate, including any analyses required by the Information and Privacy Commissioner of Ontario;
 13. Any reports and documentation used in the evaluation of AI technology;
 14. A mitigation plan to:
 1. Mitigate the risks posed by the implementation of the AI technology, including risks of biased policing, infringement of privacy or other rights, chilling effects on freedom of expression, and risks of abuse or unauthorized access to information, and including the mitigation of any bias or quality issues in the training data used by the AI technology;
 2. Ensure that any use of the AI technology will be audited to ensure adequate and lawful use, in accordance with the purposes approved by the Board, and to monitor errors; and,
 3. Notify the Information and Privacy Commissioner of Ontario and/or any other applicable legal authority of any significant privacy breaches or other significant malfunctions that may result in harm to individuals, communities or Service Members, or may impact criminal proceedings;
 4. The estimated cost of acquiring and implementing the AI technology, including Will not procure, utilize or deploy any new AI technology deemed to be of High or Moderate risk before reporting to the Board and obtaining its approval;
 15. The estimated cost of acquiring the cost of adequate training in the use of the AI technology, and any additional costs or savings expected from the implementation of the AI technology; and,
 16. Proposed indicators that will be tracked by the Chief of Police aimed at determining whether the AI technology is achieving its intended goal and whether its deployment has had any unintended consequences, until it is determined by the Board that monitoring is no longer required;
4. Will develop and implement a public engagement strategy, commensurate with the risk level assigned to the new AI technology, to transparently inform the public of the use of the new AI technology that collects data about members of the public or assists Service Members in identifying, categorizing, prioritizing or otherwise making decisions pertaining to members of the public, prior to its deployment.

Infrastructure to Support Effective Criminal AI Reporting and Transparency

Recommendations 5, 6 and 7 establish the critical infrastructure needed to support an effective criminal AI reporting and public accountability regime.

Recommendation 5 would legislate “reporting requirements to Ontario’s Inspector General of Policing (IGoP) and Law Enforcement Complaints Agency (LECA), who will provide an annual public report analyzing the use of AI by law enforcement services.” Recommendation 20 provides additional details on this structure.

Recommendation 5 has three important benefits:

First, it would build and centralize criminal AI expertise within existing independent oversight agencies. This will promote their capacity to oversee law enforcement AI systems, to effectively investigate complaints, and to provide reports on systemic issues.

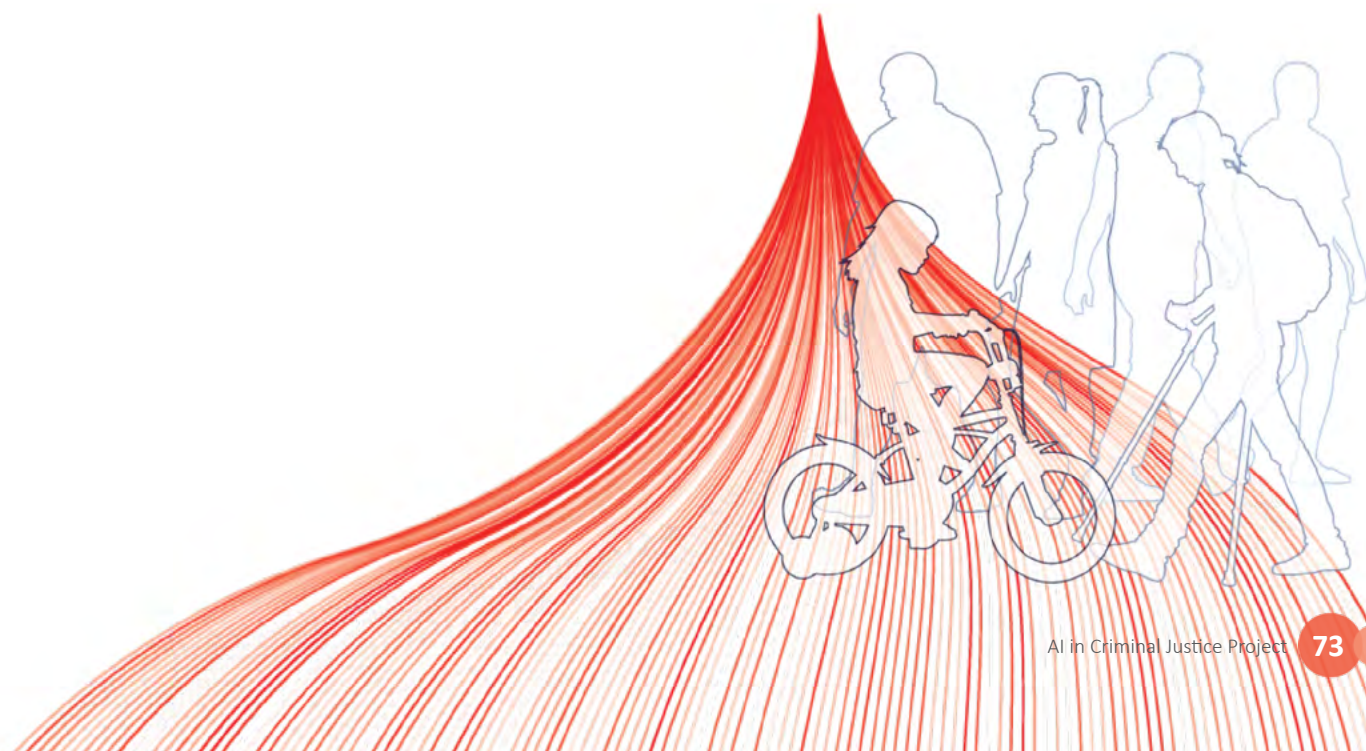
Second, it would require disclosure of all AI technologies used by law enforcement (independent of risk classification) such that these could be reported in a central public registry (discussed below).

Finally, Recommendation 5 ensures that investigative privilege is protected while continuing to provide oversight.

Recommendation 5 acknowledges that LECA and IGoP have distinct mandates and oversight roles. The implementation of this Recommendation must be flexible to account for practical issues, such as duplicate reporting, how to allocate responsibilities between the two agencies, etc.

Recommendation 5 is an interim measure. The LCO’s long-term recommendation (Recommendation 6) is to establish a dedicated provincial supervisory authority for provincial criminal AI systems. As will be discussed in greater detail below in Recommendation 19, the LCO has determined that AI technology is sufficiently distinct, complex and potentially transformative that an independent provincial supervisory authority is merited.

Finally, Recommendation 7 would establish an obligation on law enforcement services to establish dedicated AI governance and operational policies and designate officials responsible for the policy’s implementation.



Recommendation 8: Digital Sovereignty and Procurement

LCO Recommendation 8 protects digital sovereignty in Ontario's criminal AI systems. It would also establish legislative authority to regulate standard terms for third party AI vendor service contracts.

These recommendations are needed to ensure AI systems used by provincial criminal justice institutions have consistent and enforceable standards; ensure data is managed properly; respect Canadian laws; and reduce burdens on provincial criminal justice institutions.

LCO Recommendations

8. The legislation should require digital sovereignty over high risk and restricted use AI systems in criminal justice and regulate standard terms for vendor contracts necessary to fulfill all mandated assessment, disclosure and other obligations.

Digital Sovereignty

Digital sovereignty is the power of a country, organization or person to control its digital data, software and hardware. Digital sovereignty is seen as a way to protect rights, ensure privacy, control data, foster transparency and promote public trust in AI systems. Digital sovereignty is increasingly identified as a strategic national capability in sensitive sectors of the economy and public sector. Digital sovereignty also addresses operational security and continuity of operations.

A prominent example of digital sovereignty is the 2026 European Union strategy to “adopt an ambitious set of measures to bolster the EU’s digital autonomy.”³⁰⁶ The EU strategy states that the EU depends “on non-EU countries for over 80% of key digital products, services, infrastructure, and intellectual property”.³⁰⁷

The risks of digital dependence were exposed in June 2026 when the US government, citing national security concerns, ordered AI developer Anthropic to suspend foreign nationals’ access to Fable 5 and Mythos 5, two of its most advanced AI models.³⁰⁸ Anthropic promptly disabled the models for all foreign customers. Observers in Canada described the impact:

*Organizations in Canada, Europe and around the world that had embedded those tools in their workflows found them simply gone. No appeal process. No migration window. No warning. No jurisdiction over this decision... Canadian organizations need to treat AI dependency as a significant risk, not an IT purchasing question.*³⁰⁹

Los Angeles Police Department Inspector General Report

The LAPD Inspector General report discussed earlier in this report demonstrates the risks, and complexity, of digital sovereignty issues in the criminal justice system.

The LAPD Inspector General report highlighted serious concerns with the LAPD's three ALPR vendors for unauthorized data sharing, privacy violations, poor data security and retention practices, and an inability to determine contract compliance. Flock Safety was specifically criticized for apparently sharing data with federal agencies (including Immigration and Customs Enforcement (ICE)) even though it was expressly prohibited under California law.³¹⁰

To address these concerns, the LAPD Inspector General recommended several digital sovereignty-related measures, including "enforceable requirements governing data security, privacy, access controls, retention, and auditing to protect Department ALPR data and ensure accountability for its collection, use, and disclosure."³¹¹

The LAPD subsequently canceled Flock Safety camera services citing the need to renegotiate terms of service agreements to give the LAPD much greater control over the system, including proposed terms that will "require the data be stored in the continental United States" and to independently "grant the City the right to audit the vendor's data privacy and security program."³¹²

The LAPD also reports that it has begun working with the US-wide "Major City Chiefs Association to develop standardized contractual language to govern all ALPR vendor agreements going forward."³¹³

Canadian Police Services

In our consultations, Canadian police services discussed digital sovereignty and procurement issues frequently. They often told the LCO that:

- There are significant risks if domestic laws are not enforceable against foreign AI vendors.
- They often doubt AI vendor representations about the processing, storage and potential secondary uses of sensitive data.
- They are concerned about potential disputes with AI vendors about data ownership.
- They worry about their ability to negotiate vendor service contracts.
- They are concerned about their ability to conduct AI impact assessments, compliance and performance audits, source code reviews, bias testing and privacy protections.



Digital Sovereignty in Canada

Like the EU, the Government of Canada has taken several steps to address digital sovereignty in Canada.

First, it released its *Digital Sovereignty Framework* in 2025. The Strategy notes how a comprehensive level of control provides direct assurance that AI systems are operated in alignment with domestic laws, values and objectives.³¹⁴

Second, in 2026, the federal government released *Canada's National Artificial Intelligence Strategy*.³¹⁵ The *National Artificial Intelligence Strategy* includes several sections addressing digital sovereignty.³¹⁶

Finally, in 2026 the federal government introduced Bill C-36, the *Protecting Privacy and Consumer Data Act*.³¹⁷ Bill C-36 modernizes Canada's federal private sector privacy legislation. C-36 includes limited digital sovereignty provisions.³¹⁸

The LCO and our consultees believe it is important to protect digital sovereignty in the criminal justice system. Unfortunately, none of the federal initiatives address the unique and sensitive procurement risks associated with AI in criminal justice. Nor is the LCO aware of any provincial law or policy that does so. As a result, LCO Recommendation 8 recommends that provincial legislation require digital sovereignty over high risk and restricted use AI systems in criminal justice.

Standard Terms and Procurement Criteria

Recommendation 8 also recommends provincial legislation give the province the authority to specify standard terms for criminal justice AI vendor contracts.

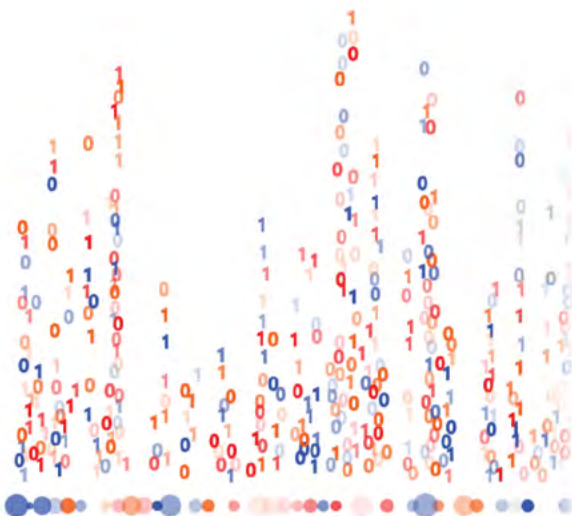
Recommendation 8 is closely tied to Recommendation 18, which would establish legislative authority to define dedicated procurement standards and regulations governing responsible software practices including software explainability, version control and archiving, training data disclosure and transparency, and the provision of reports assessing the reliability, validity and bias of the system.

These two recommendations would apply to AI systems designated as “high risk” and “restricted use” as per Recommendations 10-15. They would not apply to “low risk” AI systems.

Recommendations 8 and 18 provide four critical benefits:

First, standard terms would ensure digital sovereignty and consistent standards at scale. Among other benefits, consultees told the LCO that standard terms would:

- Ensure compliance with the AI transparency and disclosure requirements in federal Bill C-36, the *Protecting Privacy and Consumer Data Act*.³¹⁹
- Promote transparency and independent audits of the transmission, processing, storage, and potential secondary uses of sensitive data.
- Require appropriate notice periods for the withdrawal of AI services.
- Require data portability so data can be returned on request of the procuring institution.
- Prevent sensitive data from being “held hostage” by proprietary formats and contracts.



- Support pilot projects, program auditing, and continual iterative improvements.
- Facilitate direct access to the technology to test performance in “real-world conditions.”
- Facilitate independent confirmation of AI impact assessments, compliance and performance audits, privacy protections, transparency reporting, and bias testing.

Second, standard terms and procurement criteria promote consistency and efficiency between provincial institutions purchasing the same technology, alleviating the risks, costs and duplication associated with the “50 police services negotiating the same contract” issue the LCO frequently heard about.

Third, standard terms and procurement criteria could fulfill requirements essential to responsible AI or criminal law procedural and evidence requirements, such as:

- Information requirements for a public criminal AI register.
- Evidence rules that could require AI system explainability or access to source code/training data.
- Disclosure and risk mitigation requirements for AI risk assessments.
- Expert opinions, independent auditing or performance assessments for reliability and validity.
- Data privacy and security rules in sensitive court proceedings, such as sealed orders.

Finally, the LCO believes standard terms and procurement criteria will encourage vendors to build products that are “responsible AI by design.”

Why AI Procurement Standards Matter

Ontario’s Auditor General recently released a report showing how misguided procurement and assessment policies can undermine the validity and reliability of AI tools if appropriate standards and guardrails are not in place.

The report reviewed the procurement, use and performance of AI-based medical transcription and summarization tools in Ontario’s health sector.³²⁰ The report noted the reliability and accuracy of these tools is extremely important to patient safety and several statutory and professional obligations.

In practice, however, the Auditor General reported that the procurement framework developed by Supply Ontario weighed system “accuracy” at just 4% towards a system’s final procurement score.³²¹ In contrast, 30% of the score was awarded to tools “developed in Ontario.”³²² Upon review, the Auditor General found that the procured transcription tools had extremely high error rates.³²³

The lesson of this example is that the benefit of a technology can be lost if it is not assessed against foundational legal and operational requirements.

Recommendation 9: Public Engagement

Recommendation 9 requires the province to establish important public engagement and transparency measures, including public participation in AI assessment processes, annual reporting on how AI systems are being used, public participation in the provincial supervisory authority and bi-annual legislative reviews.

LCO Recommendations

9. The legislation should mandate several public engagement measures including public participation in AI assessment, annual reporting requirements, and a role for the public in the dedicated provincial supervisory authority, and legislative reviews every two years.

Public Engagement

There is a broad consensus that the public must be engaged in responsible criminal AI development, oversight and evaluation in Ontario. Public engagement is necessary to promote public safety, protect rights and ensure public trust in criminal AI systems across Ontario.

This consensus was confirmed at every stage of the LCO consultations. This consensus is also reflected in the UBC/LCO September 2026 *Draft Principles on the Governance & Use of AI by Police in Canada*. The tenth draft principle “Independent Third-Party Oversight & Public Engagement” states as follows:

*Engagement with the public and stakeholders helps build trust and ensures that rights-holders affected by AI systems have opportunities to provide meaningful input and feedback.*³²⁴

Support for public engagement is a consistent principle of responsible AI governance in every jurisdiction we researched.³²⁵

This principle is also widely acknowledged by police services across the world, including INTERPOL.³²⁶ The International Association of Chiefs of Police also states that public engagement and transparency about law enforcement use of AI is important for building trust.³²⁷

Finally, this principle has been confirmed by Canadian police services such as the TPS and RCMP and by Canadian governments.³²⁸

Recommendation 9 would elevate public engagement from an internal institutional policy to a provincial commitment. Recommendation 9 is one of several disclosure and oversight recommendations in this report.

Recommendations 10-15: Criminal AI Risk Management

LCO Recommendations 10-15 establish a comprehensive risk management framework to govern AI systems in Ontario's criminal justice system. These recommendations:

- Identify four risk categories that should be established in legislation, including prohibitions.
- Direct the province to conduct public consultations on risk management issues.
- Identify potential criteria, use cases and mitigation measures for each risk category.

Together, these recommendations match criminal AI governance obligations to a system's uses, benefits and risks; support responsible AI adoption; promote public trust; and uphold the principles and requirements of Canadian law.

Risk Management for Criminal AI Systems

AI risk management, risk categorization and “red lines” are probably the most consequential and high-profile strategy to build trust in AI systems and reduce AI risks. This is because AI risk management has the potential to eliminate or mitigate the most serious and high-profile AI risks. Not surprisingly, AI risk management and risk categories are a feature of almost all emerging responsible AI governance frameworks.

The EU *AI Act* is probably the best-known criminal AI risk management framework.³²⁹ The most notable criminal AI risk management framework in Canada is the Toronto Police Service's Use of AI Policy.³³⁰ Other Canadian examples include risk categories and frameworks adopted or recommended by the Canadian Association of Chiefs of Police, RCMP, Peel Police Service, Canadian Information and Privacy Commissioners, *EDSTA*, the LCO and others.³³¹

The LCO's research and consultations have revealed wide and deep support for criminal AI risk management. We also heard, however, that AI risk assessment regimes developed so far have important gaps and limitations. To address this need, the LCO led a two-year collaborative process to facilitate discussions on the potential objectives, risk categories and details of a risk management framework for the provincial criminal justice system. The result of this process is reflected in Recommendations 10-15.

The model and recommendations below have been widely vetted by stakeholders who reflect a wide variety of institutions in the criminal justice system. The LCO believes our recommended model consolidates best practices developed in Canada, including those developed by law enforcement agencies, courts, professional regulators and legal professionals.

Our model and recommendations reflect several principles and objectives that were widely supported in our consultations, including:

- There is a need to govern criminal AI systems based on risk.
- It is a priority to identify and mitigate the risks of high impact criminal AI systems.
- Risk management supports responsible AI adoption, legal accountability, and public trust in the criminal justice system.
- Risk management categories should be mandatory and consistent.
- Risk levels and assessment must be based on Canadian criminal law.
- There is a need to reduce duplication and ensure consistency and interoperability across and between large and small institutions.
- Risk management should be supported by centralized expertise, monitoring and certification.
- Public engagement is necessary.

Recommendations 10-15 set out a comprehensive plan and framework to fulfill these principles and objectives. Recommendations 10 and 11 establish the baseline or prerequisites of this framework. Recommendations 12 to 15 address specific issues.

Recommendations 10-11: Risk Categories and Public Consultations

LCO Recommendations

10. Provincial legislation should prescribe four risk categories for criminal justice AI systems used in Ontario, including “prohibited”, “high risk”, “restricted use” and “low risk” systems.
11. The provincial government should conduct public consultations to identify the risk criteria, contexts and uses of AI systems, including but not limited to systems that may be prohibited, pre-emptively identified as high risk, or otherwise subject to higher regulatory standards.



Legislated Risk Categories

Recommendation 10 would legislate four categories of criminal AI system risks:

- Prohibited.
- High Risk.
- Restricted Use.
- Low Risk.

In our view, these categories would establish the baseline of a provincial risk management framework for criminal AI systems. These categories reflect several decisions.

First, these categories are consistent with the risk categories in the EU *AI Act* and other international legislation and frameworks. The EU *AI Act* includes four categories of risk, including “Unacceptable Risks,” “High risk,” “Limited Risk,” and “Minimal or Low Risk” AI systems.³³²

Second, these categories are consistent with established Canadian AI risk categories, including those included the federal ADM Directive, *EDSTA* and the Toronto Police Use of AI Policy.³³³ (See the text box “**Toronto Police Services Board AI Policy Risk Categories**” on the following page).

Finally, the four risk categories reflect a “made in Canada” approach. The LCO consistently heard that the assessment of criminal AI risks and mitigation measures must prioritize compliance with Canadian criminal law, including the *Charter*, criminal law and procedure, evidence law, privacy law and human rights law. The “prohibited” and “high risk” categories recommended are directly linked to protecting these criminal law rights.

These categories were widely supported in our consultations as reflecting an appropriate sliding-scale of AI system capabilities, risks and mitigation measures.

Importantly, the LCO believes these categories should be established in legislation or regulations given their importance to responsible AI governance and the need for provincial consistency.

The LCO has already seen significant support for this approach. As discussed above, the draft Canadian Association of Chiefs of Police draft AI guidance framework and AI risk assessment tool includes a commitment to assess AI through four standard risk classifications (including AI prohibitions).³³⁴

Public Consultations

Recommendation 10 establishes broad risk categories. Recommendation 11 commits the province to public consultations important AI risk management issues within those categories, including risk criteria, context and uses of such systems.

Public consultations and engagement on these issues is crucial, particularly for high risk criminal AI systems such as FRT or predictive policing where public skepticism is high. Public consultations promote better decision-making and public trust.

In the LCO’s view, Recommendations 10 and 11 are the building blocks for any successful criminal AI risk management framework in Ontario.

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.

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

Recommendations 12 to 15: Risk Criteria, Practices and Mitigation

Broadly speaking, the purpose of Recommendations 12 to 15 is to “fill in the details” of each of the four categories established in Recommendation 10. More specifically, Recommendations 12 to 15 identify 1) the criteria or use cases to determine whether a criminal AI system should be prohibited or considered high risk, restricted or low risk, and 2) the measures to mitigate that risk.

The LCO is confident Recommendations 12-15 are coherent and sound. Nevertheless, as per Recommendation 11, the LCO believes these Recommendations should be consulted upon given their complexity and impact, and the importance of public trust.

Before discussing specific recommendations, it is important to set out two starting assumptions.

Priority for Canadian Law

As per Recommendation 4.a, the LCO believes that the rights defined in Canadian criminal law must be the principle lens through which AI technologies in criminal justice are assessed, operationalized and measured for compliance.

The LCO believes a rights-based approach addresses the most consequential risks and impact of criminal AI systems. We also believe the four risk categories will encourage if not assure thoughtful consideration of variable impact on rights between and within criminal AI systems.

Importantly, a rights-based approach is inherently linked to managing AI as a lifecycle challenge. Rights are the language and rules shared in common across criminal justice institutions. It is the bedrock on which policies, practices and procedures within and between institutions are defined. By placing these rights at the core of an assessment model, this priority promotes system-wide consistency.

Risk Criteria, AI Practices and Mitigation

Recommendations 12-15 identify specific risk criteria, practices and mitigation measures for each of our four recommended risk categories.

The risk criteria, AI practices and mitigation measures we identify for each category reflects a combination of current or emerging standards and practices in responsible criminal AI governance in Canada and internationally. Readers should note these recommendations are inclusive rather than conclusive. We recommend provincial consultations on these details to ensure the best decision-making and to promote public accountability and trust.



Recommendation 12: Prohibited AI Systems

LCO Recommendations

Prohibited AI Systems

1. Prohibited AI systems in criminal justice could include following:
 - a. Prohibited Risk Criteria
 - i. Prohibited AI systems are those posing unacceptable risks to fundamental rights and Canadian values.
 - ii. Unacceptable risks may include uses for AI that are particularly harmful and contradict Canadian values of respect for fundamental rights under the *Charter* (including fundamental freedoms, democratic rights, mobility rights, civil liberties, equality and the rule of law), rights established in federal and provincial human rights codes (including inherent dignity, equality, and protection from discrimination and harassment), privacy rights, and procedural fairness.
 - b. Prohibited AI Practices
 - i. Real-time remote biometric surveillance, including direct identification of individuals (facial recognition) or object detection for the purpose of inferring identity (object tracking, gait analysis, geolocation, etc.).
 - ii. Individual criminal offence risk assessment and prediction, including assessing eligibility and conditions for bail.
 - iii. Social scoring to evaluate or classify natural persons or groups of persons based on social behaviour or personal or personality characteristics, with the social score leading to detrimental or unfavourable treatment.
 - iv. Emotion recognition.
 - v. Biometric categorization based on biometric data to deduce or infer race, political opinions, trade union membership, religious or philosophical beliefs, or sexual orientation.
 - vi. Predictive systems to forecast the likelihood that a person will commit a criminal offense or the predicted location of criminal activity.
 - vii. Agentic AI systems, other than for backend administrative purposes deemed low risk.
 - viii. Adjudication of criminal cases and conduct investigations of criminal justice professionals.



Prohibited Criminal AI Systems

As noted above, AI prohibitions and “red lines” are probably the most consequential and high-profile strategy to build trust in AI systems and reduce AI risks. For example, AI red-lines or prohibitions on police use of live FRT could drastically minimize the risks of FRT-enabled mass surveillance, over-policing of racialized communities and mass privacy violations.

Internationally, many governments have enacted or proposed bans on certain criminal AI technologies or their use in criminal specific circumstances. The EU AI Act (Chapter II) prohibits several AI practices that are relevant to law enforcement, including:

- **Person-specific predictive policing:** AI systems that predict an individual’s likelihood of committing a criminal offence based solely on profiling or using their personality traits are prohibited. However, human investigators can be supported by AI in assessing an individual’s criminal involvement based on “objective and verifiable facts directly linked to a criminal activity”.³³⁵
- **Facial recognition using scraped images:** AI systems that indiscriminately scrape images (from the Internet or CCTV) to create or enhance facial recognition databases are prohibited.³³⁶
- **Biometric categorization for sensitive traits:** AI systems that infer protected characteristics—race, religion, political opinions, trade-union membership, sexual orientation, etc.—from biometric data are prohibited. However, law enforcement agencies may still label or filter datasets that they have lawfully acquired for investigative purposes.³³⁷
- **Real-time remote biometric identification in public spaces:** Live facial recognition—or other remote biometric ID systems—used by police in public is generally prohibited. There is an exception, with strict safeguards set out in the legislation (e.g. prior judicial approval), when strictly necessary for one of the following objectives to verify the identity of a specific individual:
 - o Targeted searches to locate specific victims or missing persons (e.g., abductees, trafficking victims).
 - o Averting an imminent, serious threat to life or a foreseeable terrorist attack.
 - o Identifying a suspect of a serious offence (punishable by at least four years’ custody) during investigation, prosecution, or sentence execution.³³⁸

The most important Canadian example of AI prohibitions and “red lines” in policing is the TPS Use of AI Policy. This policy identifies at least seven prohibited “extreme risk technologies.” which “may not be considered for adoption”:

1. Any application where there is no qualified “human-in-the-loop”. A qualified human must evaluate a recommendation from an AI tool before consequential action is taken, and be accountable for any decision made based on this recommendation.
2. 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.
3. 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.
4. 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.

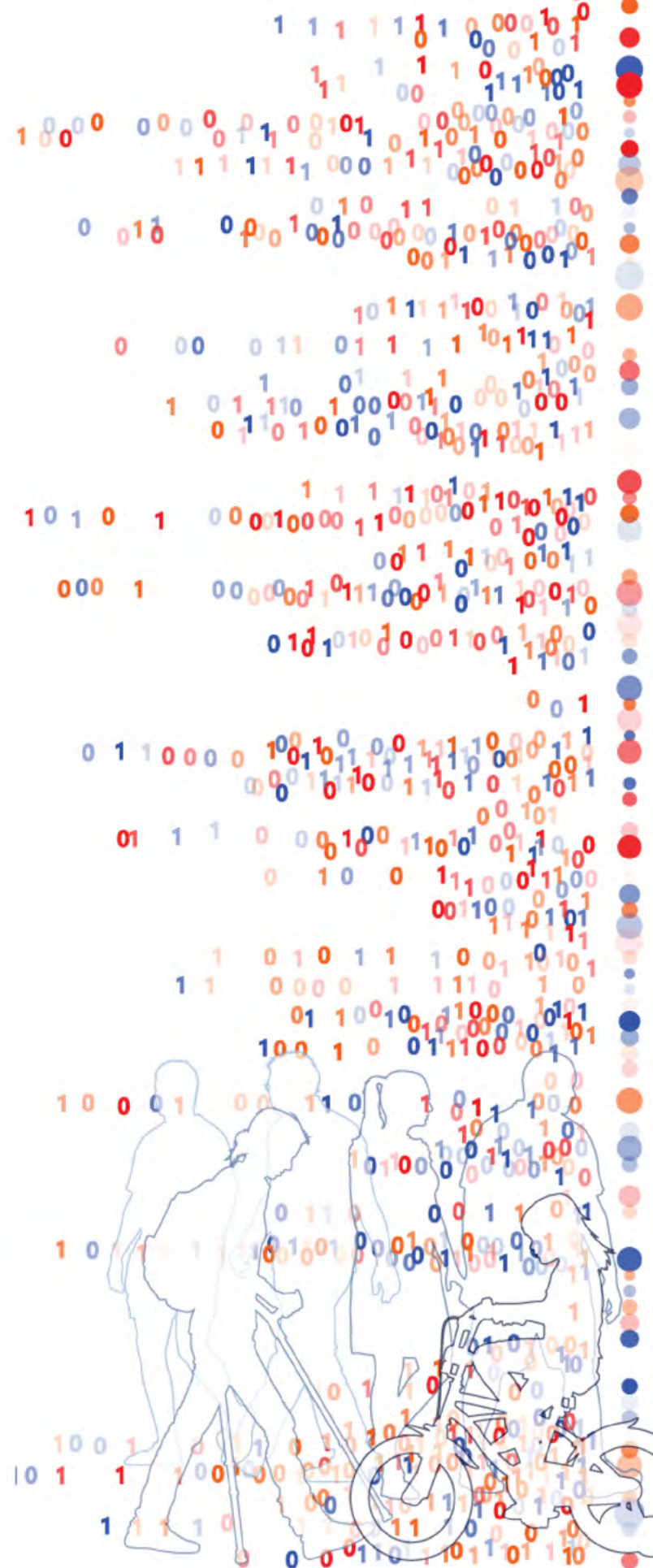
5. Any application used to predict or assign likelihood of an individual or group of individuals to offend or reoffend;
6. Any application making use of data collected in accordance with the Board's *Regulated Interaction with the Community and the Collection of Identifying Information Policy*, or any Historical Contact Data as defined in that Policy; or,
7. Where training or transactional data is known or thought to be illegally sourced, or where it is from an unknown source.³³⁹

The authority to legislatively prohibit certain kinds of AI systems is also included Ontario's *EDSTA*³⁴⁰ and in the proposed federal *Artificial Intelligence and Data Act*.³⁴¹

The LCO / UBC Law Vancouver Symposium on AI in Policing demonstrated substantial support for the prohibited uses of AI set out in the EU *AI Act* and the TPS Use of AI Policy. Participants also noted that:

- A thoughtful list of presumptive “red lines” or prohibitions could prevent overbroad use of FRT.
- Baseline expectations governing all AI systems would be helpful.
- There is support for prohibiting the autonomous use of force by AI-enabled police robots/drones.

Recommendation 12 reflects the LCO's preliminary assessment of criminal AI systems with the highest risks/impact and that could affect the most people. The proposed list of Prohibited AI practices reflect consensus throughout LCO's consultations and reflects areas where police and other criminal justice institutions have demonstrated hesitancy to adopt AI.



Recommendation 13: High Risk AI Systems

LCO Recommendations

High Risk AI Systems

13. High risk AI systems in criminal justice could include the following:

a. High Risk Criteria

- i. High risk AI systems are those posing a reasonably foreseeable risk of harm to fundamental rights under the *Charter* (including fundamental freedoms, democratic rights, mobility rights, civil liberties, equality and the rule of law), rights established in federal and provincial human rights codes (including inherent dignity, equality, and protection from discrimination and harassment), privacy rights, or procedural fairness.
- ii. Reasonably foreseeable risks include but are not limited to: systems that materially influence the outcome of a decision or have a differential impact on vulnerable groups.

b. High Risk AI Practices

- i. Biometric Identification.
- ii. Object identification and tracking systems, such as license plate readers.
- iii. Surveillance, including the collection use and analysis of personal information or online “open-source” publicly available personal information, and surveillance on the basis of personal characteristics and behavior such as location and movement, speech, features, and physical interactions amongst groups and/or individuals.
- iv. Forensic analysis, including analyzing both digital and physical evidence as it relates to investigating a specific criminal incident.
- v. AI generated description, summary or transcription of speech and events, and the generation or editing of incidence / occurrence reports.

vi. Production of any forms of AI evidence that may be relied on in proceedings with lower evidentiary burden including bail hearings, diversion hearings, and applications for judicial authorization.

vii. Cross-linking, comparing, comingling or otherwise subjecting different databases to AI analysis, including voluntary third party disclosures.

c. Mitigation

- i. Risk-based regulations should tailor legal obligations proportionately so that the most onerous obligations only attach to the highest risk systems. Risks associated with High Risk AI Systems could be mitigated measures including, but not limited to:
 - rights impact assessment and assessment of lawful purpose and scope of use;
 - procurement standards;
 - a requirement to only use previously assessed and authorized AI software and devices in the scope of any profession duty;
 - procedural protections including human-in-the-loop certification of outputs and ongoing labeling of AI throughout the chain of evidence;
 - AI compliance by design including audit trails for prompts and alterations;
 - adequate technical and performance assessment for reliability, validity and bias tested in real-world conditions; and
 - ongoing documentation, transparency, reporting, oversight and quality management systems.



Recommendation 13 identifies proposed criteria and practices to identify “high risk” criminal AI systems. These systems would not be prohibited but subject to comprehensive mitigation measures, which are also identified in the recommendation.

In the LCO’s view, AI systems should be considered “high risk” where they present foreseeable risks and impacts to fundamental rights and freedoms, including legal rights established under the *Charter*, criminal common law, evidence law, procedural fairness, and human and privacy rights. LCO consultations confirmed a generally held view against the idea of assessing a hierarchy of “diminished” or “low” risks to rights when any risk to rights is of high risk to individuals and society.

A rights-based approach to risk assessment is more inclusive, grounded in Canadian law, and technologically neutral. For example, it would encompass the several specific examples of pre-emptively designated “high risk technologies” in the TPS Use of AI Policy, including:

1. 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;
2. Where training data can be influenced or biased by malicious actors;
3. Applications which link biometrics to personal information (e.g. facial recognition);
4. Where the proposed system could be used to assist in the identification of individuals for the purpose of their arrest, detention or questioning;
5. Where the process involved suggests an allocation of policing resources;
6. Where a system that otherwise merits a Moderate risk assessment lacks independent validation; or,
7. Where a system cannot be fully explainable in its behaviour;

Chapter III of the EU *AI Act* also 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.³⁴² The EU *AI Act* sets out important mitigation 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.³⁴³

Recommendation 13 includes systems that are high risk and high-impact, and which may impinge on positive and negative rights defined in criminal common law and procedure. The proposed list of high risk AI practices reflects real-world applications of AI that are raising concerns in Canada and across the world.

The Role of Exemptions, Emergencies and Exigent Circumstances

LCO consultations discussed the role for exemptions, emergencies and exigent circumstances under the prohibited and high risk assessment categories.

For instance, at the Vancouver Symposium, participants discussed the benefits of identifying authorized uses of FRT in advance, such as FRT to assist police in public emergencies or to support investigations for human trafficking, missing persons, or child sexual exploitation cases. Participants noted that any list of authorized FRT uses needed to account for the wide range of police services and responsibilities in Canada. The RCMP, for example, has a protective mandate for domestic and foreign VIPs, which may require different standards.

The LCO has chosen not to make recommendations on potential exemptions, emergencies or exigent circumstances authorizing criminal justice AI use for several reasons.

First and foremost, the issue of exceptions, emergencies and exigent circumstances involve legally complex and nuanced analysis of judicial authorization, emergency proceedings, etc. This project did not have the time or capacity to assess these issues. The LCO suggests that future work developing a legislated and regulatory framework for AI in criminal justice take up these issues.

That said, the LCO offers a few comments.

First, the LCO was told that many potential exceptional uses of police AI, such as mass real time biometric surveillance, could infringe the *Charter of Rights* suggests that many proposed exceptions are likely to violate fundamental rights of Canadians. This position is proven, perhaps, by the fact that no police force in Canada has as yet (as far as we know) proposed using such a system.

Second, the exceptions, exigent circumstances and emergency contexts included in the EU *AI Act* are not necessarily comparable or applicable to Canadian law. The EU has a unique governing structure between member states. Exceptions defined under the EU *AI Act* do not automatically operate as national exceptions but rather must be interpreted within the context of each nation's domestic law.³⁴⁴

Why are AI Scribes A “High Risk” Technology?

“AI scribe” systems can be put to a variety of tasks in criminal justice. In policing they are often marketed for their ability to streamline evidence review and redaction; scan hundreds of hours of video to identify, describe, transcribe and summarize events; and to draft police incident reports.³⁴⁵

While the benefits are obvious, the risks are less so. Yet AI scribes can pose systemic risks to the reliability and validity of evidence in criminal justice, and undermine criminal law rights.

First, AI scribes may hallucinate, mischaracterize key issues, or provide sycophantic output.³⁴⁶ For instance, body cam video is recorded at a perspective can give routine activities a dramatic effect, and this can be misinterpreted or mischaracterized by the AI summary.³⁴⁷ While the introduction of errors may be occasional or appear inconsequential, such errors can be multiplied in systems used at scale. This is particularly the case if human investigators are unable to adequately confirm the AI output.

Other jurisdictions demonstrate how AI scribes may be manipulated or abused, can distort police testimony and recollection, and are often used without disclosure.³⁴⁸

Peel Police Service is among the first major police forces to formally adopt AI scribe tools, having assessed the need to invest significant procedural checks and balances to use the technology safely and with a continuous and layered “human in the loop” process.³⁴⁹

Recommendation 14-15: Restricted Use / Medium Risk and Low Risk Technologies

LCO Recommendations

Restricted Use AI Systems

14. Restricted use AI systems in criminal justice could include the following:

a. Restricted Use Risk Criteria

- i. Restricted Use AI systems are those posing risks of adverse impacts on individuals or society; harm to the administration of justice; or which may undermine public confidence in the criminal justice system.

b. Restricted Use AI Practices

- i. Front-end support tools that aid in non-investigatory interactions with the public. Examples include (but are not limited to):
 1. Voice recognition or chatbot systems that provide an intake, triage, or informational function.
 2. Translation and transcription, including post-facto and real-time services.
 3. Generating or altering audio, image, video or text content.
 4. AI queries for legal or policy information or guidance shared or acted on in the course of professional duties to the public.
- ii. Use of AI by judges, crowns, and defence to analyze or prepare legal materials or submissions including evidentiary analysis, disclosure, facts and submissions, as an aid to drafting judgments, and other material.

c. Mitigation

- i. Risk-based regulations should tailor legal obligations proportionately so that the most onerous obligations only attach to the highest risk systems. Risks associated with Restricted Use AI systems could be mitigated measures including, but not limited to:
 - Rights impact assessment;
 - Assessment of lawful purpose and scope of use;
 - Procurement standards;
 - A requirement to only use previously assessed and authorized ai software and devices in professional duties;
 - Procedural protections including human-in-the-loop certification of outputs and ongoing labeling throughout the chain of evidence;
 - Development of the ai system to achieve compliance by design including audit trails for prompts and alterations;
 - Adequate technical and performance assessment for reliability, validity and bias tested in real-world conditions;
 - Ongoing documentation, transparency, reporting, oversight and quality management systems.
 - Ongoing professional training and practice enforcement related to the weaknesses and responsible use of ai systems and notice to the public about the use of an AI system.



Restricted Use Technology

Recommendation 14 identifies proposed criteria and practices to identify “restricted use” criminal AI systems. These systems would not be “prohibited” or “high risk” but are subject to comprehensive mitigation measures, which are also identified in the recommendation.

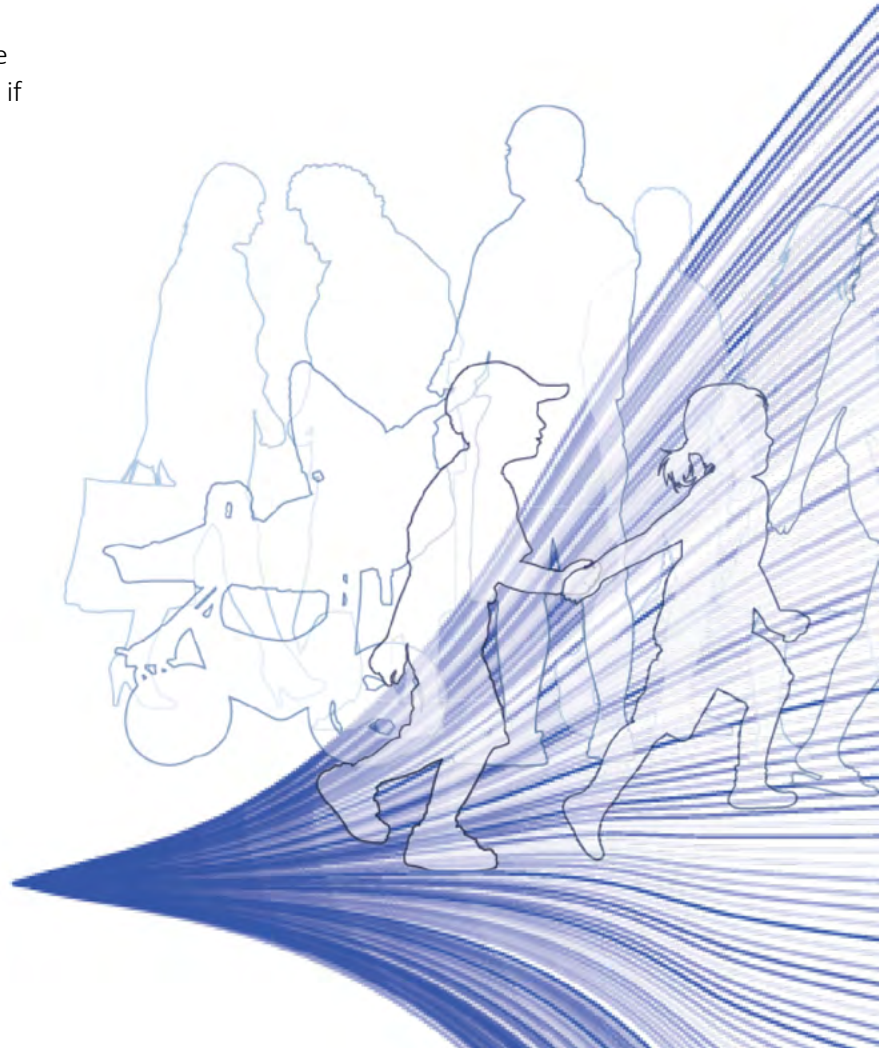
In the LCO’s view, AI systems should be considered “restricted use” where they pose risks of adverse impacts on individuals or society; harm to the administration of justice; or which may undermine public confidence in the criminal justice system.

The LCO’s “restricted use” AI systems are often described as “medium risk” in other risk assessment regimes. LCO consultees preferred the term “restricted use” because it acknowledges the ongoing potential of these systems to violate rights.

Many “restricted use” AI systems take the form of administrative or procedural aids that can supplement or supplant human-based work and systems to achieve greater productivity and efficiency. While perhaps outwardly benign, these systems can pose systemic risks to the criminal justice system.³⁵⁰ These risks could appear in individual cases or systemically if these AI tools are adopted widely.

Recommendation 14 identifies several such AI technologies, including:

- Voice recognition or chatbot systems that provide an intake, triage, or informational function.
- Translation and transcription systems, including post-facto and real-time services.
- Systems that generate or alter audio, image, video or text content.
- AI queries for legal or policy information or guidance shared or acted on in the course of professional duties to the public.
- Use of AI by judges, Crowns, and defence to analyze or prepare legal materials or submissions including evidentiary analysis, disclosure, facts and submissions, or as an aid to drafting judgments, and other material.



LCO Recommendation

Low Risk AI Systems

15. Low Risk Uses of AI in Ontario's criminal justice system should consider incorporating the following:
 - a. Low Risk Criteria
 - i. Low Risk AI systems are those that do not pose any risk of harm to fundamental rights, risk of adverse impacts on individuals or society, harm to the administration of justice, or which may undermine public confidence in the criminal justice system.
 - ii. Low Risk AI systems include AI systems which perform a narrow procedural or preparatory task, do not materially influence or replace the outcome of an assessment or decision making, and are easily corrigible or reversible.
 - b. Low Risk AI Practices
 - i. Backend administrative systems that may aid in routine internal functions or management operations, reducing time or labor, gaining efficiencies or training.
 - ii. AI systems that perform an assistive function for standard editing or do not materially alter the input data provided by the user.
 - iii. Use of AI enabled security tools for the purpose of data security within criminal justice organisations.

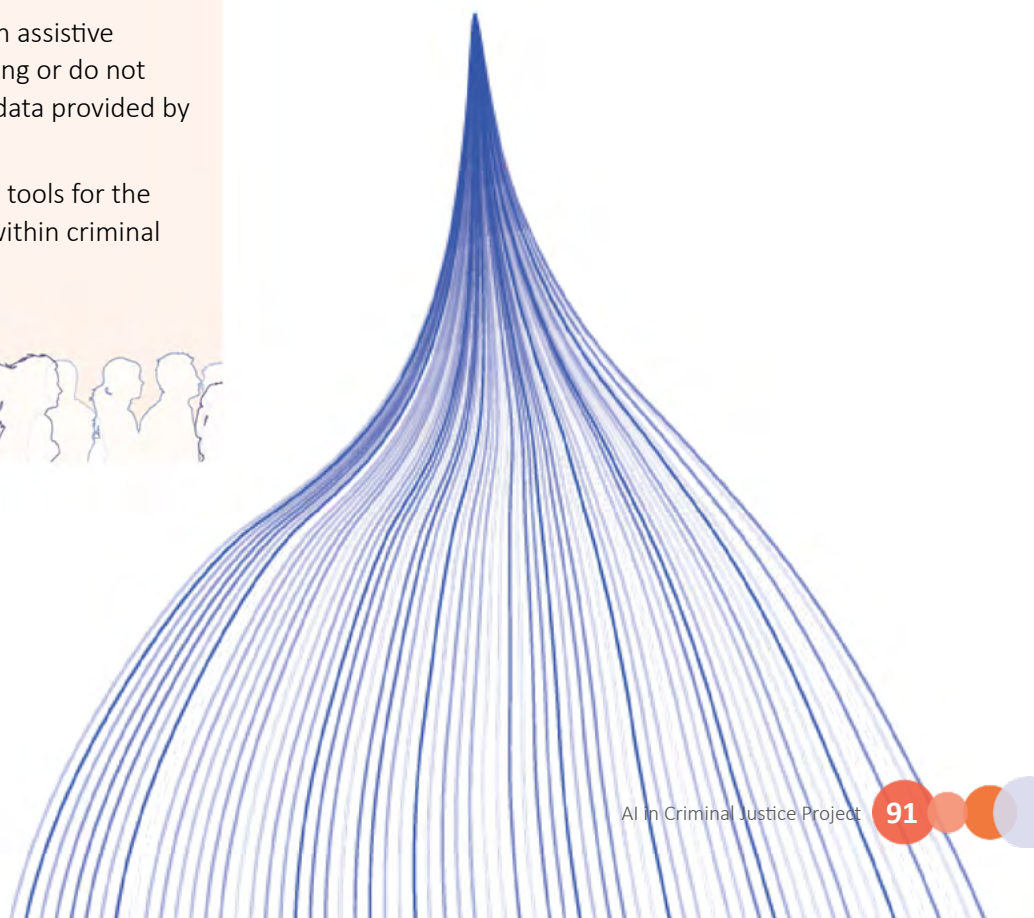
Low Risk Systems

Recommendation 15 proposes criteria to identify “Low Risk” AI systems as those that do not pose any risk of harm to fundamental rights, risk of adverse impacts on individuals or society, harm to the administration of justice, or which may undermine public confidence in the criminal justice system.

“Low Risk” systems perform a narrow procedural or preparatory task, do not materially influence or replace the outcome of an assessment or decision making, and are easily corrigible or reversible.

In our view, the precautionary principle included in Recommendation 4 means that “low risk” systems should still be identified, assessed and categorized. This would ensure low risk systems are registered, reported and publicly scrutinized to protect against misclassification and under-estimation of risks.

Examples of “low risk” practices include backend administrative systems that may aid in routine internal functions or management operations, standard editing (such as spell checkers) that do not materially alter the input data provided by the user, and the use of AI enabled security tools for the purpose of data security within criminal justice organisations.



Recommendation 16: Public Criminal AI Registry

Recommendation 16 establishes a comprehensive public registry for AI systems used in Ontario's criminal justice system. The Recommendation identifies key details to be included and mandates regular reporting obligations.

LCO Recommendation

16. Provincial legislation should require mandatory disclosure of AI systems in criminal justice, including posting of key details about the system on a public registry.
 - a. Public disclosures should include key information about the purpose, general capabilities, risk categorization, mitigation strategies, and relevant impact assessments about the AI systems.
 - b. Public disclosure obligations reports should account for the independence of the judiciary and investigative privilege for law enforcement.
 - c. Public disclosures should be updated upon a material change in the capabilities, purpose or use of the system or annually, whichever comes first.

Public Criminal AI Registry

LCO research demonstrates that many leading jurisdictions have adopted AI registries and/or transparency reporting requirements as critical planks in their responsible AI governance strategies.

For instance:

- The Government of Canada has established an AI Register that includes information about 414 AI systems “that are or have been in use within the GC” including from some institutions that “have also chosen to provide information about pilot and proof-of-concept projects.”³⁵¹
- Two of Canada's largest law enforcement agencies have each adopted voluntary AI transparency practices. The RCMP's National Technology Onboarding Program has published several assessments using the federal Algorithmic Impact Assessment Tool; and the Toronto Police Service have created a public website listing AI being used or under consideration.³⁵²
- US states including New York, Texas, Washington and Connecticut either expressly require transparent registration of law enforcement and criminal justice uses of AI or include criminal justice institutions in general AI registers. Several other states, most notably California, have mandatory reporting requirements but not necessarily a public registry.³⁵³
- The EU AI Act establishes centralized registry databases for high risk and lower-risk systems, maintained by the European Commission in cooperation with Member States, and includes provisions to protect sensitive systems used by law enforcement.³⁵⁴

AI Registries in Ontario

The province of Ontario has established a Trustworthy AI Framework that includes *EDSTA*, the *Responsible Use of AI Directive* and the “AI Use Case Inventory” which “lists AI tools and solutions used across the Ontario Public Service”.³⁵⁵

The Framework demonstrates the province's commitment to making AI governance and transparency tools accessible to the public, including mandatory transparency through a public AI registry. Notably, the Framework is sensitive to specific systems and use case.³⁵⁶

Notwithstanding this commitment, Ontario's current AI use case registry is very limited. Only three “AI use cases” are disclosed from across the entire OPS (despite various news headlines, investigative reports, and public presentations disclosing many other consequential uses).³⁵⁷

The LCO is also concerned that the information provided is rudimentary and not actionable.³⁵⁸ Further, the registry excludes any AI systems “in the planning/development stages” that “have not yet been deployed into production.”³⁵⁹ Most critically, the Framework excludes criminal justice institutions, which means they are not obligated to post AI their systems on Ontario's public registry. As a result, criminal AI disclosure in Ontario is on a voluntary, self-governing, and effectively *ad hoc* basis.

Many of these issues were discussed in a recent Auditor General of Ontario report criticizing the provincial government's lack of “measured and planned approach to identify and prioritize the use of AI within various sectors or program areas in the OPS.”³⁶⁰ The Auditor General was also concerned that the government has “not explicitly identified any prohibited AI practices or areas where the use of AI may pose unacceptable risks to the public and should be banned.”³⁶¹ These same criticisms could be made of AI in Ontario's criminal justice system.

Currently, the leading criminal AI justice disclosure/reporting regime in Canada is the Toronto Police Services Board “Use of Artificial Intelligence” policy.³⁶² The full details of the TPS's reporting obligations are included in the text box “**Toronto Police Service – Reporting Requirements.**” These commitments have been operationalized, in part, by a public website which appears to be an ongoing registry of AI uses by the TPS.³⁶³

The TPS AI registry includes several transparency practices both crucial and specific to the high risk nature of using AI tools in criminal justice.

First, each technology is disclosed and categorized according to the TPS's self-assessed AI risk scale. This is important because it demonstrates the practicality of disclosing all AI uses cases, including those deemed “low risk” uses. The risk categorization flag also provides the public with actionable information. Under the TPS Use of AI policy, for example, each risk category correlates to a proportionate series of governance and operational guardrails. The registry helps the public understand—or question—the sufficiency of governance and operational guardrails for specific AI use cases.

Second, the TPS AI registry lists all AI technology use cases, including systems currently being tested or piloted.³⁶⁴ This practice is distinguished from the Ontario government's AI Use Case registry, which specifically excludes disclosure of AI systems “in the planning/development stages” that “have not yet been deployed into production.”³⁶⁵ The TPS disclosure provides the public with an opportunity to engage with technologies before they are relied upon in high-stakes circumstances that may be subject to investigative privilege and other exemptions (and thus shielded from public input).

Third, the TPS registry provides more information than the Ontario AI registry about high risk technologies. Reporting headings for high risk technologies include:

- The name of the vendor.
- A description of the technology and its intended use case.
- How the system collects and processes information.
- Who the authorized users are (and thus who is responsible to answer for the system).
- Steps taken to mitigate risks associated with use of the system.

The LCO's assessment of the TPS registry is that it is commendable but limited. For example, RCMP assessment reports provided under the federal Algorithmic Impact Assessment provide a much fuller picture of the benefits and limitations of AI systems.³⁶⁶ Unlike the TPS registry, RCMP reports outline the lawful authority and use case for using the tool; the reliability and validity of the tool, including any independent assessment studies; the results of privacy impact assessments; and an outline mitigation measures.

AI disclosure and transparency concerns are not limited to police services. For their part, Ontario courts have established, or are in the process of establishing, various AI disclosure, practice, and evidentiary rules. However, these rules are generally directed at litigants.³⁶⁷ In contrast, the Canadian Judicial Council's *Guidelines for the Use of Artificial Intelligence in Canadian Courts* is more comprehensive and outlines various risks and best practices for the use of AI by judges.³⁶⁸

Notwithstanding these efforts, concerns have been raised about transparency in the use of AI tools by the judiciary and court staff. Professor Amy Salczyn, for example, has discussed the "growing problem of shadow AI use" by the judiciary, including those "uses of AI that are not formally approved or are even contrary to formal policies."³⁶⁹ Professor Salczyn states that these concerns

*...highlight the need for more transparency and greater public conversation about the use of AI [by courts] in our justice system. It would be much better to have this conversation publicly and proactively, rather than reactively when AI-generated errors are spotted in judicial decisions or when judgments without any errors are audited for AI-generated content.*³⁷⁰

The LCO believes it may be possible for an AI registry to address judicial AI use thoughtfully. For instance, while courts may have clear internal policies governing AI use, an AI registry could include public versions of those policies that would promote transparency and build confidence in the administration of justice and protect judicial independence.

Finally, there are concerns about the use of AI by Crown Attorneys. Ontario's Ministry of the Attorney General is known to use tools including Microsoft Co-Pilot AI in the preparation of cases and for research on internal databases of cases, memos, templates, policies, and other material.³⁷¹ At present, there is no entry in the Crown Prosecution Manual reporting on how AI tools are used by the Crown, including in potentially public- and court-facing documents.³⁷² Courts and defence counsel have raised concerns that Crown documents may become less trustworthy if Crown AI tools are not disclosed or governed appropriately.

Over the last several years, there have been many discussions about the level of detail that should be included in AI disclosure and transparency policies. The LCO acknowledges these are complex issues. Fortunately, there are many helpful precedents to guide provincial policymakers, including the TPS AI Policy and the EU *AI Act*. The EU *AI Act*, for example, requires criminal AI systems disclosure to include:

- Vendor identity and contact information.
- AI system name/trade name.
- Lawful purpose and use case.
- A basic description of the inputs/data and operating logic.
- System status; including as an operational technology, pilot project, or under evaluation.
- Identification of a most-responsible human-in-the-loop.
- Summaries of impact assessments, including criminal rights, evidence law, privacy law, human rights, and procedural fairness.³⁷³

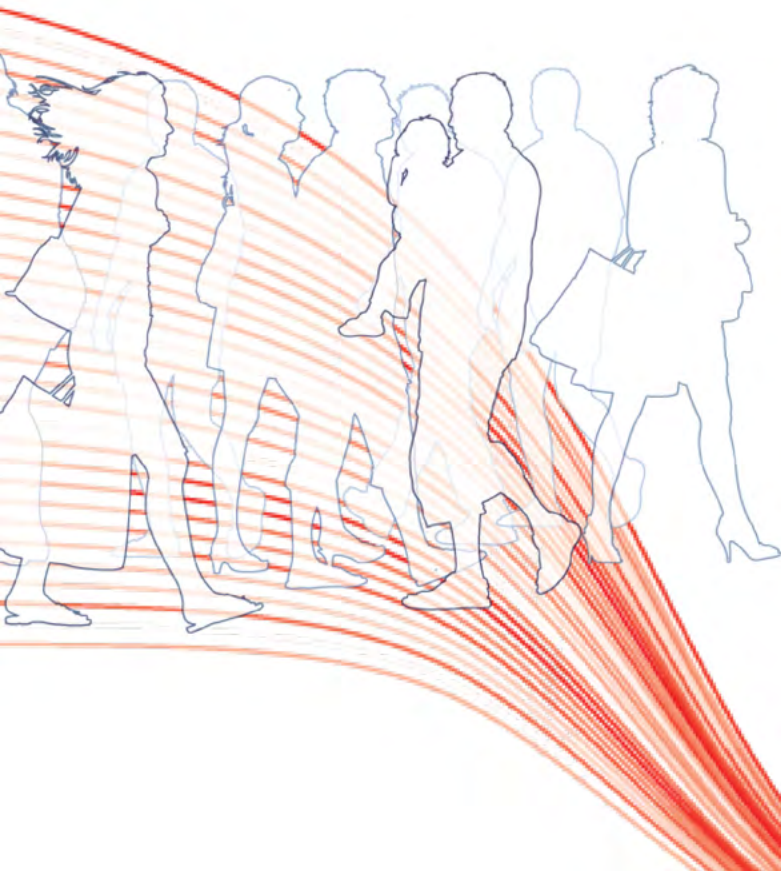
The EU *AI Act* is also clear about protecting judicial independence, investigative privilege, and other sensitivities. For example, registration of EU AI systems that are deemed sensitive occur in a secure, non-public section of the EU database.³⁷⁴

LCO research and consultations confirm that public transparency and disclosure of key information is essential to achieving responsible AI in criminal justice. As a result, Recommendation 16 would require provincial legislation to include:

- Mandatory disclosure of AI systems in criminal justice, including law enforcement, courts, Crowns, legal aid, and correctional services.
- Post key details about the system on a public registry, including the purpose, general capabilities, risk categorization, mitigation strategies, and relevant impact assessments about the AI systems.
- Ensure entries into the registry should be updated upon a material change in the capabilities, purpose or use of the system or annually, whichever comes first.
- Incorporate necessary legislative and/or regulatory consultations to tailor specific transparency practices related to judicial independence, investigative privilege, government secrecy and sensitivity classifications, etc.

Recommendation 16 would fulfill several responsible criminal AI objectives, including :

- Fulfilling the provincial government's commitment that there be "no AI in secret".³⁷⁵
- Ensuring consistent disclosure across Ontario's criminal justice system.
- Promoting systemic oversight, more effective monitoring of specific technologies; and evidence-based rule-making and oversight.
- Establishing clear expectations to AI vendors.
- Ensuring specialized rules to account for judicial independence, investigatory privilege, etc.
- Fostering public confidence in the administration of justice.



Recommendation 17: Standard Risk Assessment

Recommendation 17 commits the Government of Ontario to engage different criminal justice sector institutions in developing a standard risk assessment framework.

LCO Recommendation

17. The Government of Ontario should work with relevant stakeholders to develop a dedicated and mandatory impact assessment for AI systems in criminal justice. The impact assessment should assess the AI system for:
- a. Compliance with the *Charter*, principles of criminal procedural fairness, criminal common law precedents, human rights law, and privacy law.
 - b. Lawful authority and lawful purpose.
 - c. Evidentiary admissibility.
 - d. Bias.
 - e. Other technical, safety, and assurance factors.

Standard Risk Assessment

Stakeholders consistently told the LCO that common risk assessment criteria, categories, and mitigation measures would ensure a consistent approach to AI across different criminal justice institutions.

The LCO supports this approach and recommends that a dedicated risk assessment reflect the risk assessment criteria proposed in Recommendation 12-15. The LCO stresses, however, the need to tailor criminal AI risk assessments appropriately. For example, police may develop additional criteria to determine how and when to invoke investigative privilege. Similarly, courts could evaluate AI systems in a manner to protect judicial independence.

Recommendation 17 is designed to create a shared baseline for assessing risk and protecting rights while ensuring institutions have the opportunity to address specific issues within their mandate.



Recommendation 18: AI Pilots, Procurement and Digital Sovereignty

Recommendation 18.a establishes legislative authority to set standards for AI pilot projects and real-world performance evaluations.

Recommendations 18.b and 18.c establish dedicated procurement standards for software and protects digital sovereignty. These recommendations are discussed at Recommendation 8.

LCO Recommendation

18. Additional legislative or regulatory provisions should include:
- a. Explicit authorization of pilots to evaluate the use, effectiveness, legality, and cost-benefit of AI systems in criminal justice in real-world conditions.
 - b. Dedicated procurement standards and regulations governing responsible software practices including software explainability, version control and archiving, training data disclosure and transparency, and the provision of reports assessing the reliability, validity and bias of the system.
 - c. Requirements to protect digital sovereignty in AI systems in criminal justice, including requirements that the collection, use, processing, transmission and storage of information associated with high risk and restricted use systems and data occurs within Canada, and by regulating standard terms for vendor contracts necessary to fulfill all mandated assessment, disclosure and other obligations.

AI Pilot Projects

Recommendation 18 would provide legislative and/or regulatory authority to define and establish AI pilot projects. The LCO heard widespread support for this recommendation.

The Edmonton Police Service pilot discussed in Sections 2.1 and 3.1 illustrates the need for this recommendation.

As noted, the Edmonton Police Service developed a sophisticated pilot project to test a digital evidence management system operating in conjunction with body cam video.³⁷⁶ The system includes an AI system that uses FRT to recode body cam video and compare faces to an approximately 7,000-person watchlist, based on mugshots of people police say have serious criminal warrants or are flagged as potential safety risks.³⁷⁷

Absent more information, the Edmonton pilot appears both structured and sophisticated.³⁷⁸ Nevertheless, it has several features justifying a more rigorous pilot evaluation framework.



First, according to Edmonton Police, they "will be the first police service in the world to test Axon's body-worn video camera recognition technology."³⁷⁹

Second, the Edmonton pilot is a high risk AI system. Kate Robertson, a senior research associate with Citizen's Lab, has stated:

*As someone who has been studying algorithmic policing technologies for nearly a decade, and [previously] a lawyer in Canada's justice system, I have to say that this is likely the most high risk algorithmic surveillance program that I have observed to date in Canada.*³⁸⁰

Third, according to a CBC news report, the pilot proceeded *without* approval from Alberta's information and privacy commissioner, Diane McLeod. According to Commissioner McLeod,

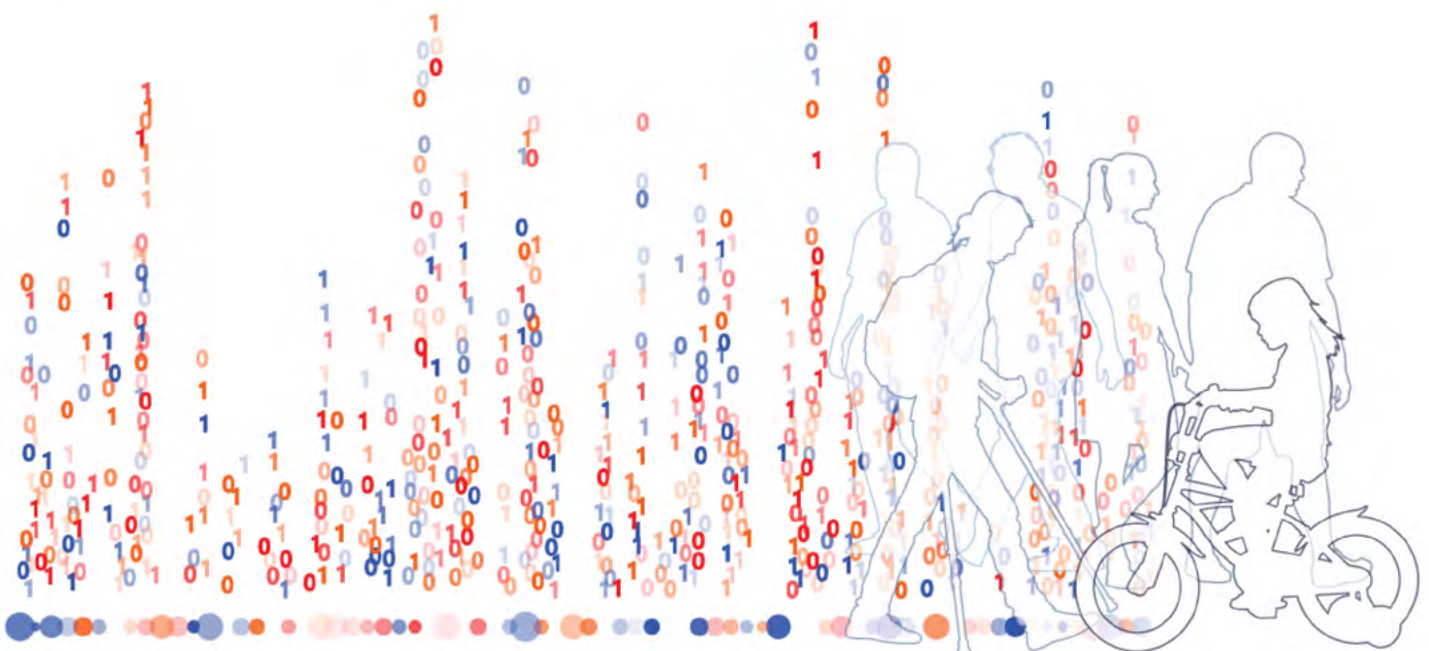
*There is no exception in the act for pilots. [Provincial privacy] law applies if you're collecting, using or disclosing personal information. You're subject to the law, no matter what phase of your technology testing you're in.*³⁸¹

In response, Edmonton Police say they do not legally require what they describe as "feedback" from the Commissioner during the trial or proof of concept stage.³⁸¹

A provincial pilot evaluation framework could address these issues. For example, a provincial pilot evaluation framework could establish appropriate and transparent parameters and requirements to test and report on high risk AI systems. A provincial pilot evaluation framework could also confirm the appropriate legal standard applicable to them, thus reducing legal uncertainty and building public confidence in the eventual pilot evaluation.

Another benefit of an organized and standardize pilot framework is the value in having real-world performance testing of AI systems. The LCO heard that in some jurisdictions investigative AI systems are effectively being live-tested on the public without appropriate evaluative frameworks in place. The LCO also heard concerns that AI tools may be assessed under ideal or abstracted lab-like conditions, demonstrating a potential gap between assessed performance and actual performance in complex, real-world use cases.³⁸²

A final benefit of regulated pilot projects is the creation of a standard evaluation format that can be easily shared, reducing the need to constantly re-assess similar systems deployed in similar circumstances and governance regimes.



Recommendations 19-20: Oversight and Reporting Requirements

LCO Recommendations 19-20 establish responsible criminal AI oversight and reporting obligations. These recommendations have two parts: Recommendation 19 commits the province to establishing a dedicated supervisory body for AI systems in criminal justice. Recommendation 20 mandates interim reporting, oversight and advisory functions to Ontario's Inspector General of Policing, Law Enforcement Complaints Agency, and others pending the creation of that body.

LCO Recommendations 19-20

19. The Province of Ontario should create an independent supervisory body for AI systems used in the in provincial criminal justice system. This body should be established in provincial legislation. This body's mandate should include:
 - a. AI assessment, certification, and ongoing evaluation.
 - b. Creation of a multi-disciplinary public advisory board and technical work groups.
 - c. Availability of expert opinions and witnesses.
 - d. Maintaining a provincial registry of AI systems in criminal justice including publication of associated mandatory AI assessment reports.
 - e. Enforcement of related standards and duties.
20. Pending establishment of the supervisory body, the Province of Ontario should enact interim legislation, regulations, or rules and policies to ensure existing institutions can fulfil oversight roles for AI systems in criminal justice, including:
 - a. Requiring that Ontario's Inspector General of Policing and Ontario's Law Enforcement Complaints Agency receive yearly reports from law enforcement agencies with a comprehensive inventory of criminal justice AI systems, risk assessments, and AI governance and operational policies.
 - b. Requiring that Ontario's Inspector General of Policing and Ontario's Law Enforcement Complaints Agency publish annual public report analyzing the use of AI by law enforcement services and any regulatory actions taken, including development of model AI governance and operational policies for law enforcement.
 - c. Establishing a Crown Criminal AI Advisory Office within the Minister of the Attorney General to provide advice to law enforcement on the investigative uses of AI and to inform AI assessments.

Independent Supervisory Body for AI Systems in Criminal Justice

Recommendation 19 would create an independent supervisory body for AI systems used in the provincial criminal justice system. This body should be established in provincial legislation.

The supervisory authority would have a provincial mandate to:

- Conduct AI assessment, certification, and ongoing evaluation.
- Provide advice on AI governance and operational policies and practices.
- Convene a multi-disciplinary public advisory board and technical work groups.
- Make available expert opinions and witnesses for litigants.
- Maintain a provincial criminal AI registry including publication of associated mandatory AI assessment reports and other materials in open data format.
- Enforce related standards and duties.

LCO consultations found considerable support for this recommendation.

There is already an established precedent in Ontario for this model. Recently, Ontario's Cabinet Office established a dedicated AI team providing many of these functions.³⁸³

Several jurisdictions have established or proposed to establish similar centralized oversight agencies for AI in criminal justice.

In the EU, the European AI Office was established as the foundation for a single AI governance system.³⁸⁴ Reporting to the European Commission, the AI Office has a mandate to:

- Develop tools, methodologies, benchmarks and risk classifications for AI systems.
- Prepare codes of practice and guidance on implementing AI standards.
- Oversee AI pilot and sandbox projects, including real-world testing.
- To investigate and enforce regulatory and safety compliance.³⁸⁵

The AI Office additionally coordinates with the AI Act Scientific Panel of independent experts and the AI Act Advisory Forum, a advisory panel with 174 members drawn from civil society, academia, industry, start-ups, and small and medium enterprises.³⁸⁶

The United Kingdom also recently announced PoliceAI, "a national AI centre to help policing work smarter."³⁸⁷

The functions and services the center intends to facilitate include:

- Independently testing police AI models for accuracy and bias.
- Publishing a public registry of AI tools in use across policing.
- Overseeing large-scale pilot projects simultaneously across several local police jurisdictions to better understand the risks, impacts, governance and operation of various AI tools.
- Developing safeguards and designing how to deploy AI systems responsibly.
- Centralizing expertise, technology and training in deep fake and non-consensual intimate image detection.³⁸⁸

The impact of the UK's supervisory body is already being demonstrated. In June, PoliceAI "issued guidance advising officers to stop using generative AI to prepare court statements due to the tech's tendency to hallucinate answers," finding that "you can't do that, because we haven't gone through all the checks and balances... We need to slow it down a bit."³⁸⁹

Mandatory Reporting to LECA and IGoP

The Supervisory Authority would take time and work to establish. In the interim, the LCO recommends several important oversight functions be performed by existing institutions.

Accordingly, Recommendations 20.a and 20.b would legislatively require Ontario's Inspector General of Policing and the Law Enforcement Complaints Agency to receive yearly reports from law enforcement agencies with a comprehensive inventory of criminal justice AI systems, risk assessments, and AI governance and operational policies. The Recommendations would also require LECA and IGoP to publish public annual reports analyzing the use of AI by law enforcement services and any regulatory actions taken.

These reporting requirements are discussed in detail in Recommendation 5.

What Should Be Reported?

The LCO heard many ideas about what needed to be reported to ensure effective oversight and responsible criminal AI deployment. Many of these issues or topics are consistent with the reporting provisions set out in TPS Use of AI Policy above. Suggested reporting obligations included:

- How AI systems are being used in criminal justice.
- Who is using them.
- Who is providing them.
- What kinds of assessment, oversight and performance auditing are ongoing (or not).
- How risk classifications are defined, interpreted, and applied.
- Whether systems have been independently demonstrated as reliable, valid and free of bias.
- Whether systems are used for a lawful purpose and compliant with Canadian law.
- Whether impacts on individual and collective rights are lawful, proportionate, and mitigated.
- Whether the public has been meaningfully engaged and consulted.
- Whether AI systems are cost effective and are an improvement on other police practices.
- What terms and conditions of use may bind law enforcement.
- Whether digital sovereignty and security over sensitive information is assured and confirmed.

Although there were many different opinions on the specific details of public reporting, there was broad agreement that public reporting had to be consistent, regular and comprehensive.

Interestingly, several commentators also suggested provincial authorities be given the power to order special reports or that reports could be automatically triggered in specific circumstances similar to use of force reports.

Crown Criminal AI Advisory Office

Finally, Recommendation 20.c would establish another important oversight and advisory body: a Crown Criminal AI Advisory Office.

As discussed in LCO Issue Paper 2, **Use of AI by Law Enforcement**, the Crown prosecutor service provides a series of critical advisory functions to law enforcement on the use of investigative technologies.³⁹⁰

During consultations, the LCO heard that many of these functions are provided on an ad hoc basis, often on a regional or local level, and are generally under-resourced. This limited model is compounded by the need for AI expertise to properly advise police in that context.

Both police and Crowns commented on the many potential benefits of a more formalized, better resourced Crown Criminal AI Advisory Office.

The general view of those who the LCO consulted is that such an Office would lead to centralized AI expertise, reduced errors, better and more consistent disclosure practices between police and Crowns, a reduction in the use of unreliable and inadmissible AI systems, fewer wasted resources and failed prosecutions, and better protection of individual and collective rights.

Recommendations 21-24: AI Evidence

LCO Recommendations 21 – 24 address AI-created or AI-enhanced evidence that might be used in criminal proceeding or during a criminal investigation. These recommendations address:

- The shared jurisdiction in these matters between the provincial government, federal government and various Rules committees.
- The need for dedicated evidentiary rules at different stages of the criminal justice process.

LCO Recommendations

21. The Province of Ontario should encourage the federal government to convene a joint Federal-Provincial Criminal AI Evidence Rules Committee and consultation process. The mandate of this committee should be comparable to that of the Ontario Civil Rules Committee Artificial Intelligence Sub-Committee to study and recommend a set of minimum safeguards for AI evidence rules for criminal matters.
22. The Courts of Criminal Justice in Ontario should use powers delegated under the *Courts of Justice Act* and the *Criminal Code* to convene a Criminal Proceedings Rules AI Evidence Sub-Committee. The mandate of the committee should be comparable to that of the Ontario Civil Rules Committee AI Sub-Committee to study and recommend a set of AI evidence rules for different provincial criminal proceedings.
23. The Province of Ontario Minister of the Attorney General should establish an AI Evidence Policy and Procedure Committee. The mandate of the committee should be to study, consult on, and draft a set of AI evidence procedural policies for different provincial criminal proceedings. In particular, policies should:
 - a. Confirm the prohibition on the use of AI tools for the purpose of assessing risk, and the high risk designation of AI evidence in bail proceedings, consistent with LCO Recommendations 12.b.ii and 13.b.vi; and
 - b. Establish a disclosure and certification process for any forms of AI evidence that may be considered in a bail proceeding.
24. The Province of Ontario Minister of the Attorney General should amend the Crown Prosecution Manual with policy directives implementing the recommendations developed above.



AI Evidence in Criminal Justice

The LCO and our consultees researched and discussed the impact and regulation of AI evidence in Canadian criminal proceedings at length.

Everyone agreed that AI tools have the potential to significantly improve criminal investigations, improve efficiency and improve public safety. For example, many police investigators now use AI to expedite the investigation of complex financial crimes and to distinguish real victims among thousands of AI-generated child sexual abuse images.³⁹¹

Consultees also agreed there are serious risks within two emerging classes of AI evidence: 1) acknowledged AI evidence, and 2) unacknowledged AI evidence, including deep fakes.

Examples of acknowledged AI evidence include:

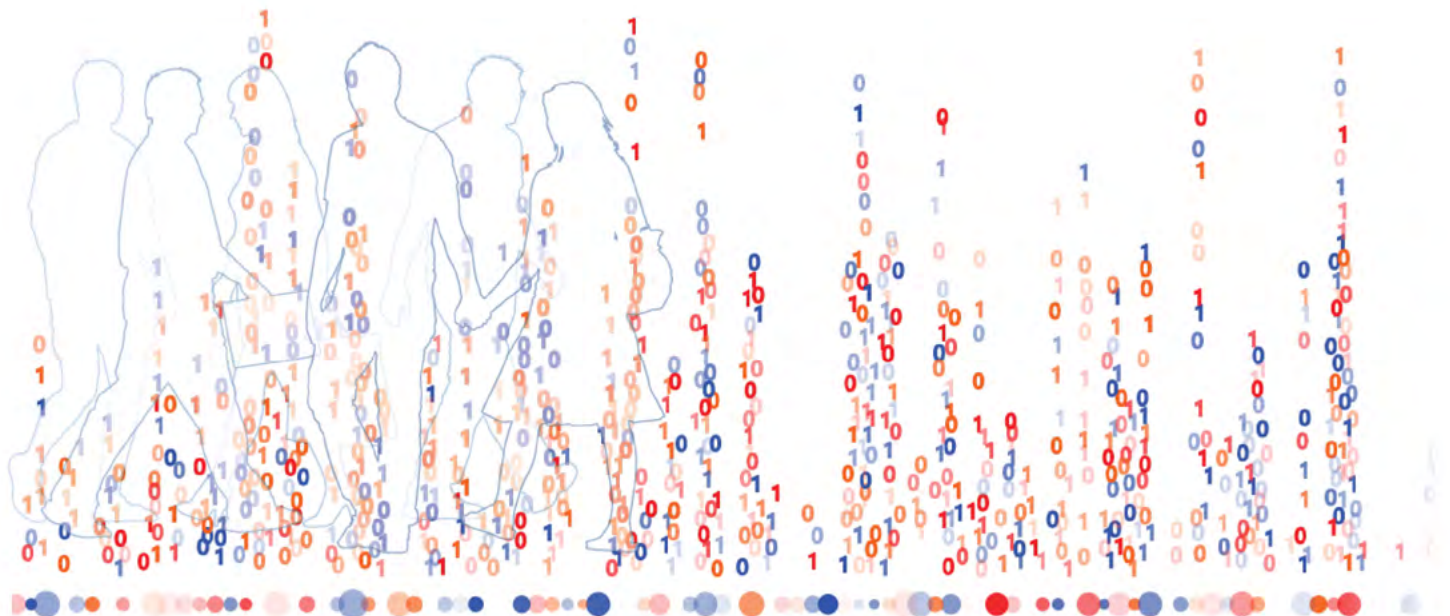
- AI tools used to support investigations, such as FRT, ALPRs or tools that scan emails or texts to map relationships in organized crime investigations.
- AI scribes used to transcribe or describe video and audio, and to write police incident reports.
- AI tools for conducting legal research and drafting legal materials.

Examples of unacknowledged AI evidence may include:

- Police investigations that receive unreliable “deepfake” evidence from third parties.
- Police members who make use of unauthorized but publicly available AI tools like geolocation and facial recognition apps, or rely on information gathered through surveillance systems at risk for discrimination and bias.
- Raw images or video artificially “enhanced” by an AI system that does not resolve detail but rather infers or adds it, undermining the reliability and validity of the evidence.
- Documents drafted, altered or edited with AI assistance – such as police notes and incident reports, document summaries or audio and video transcripts and descriptions – that may contain hallucinated or sycophantic errors.

To assess these issues, the LCO convened several consultation sessions to address AI evidentiary issues, including the Toronto Roundtable on AI Evidence.³⁹²

Participants included representatives from Ontario’s judiciary, the federal and provincial Attorneys General, federal and municipal law enforcement, Crowns, private bar and legal aid defence counsel, provincial human rights and privacy agencies, academics, and public interest advocates representing a variety of communities.



Notwithstanding their different professional backgrounds, it quickly became apparent that everyone shared several related concerns. Many consultees reported that these issues are already appearing in Canadian courts.

- AI tools are very new. As a result, police, Crowns, defence counsel and courts have to address novel and complex questions about AI evidence reliability, validity and bias.³⁹³
- The "human in the loop" may be unqualified, under-resourced or lack independence.³⁹⁴
- There is no consistent obligation to disclose the use of AI or reliance on AI evidence. Nor is there clarity on what AI disclosure should entail. Nor is there clarity on what AI disclosure should entail, including rules and procedures regarding the timing, extent or format of disclosure.
- Proceedings with lower evidentiary thresholds are less likely to effectively test AI systems. Consultees were especially concerned about AI-aided risk assessments in bail hearings, where the rapid pace, high-pressure, and reduced evidentiary burden means AI evidence is unlikely to be reviewed appropriately.
- Access to AI experts is challenging. There is no professional designation or certification for "AI experts." Many stakeholders were also worried that defence counsel and duty counsel will have less access to experts, undermining the fairness of criminal proceedings.

- Courts may need to consider many different AI tools simultaneously. A single proceeding could involve an FRT match identifying a suspect, an AI bail algorithm, AI-generated transcripts or translations, algorithmically assessed genetic evidence, and more.
- Regulation by litigation is unlikely to be effective. Consultees were emphatic that a case-by-case approach was certain to increase systemic risks, including improper arrests, wrongful convictions, and increased litigation costs and delays.
- Deepfakes are an emerging problem. Current AI tools make evidence manipulation more accessible and difficult to detect. Consultees were worried about faked or altered images, video, audio and documents. Consultees also point out that deepfake evidence may now come from defendants, third party witnesses, and even investigators.³⁹⁵

Stakeholders acknowledged that criminal evidence law is flexible and routinely adapted to novel technologies. They believed, however, that existing provisions in the *Canada Evidence Act* and *Ontario Evidence Act* governing electronic or business records were not well-suited for AI evidence. For example, granting the same presumptive integrity to AI-generated evidence as to other routinely generated or stored electronic records could mean courts fail to properly evaluate AI systems that produce outputs that are invalid, unreliable or biased. Similarly, existing evidentiary principles and procedures may be too vague or inappropriate to govern disclosure of technically complex and dynamic AI systems, such as the "disclosure" example given above.

To address these issues, the LCO is making a series of recommendations that would:

- Establish procedural rules governing criminal AI evidence in Ontario.
- Establish protections for AI evidence in bail proceedings.
- Establish disclosure rules, guardrails and certification requirements for law enforcement and Crown prosecutors.

Establishing Procedural Rules Governing Criminal AI Evidence in Ontario

In light of the issues above, the LCO and consultees generally agreed that AI evidence should be recognized as a distinct class of evidence with a set of dedicated rules and procedures in criminal justice.

Participants pointed to existing precedents for this approach within the civil justice system: In July 2025, the Ontario Civil Rules Committee Artificial Intelligence Sub-Committee (“AI Sub-Committee”) proposed a set of new *Rules of Civil Procedure* relating to both deep fakes and AI evidence.³⁹⁶

The AI Sub-Committee subsequently consulted on a draft set of rules which have been approved by the Civil Rules Committee and have been submitted to the Minister of the Attorney General for review.

In summary, the AI Sub-Committee proposes a comprehensive set of rules for governing the use of AI-generated or AI-assisted evidence in civil court proceedings. The proposals would establish a broad definition of AI intelligence and create distinct but complementary rules for acknowledged AI evidence, where a party discloses the use of AI, and unacknowledged AI evidence, where evidence presented as authentic was generated or altered by AI.

The proposed rules would also establish standards and procedures for assessing the reliability, validity, and potential bias of AI systems. Parties seeking to introduce AI evidence would bear disclosure and evidentiary obligations, including identifying the AI system used, relevant training data, inputs and information provided to the system, and evidence demonstrating the reliability and validity of its outputs. Courts would also have discretion to require disclosure of prompts.

Where AI evidence forms part of expert evidence, the expert would need to provide sufficient information for the court to assess its necessity, reliability, methodology, application, error rates, testing, peer review, scientific acceptance, standards and controls and potential bias.

The proposals would also address suspected AI fabrication. Evidence reasonably believed to constitute unacknowledged AI evidence would be presumptively inadmissible when challenged, unless the proponent demonstrates that its probative value outweighs its prejudicial effect.

Finally, the proposed Rule would give courts the authority to impose remedies for abusive unacknowledged AI use, including costs, additional disclosure or examinations, and striking some or all of a party’s evidence.

The AI Sub-Committee’s proposed civil AI evidence rule is the first of its kind in Canada. American courts are considering a similar rule: In 2024 the U.S. Judicial Conference’s Advisory Committee on Evidence Rules began meeting to develop a regulation on the admission of AI-mediated evidence, including deep fakes.³⁹⁷

The LCO and consultees agreed that the proposed civil AI evidence rules are an important precedent for equivalent rules in the criminal justice system. The LCO and consultees also agreed that any equivalent criminal rules would have to be adapted to criminal proceedings. For example, the right against self-incrimination and the right to silence mean the defence does not have to disclose AI evidence to the Crown, which is quite different than the reciprocal disclosure obligations in civil cases.

Consultees also cautioned that criminal justice AI evidence rules should not be interpreted or understood as automatically accepting AI evidence. Rather, it was noted that the rules are the minimum safeguards to advance to the testing phase of a criminal justice proceeding.

Any initiative to develop a provincial criminal AI evidence rule should proceed through established channels. As a result, Recommendation 22 proposes that the Courts of Criminal Justice in Ontario should use powers delegated under the *Courts of Justice Act* and the *Criminal Code* to convene a Criminal Proceedings Rules AI Evidence Sub-Committee. The mandate of the committee should be comparable to that of the Ontario Civil Rules Committee AI Sub-Committee to study and recommend a set of AI evidence procedural and disclosure rules for different provincial criminal proceedings.

The LCO also heard that there are limits on the inherent jurisdiction of Ontario criminal courts to govern their disclosure process. Matters of criminal AI evidence raise federalism issues, particularly where federal government maintains (broadly speaking) jurisdiction over the *Criminal Code*, judicial authorizations, and the admission of evidence. However, the *Criminal Code* also provides authority of Superior Courts to enact rules “applicable to any prosecution, proceeding, including a preliminary inquiry... within the jurisdiction of that court” and to “regulate the pleading, practice and procedure in criminal matters, including pre-hearing conferences... [and] proceedings with respect to judicial interim release and preliminary inquiries...”³⁹⁸

To address these issues, Recommendation 21 proposes that the Province of Ontario should encourage the federal government to convene a joint Federal-Provincial Criminal AI Evidence Rules Committee and consultation process. The mandate of this committee should be comparable to that of the Ontario Civil Rules Committee Artificial Intelligence Sub-Committee to study and recommend a set of minimum safeguards for AI evidence rules for criminal matters.

AI Evidence in Bail Proceedings

AI evidence and AI-based risk assessment tools and reports create a particular challenge in bail proceedings. A detailed review of these issues is in LCO Criminal AI Project consultation paper, **AI and the Assessment of Risk in Bail, Sentencing, and Recidivism**.³⁹⁹

LCO consultations with police, Crowns, defence counsel and courts confirm a shared and serious concern with the reliance on AI evidence or AI risk assessment in bail. Consultees expressed the view that bail court is fast-paced and operates with limited time and focused materials. Recent bail practice directions emphasize same-day hearings, streamlined records, and short time targets. Many contested hearings are expected to proceed on brief summaries and be completed in approximately 30 minutes. Bail hearings also operate with a much lower standard for the admissibility of evidence, requiring evidence to satisfy a “trustworthy and credible” threshold.⁴⁰⁰

In these circumstances, it was widely agreed that that any reliance on AI evidence could be very prejudicial and of high risk to accused. Duty counsel and defence counsel emphasized that they cannot realistically assess complex or opaque AI outputs in real time. This creates a significant risk of unfairness for accused persons and undermines courts as a crucial check and balance on rights offending uses of AI.



In this context, several foundational suggestions were made:

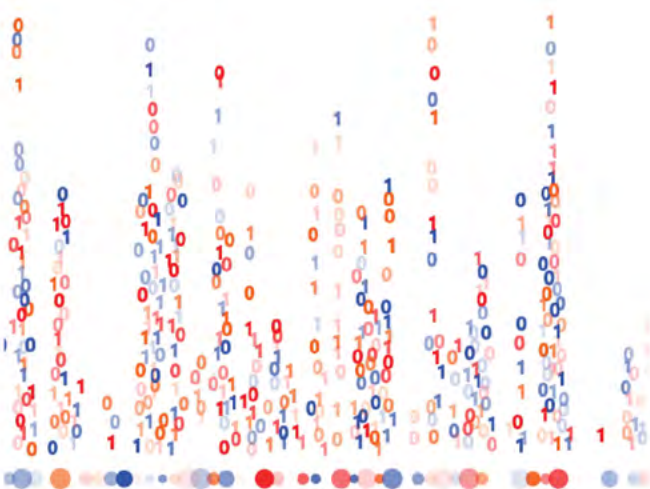
- Disclosure provided at bail (i.e. the bail brief) should make the use of AI explicit. All parties – the defence, the prosecution and the court – should be alive to concerns relating to possible AI-generated or AI-assisted evidence.
- Rules should provide simple and practical direction on the use of AI at the bail phase. The rule should make explicit all of the prohibited and high risk AI practices as outlined in the LCO's recommendations.
- “Human in the loop” accountability needs to be formalized, with clear confirmation of whether AI was used; what it was used for; and who reviewed it. General assurances will not be sufficient in high-volume court settings.
- Where defence counsel suspect evidence is AI-based but not disclosed, inquiries should not cause delays that would prejudice the accused. Accurate information about the use (or not) of AI should be made easy to obtain, such that the Crown’s office can promptly respond to inquiries.
- Additional resources for the defence – including case summaries, sample submissions and other ready-to-use reference materials – need to be in place for duty counsel to meaningfully respond to the use of AI in bail courts.

Recommendation 23 responds to these concerns by proposing the province establish an AI Evidence Policy and Procedure Committee. The mandate of the committee should be to study, consult on, and draft a set of AI evidence procedural rules and policies for provincial criminal proceedings that are more summary in nature, including bail, applications for judicial authorization, sentencing, dangerous offender hearings, and others. In particular, the rules should:

- Confirm the prohibition on AI-based predictive risk assessments, consistent with LCO Recommendation 12.b.ii.
- Confirm the high risk designation of AI evidence in bail proceedings, consistent with LCO Recommendation 13.b.vi.

The LCO further recommends that the AI Evidence Policy and Procedure Committee consider adopting a disclosure and certification rule. This rule would 1) mandate the disclosure of any high risk or restricted use AI systems or evidence; and 2) establish an AI evidence certification process between police and the Crown.

A rule mandating disclosure is critical. LCO consultations frequently heard concerns for both formal and informal uses of AI that may not be disclosed. Without disclosure, the investigative use of AI systems are often invisible to the people being analyzed and to the justice system generally. LCO research confirms that many AI technologies – particularly facial recognition systems – have frequently been criticized for their lack of disclosure. In the US, for example, a recent investigation across 15 states and over 1,000 criminal prosecutions concluded that “police seldom disclose use of facial recognition despite false arrests... [while] many defendants were unaware of the technology’s role in linking them to crimes.”⁴⁰¹ The investigation concludes this denies accused “the opportunity to contest the results of an emerging technology that is prone to error, especially when identifying people of color.”⁴⁰²



The certification process would formalize the “human in the loop” role in a police investigation with three key responsibilities:

- 1) To disclose any evidence generated through the use of an AI system.
- 2) To review and certify the outputs of those systems, identifying the certification officer as responsible for the AI system.
- 3) Making the certification officer available to testify as to the assessment, operation, and reliability and validity of the AI system.

Several other LCO Recommendations create necessary infrastructure to support this process, including Recommendation 4 establishing a precautionary principle and requirement to assess AI systems before use; Recommendations 10-15 establishing a detailed AI risk assessment and reporting regime; Recommendations 8 and 18 requiring AI vendors to provide detailed assessment and operational information; and Recommendation 24, requiring the Crown to receive and review the certification and sign-off on it.

In sum, the proposed rule would ensure that only pre-vetted, properly disclosed, and well-supported AI evidence would be entered into the bail brief. It would flag AI evidence to all the parties. And it makes information about the AI system easy to obtain and readily available, ensuring inquiries are promptly responded to and reducing prejudice to the accused.

In addition to these core function, The AI Evidence and Policy should also consider related matters relevant to bail and other summary proceedings, such as:

- The threshold for evidentiary admissibility, reliability and bias of AI evidence.
- Rules directing challenges on the basis of declared or undeclared deep fake evidence.
- Rules governing third party expert assessments that may rely on AI – such as from health and social service providers – and which inform bail eligibility, bail conditions, or diversion eligibility.

Amending the Crown Prosecution Manual

LCO Recommendation 24 proposes that the provincial Attorney General amend the Crown Prosecution Manual with policy directives implementing the recommendations developed above.

An amendment to the Crown Prosecution Manual would formalize an obligation on the Crown to receive and review the certification of AI evidence received in disclosure from police. The amendment would also specify the roles and steps in this process. The effect of this Recommendation would be to:

- Identify a responsible Crown such as inquiries between the defence and police are readily and fully responded to.
- Oversee police certification and evidentiary assessment practices, ensuring a high and consistent standard for the “human in the loop”.
- Set province-wide standards for Crown prosecutors, thus promoting consistent standards and practices in criminal courts across Ontario.

Recommendations 25-29: Access to Justice and System Capacity

Recommendations 25-29 address the need to ensure criminal accused and defence counsel have meaningful access to justice in criminal proceedings involving AI systems. These recommendations also address the need to increase capacity within provincial criminal justice institutions to effectively respond to the foreseeable challenges of AI systems, including the need for access to experts and forensic tools.

LCO Recommendations

25. The provincial Ministry of the Attorney General should increase funding and other resources for Legal Aid Ontario as necessary to ensure criminal defense counsel are able to make a full answer and defence in cases involving AI evidence.
26. Legal Aid Ontario should establish an AI Centre of Excellence with the mandate and resources to support staff and private bar defence counsel, duty counsel, and legal aid clinics with:
 - a. Comprehensive training on criminal justice AI-related laws and procedures.
 - b. Standards for professional competence in AI legal research and advocacy.
 - c. Legal research on AI issues and cases.
 - d. Support for individual and systemic AI test cases.
27. Legal Aid Ontario should establish an external advisory committee with a mandate to meet regularly and advise LAO's board and management on the purpose, design, implementation and foreseeable impacts of any proposed criminal justice related AI systems, programs, procedures or services.
28. Pending establishment of the supervisory authority for AI in criminal justice recommended above, the Centre of Forensic Sciences should develop a program freely available to criminal defence counsel who seek an opinion on the reliability, validity and bias of AI evidence, investigation tools, and investigation practices. This program could include a roster of independent AI experts available to the defense.
29. Pending establishment of the supervisory authority for AI in criminal justice recommended above, the Centre of Forensic Sciences should develop a program for the certification and provision of AI-related forensic tools to legal counsel, such as platforms for identifying deep fake evidence and documents.



Legal Aid Ontario

Recommendations 25-27 would build the capacity needed to ensure accused and their counsel have effective access to justice and are able to make a full answer and defence to AI-enabled investigations.

There are three critical commitments.

First, Recommendation 25 would commit MAG to provide funds and other resources to Legal Aid Ontario (LAO) as necessary to ensure criminal defense counsel are able to make a full answer and defence in cases involving AI evidence.

The LCO heard that current legal aid programs and funding arrangements – including legal aid certificates, the duty counsel program, and discretionary funding including Big Case Management and test case funding – will be insufficient to respond to the systemic nature of AI evidence.⁴⁰³ The LCO also heard that discretionary court funding for legal counsel – such as amicus appointments and *Rowbotham* orders – are similarly limited.

Recommendation 25 would establish a more intentional and coordinated funding program to address the legal challenges that are certain to arise at every step of a criminal legal proceeding, including:

- Bail hearings.
- Pre-hearing proceedings including disclosure, applications for judicial authorization, and diversion applications.
- Trials.
- Sentencing.
- Appeals.
- Dangerous offender hearings.

Challenges to AI evidence in these proceedings will require significant resources to test issues related to reliability, validity, lawful purpose, operational standards, bias, and other factors. Within current legal aid and other funding arrangements, counsel to not have the time or resources to address these issues.

Accordingly, the LCO recommends that MAG and LAO, in consultation with the criminal defence bar and legal aid staff lawyers, develop a sustainable funding model that proactively anticipates forthcoming litigation challenges associated with AI evidence.

Second, to build litigation capacity within LAO and the broader criminal defence bar, Recommendation 26 would establish an AI Centre of Excellence within LAO. Practically speaking, this recommendation mirrors Recommendation 20.c establishing a Crown Criminal AI Advisory Office. The mandate of the Centre would be to support staff and private bar defence counsel, duty counsel, and legal aid clinics with a variety of services and resources that enhance knowledge and skills related to AI uses in criminal justice. The Centre would facilitate:

- Comprehensive training on criminal justice AI-related laws and procedures.
- Standards for professional competence in AI legal research and advocacy.
- Legal research on AI issues and cases.
- Support for individual and systemic AI test cases.

As a province-wide service, the Centre would help elevate consistent and best practices across all criminal jurisdictions, reducing disparities between regions and ensuring effective and adequate access to justice for all accused. The Centre would also have expertise to assess and provide funding for systemic AI test cases, strategically supporting the development of leading legal precedents with a normalizing effect on practices across the province.

Finally, Recommendation 27 would establish an external advisory committee with a mandate to meet regularly and advise LAO's board and management on the purpose, design, implementation and foreseeable impacts of any proposed criminal justice related AI systems, programs, procedures or services. This would ensure a strong voice for the criminal defence bar and legal aid staff lawyers in the development, funding and operation of AI-related access to justice initiatives, better ensuring programs are effective, lasting, and responsive to the needs of criminal defence advocacy.

Access to Experts and Forensic Tools

Recommendations 28-29 are transitional recommendations. Pending creation of the proposed criminal AI Supervisory Authority (discussed in Recommendation 19), these recommendations would ensure much needed litigation resources are made available through the Centre of Forensic Sciences (CFS).

The CFS is one of the most extensive forensic science facilities in North America, conducting scientific investigations in cases and crimes against people and property. CFS teams conduct highly specialized forensic examination, analysis and research in areas including body fluid identification and DNA profiling; firearms and ammunition analysis; toxicology assessment; chemical analysis of materials and trace evidence; and document analysis for authenticity, alternations, and relations to persons and places.⁴⁰⁴

Importantly, the CFS also conducts research and development, ensuring cutting edge forensic science is used to deliver services to official investigative agencies, and to provide specialized training in the use of investigative technologies, like intoxilyzers.⁴⁰⁵

The CFS can also be called on as an expert to assist in assessing evidence as part of a litigation. The CFS provides a range of such services, including expert witnesses, letters of opinion, interpretive reports, and analytical reports.⁴⁰⁶

LCO consultees believe considerable AI expertise will be needed to test and adjudicate AI evidence. It was felt that as a transitional recommendation, the CFS could leverage its existing mandate and provide expert forensic services in relation to AI systems and tools used in criminal justice.

Recommendation 29 prioritizes two important initiatives within the CFS.

First, the CFS should develop a program freely available to criminal defence counsel who seek an opinion on the reliability, validity and bias of AI evidence, investigation tools, and investigation practices. Access to independent expert assessment, opinions and reports and witnesses is a longstanding

concern of the criminal defence bar. The LCO heard that existing funding options are very limited, often not available, and create difficulties in retaining independent experts with any regularity or predictability. In context of AI-related litigation, which is certain to be frequent, highly complex, and routinely raise novel technological issues, barriers to accessing experts are certain to have a distorting effect. The proposed program could include a roster of independent AI experts available to the defense.

Second, the CFS should develop a program for the certification and provision of AI-related forensic tools to legal counsel, such as platforms for identifying deep fake evidence and documents.

The LCO heard that there is an “authenticity arms race” under way between systems designed to generate fake but convincing images, video and audio versus systems designed to identify such material or alterations. This is a rapidly evolving field in which standards and practices like indelible digital watermarking of AI-manipulated or generated content are only beginning to be established and operationalized.⁴⁰⁷ In a litigation context, there is considerable uncertainty over the evidentiary standards that may apply to deep fake or allegedly deep fake material. For example, cases have only begun to contend with issues like a greater burden of proof on the Crown where digital manipulation of key evidence is alleged.⁴⁰⁸

Against this background, the LCO was told that it would be enormously helpful for a central authority – such as the CFS – to have expertise in assessing the efficacy of different “deep fake” detection systems, to certify the best systems for use by counsel, and to make such systems available to counsel for analyzing disclosure. CFS is also well primed to provide training in the use of such technology, not unlike their mandate to provide training on the use of other investigative technologies like intoxilyzers.

As mentioned, the LCO proposes Recommendations 28-29 as transitory provisions. The functions ascribed to the CFS could later be transferred to the Supervisory Authority established under Recommendation 19.

7. Endnotes

- 1 Information about the LCO's AI in Criminal Justice project is available at <https://www.lco-cdo.org/CrimAI>.
- 2 UK Parliament, "Facial recognition technology in policing" [UK Parliament FRT] (April 8 20260, online: <https://post.parliament.uk/facial-recognition-technology-in-policing/>).
- 3 See generally, DeFlock, an American "open-source project mapping licence plate readers" [DeFlock], online: <https://deflock.org/>. (Accessed September 14, 2026).
- 4 CBS 12 News WPEC, "Governor DeSantis calls Flock license plate readers "out of control."" [CBS 12 News] (August 26, 2026), online: <https://www.youtube.com/shorts/m1lItxEuS38>.
- 5 DeFlock, "City Council", online: <https://deflock.org/council#wins>. See generally, DeFlock, an American "open-source project mapping licence plate readers" [DeFlock], online: <https://deflock.org/>. (Accessed September 14, 2026).
- 6 UK Government, "PoliceAI to speed up investigations and fight crime" (June 10, 2026), online: <https://www.gov.uk/government/news/policeai-to-speed-up-investigations-and-fight-crime>.
- 7 All Issue Papers and other material published by the LCO AI in Criminal Justice Project are available at <https://www.lco-cdo.org/CrimAI>.
- 8 All Issue Papers and other material published by the LCO AI in Criminal Justice Project are available at <https://www.lco-cdo.org/CrimAI>.
- 9 A complete list of LCO events is available upon request.
- 10 Professor Perrin's UBC Artificial Intelligence and Criminal Justice Initiative is the leading academic criminal AI research organization in Canada. Their reports and resources are available online: <https://benjaminperrin.ca/ai>.
- 11 Government of Canada AI Register, Records 747-760, accessed August 18, 2026. Online: <https://open.canada.ca/data/en/dataset/fcbc0200-79ba-4fa4-94a6-00e32facea6b/resource/369f6f34-148a-42ed-b581-8c164e941a89>.
- 12 Toronto Police Service, "Artificial Intelligence" [TPS AI Policy] online: <https://www.tps.ca/police-reform/artificial-intelligence/>. (Accessed September 14, 2026),
- 13 Benjamin Perrin, Geoffrey Liew & Isabelle Sweeney, *AI & Policing: Research Report on the Governance & Use of Artificial Intelligence by Police in Canada* (UBC AI & Criminal Justice Initiative, 2026) [UBC Police AI Report], at 13-53, online: <https://canlii.ca/t/7nrqc>.
- 14 This list was compiled from several sources, including Benjamin Perrin, Geoffrey Liew & Isabelle Sweeney, *AI & Policing: Research Report on the Governance & Use of Artificial Intelligence by Police in Canada* (UBC AI & Criminal Justice Initiative, 2026) [UBC Police AI Report], online: <https://benjaminperrin.ca/f/ai-policing-research-report-published>; the LCO's Criminal AI Issue Papers; various media reports cited in this report; Citizen Lab, "Algorithmic Policing in Canada Explained" (September 1 2020), online: <https://citizenlab.ca/research/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/algorithmic-policing-in-canada-explained/>; and Ben Perrin, *Artificial Intelligence & Criminal Justice: Cases and Commentary* (updated February 2 2026), online: <https://canlii.ca/t/7njwh>.
- 15 Europol, *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement* [EUROPOL] (2024), at 8, online: <https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing>.
- 16 UBC Police AI Report.
- 17 See: Metropolitan Police, Live Facial Recognition Annual Report, [Met LFR Report] (2025), online: <https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/facial-recognition-technology/> at 5. See also, Staff Sergeant Jeff Bassingthwaite, Toronto Police Service, "Tricked-Out-Ride: Outfitting Cars with Computers, Cameras and Integrating ALPR" (4th Annual Police Tech Conference and Expo Mississauga, November 11 2025), slide deck on file with the LCO.

- 18 Law enforcement FRT is discussed in Law Commission of Ontario, *Issue Paper 2: Use of AI by Law Enforcement* (LCO Police AI Issue Paper), (2025), online: <https://www.lco-cdo.org/CrimAI>. See also generally, International Criminal Police Organization (INTERPOL), *A Policy Framework for Responsible Limits on Facial Recognition* [INTERPOL Policy Framework] (2021), online: <https://unicri.org/A-Policy-Framework%20for-Responsible-Limits-on-Facial-Recognition>; 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/>; and 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>.
- 19 The Information and Privacy Commissioner of Ontario defines facial recognition technology (FRT) as:
...an artificial intelligence (AI) technology that collects and processes sensitive personal information to identify or verify an individual's identity... 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.
See: IPC FRT Report at 1.
- 20 International Criminal Police Organization (INTERPOL), *Introduction to Responsible AI Innovation* (2024) [INTERPOL AI Introduction], online: <https://www.interpol.int/en/How-we-work/Innovation/Artificial-Intelligence-Toolkit> at 21.
- 21 *R. v. Kawall* (2022 ONCJ 475). An appeal in this case was heard before the Ontario Court of Appeal in March 2026, judgement pending. See also Canadian Civil Liberties Association, "CCLA Intervenes in Kawall appeal on police use of intrusive facial recognition technologies" (March 20 2026), online: <https://ccla.org/privacy/ccla-intervenes-in-kawall-on-police-use-of-intrusive-facial-recognition-technologies/>.
- 22 See generally, EUROPOL at 21-29.
- 23 According to the Atlas of Surveillance, an open-source research project of the Electronic Frontier Foundation, there could be as many as 980 locations or applications of FRT in various law enforcements and government agencies across the United States as of September 2026. [Atlas of Surveillance], online: <https://atlasofsurveillance.org/atlas>.
- 24 Office of the Privacy Commissioner of Canada, *Police use of Facial Recognition Technology in Canada and the Way Forward* [OPC 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/>.
- 25 Toronto Police Service, "Use of Artificial Intelligence Technology" (introduced February 28 2022, updated January 11 2024), online: <https://tpsb.ca/home/about/policies-by-laws/board-policies/use-of-artificial-intelligence-technology/> [TPS AI Policy].
- 26 UBC Police AI Report at 14.
- 27 Ottawa Citizen, "Ottawa police moving forward with first phase of AI facial recognition" (July 3 2026), online: <https://ottawacitizen.com/news/ottawa-police-ai-facial-recognition> and CBC News, "Edmonton Police Service partners with U.S. company to test use of facial-recognition bodycams" (December 2 2025), online: <https://www.cbc.ca/news/canada/edmonton/edmonton-police-facial-recognition-cameras-9.7000389>.
- 28 Ottawa Police Service Board, *Ottawa Police Service Facial Recognition Initiative* [Ottawa FRT Initiative], June 22 2026 at 3-4. See also Ottawa Citizen, "Ottawa police moving forward with first phase of AI facial recognition" (July 3 2026), online: <https://ottawacitizen.com/news/ottawa-police-ai-facial-recognition>.
- 29 Ottawa FRT Initiative at 1-2.

- 30 CBC News Edmonton, “Edmonton police emails, documents provide new information on Canada-first AI facial recognition bodycam project” [CBC News Edmonton] (April 13, 2026), online: <https://www.cbc.ca/news/canada/edmonton/edmonton-police-emails-documents-provide-new-information-on-canada-first-ai-facial-recognition-bodycam-pilot-9.7157991>. According to the Edmonton police, officers will not get alerts or notifications about facial resemblance while on duty. If a person is within four metres of a bodycam, their face is detected and the data is sent to the cloud to compare against the EPS database of persons of interest. If it’s not a match, then the facial data is immediately discarded.
- 31 Edmonton Police Service, “Facial Recognition”, online: <https://www.edmontonpolice.ca/News/FacialRec>. (Accessed September 14, 2026).
- 32 Tracey Nagai, Global News, “Need to do things differently’: Alberta police services look to AI for future” (February 26, 2026), online: <https://globalnews.ca/news/11708183/need-to-do-things-differently-alberta-police-services-look-to-ai-for-future/>.
- 33 New York University, Policing Project, “How Policing Agencies Use AI”, [Policing Project How Police Use AI], online: <https://www.policingproject.org/ai-explained-articles/2024/9/6/how-policing-agencies-use-ai>.
- 34 UK Parliament FRT.
- 35 BBC, “Police start facial recognition trial at stations,” (February 11, 2026), online: <https://www.bbc.com/news/articles/cz6ejlq7j08o>.
- 36 BBC, “Facial recognition to be trialled at Tube stations,” (August 10, 2026), online: <https://www.bbc.com/news/articles/c07r0gvgjxyo>.
- 37 UK Parliament, “Written questions, answers and statements, (January 28, 2026), online: <https://questions-statements.parliament.uk/written-statements/detail/2026-01-28/hcws1285>.
- 38 UK Parliament FRT.
- 39 UK Parliament FRT.
- 40 Metropolitan Police, Live Facial Recognition Annual Report, [Met LFR Report] (2025), online: <https://www.met.police.uk/police-forces/metropolitan-police/areas/about-us/about-the-met/facial-recognition-technology/> at 5.
- 41 Metropolitan Police, “Met Commissioner to announce plans to introduced LFR into crime hotspots across West End” [Met FRT Plans] (June 23, 2026), online: <https://news.met.police.uk/news/met-commissioner-to-announce-plans-to-introduce-lfr-into-crime-hotspots-across-the-west-end-510675>.
- 42 Met FRT Plans.
- 43 Metropolitan Police, “The Commissioner’s full speech on the Met’s use of technology” (June 24, 2026), online: <https://news.met.police.uk/news/the-commissioners-full-speech-on-the-mets-use-of-technology-510746>.
- 44 Big Brother Watch, “Stop Facial Recognition”, online: <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/>. (Accessed September 14, 2026).
- 45 See, for example, Equality and Human Rights Commission, “Met Police’s use of facial recognition tech must comply with human rights law, says regulator” (August 20, 2026), online: <https://www.equalityhumanrights.com/met-polices-use-facial-recognition-tech-must-comply-human-rights-law-says-regulator?return-url=https%3A%2F%2Fwww.equalityhumanrights.com%2Fsearch%3Fkeys%3Dfacial%2B>; Liberty, “Liberty responds to Oxford Street Facial Recognition”, (August 12, 2026), online: <https://www.libertyhumanrights.org.uk/issue/oxford-street-facial-recognition-plans/>; and The Guardian, “Essex police pause facial recognition camera use after study finds racial bias”, (March 20, 2026), online: <https://www.theguardian.com/technology/2026/mar/19/essex-police-pause-facial-recognition-camera-use-study-racial-bias>; and PROBable Futures, *Government consultation on a new legal framework for law enforcement use of biometrics, facial recognition and similar technologies* (February 10, 2026), online: https://research.northumbria.ac.uk/probablefutures/?page_id=2572 at 11.
- 46 For an extensive critique of the UK biometric regulatory landscape, see Ada Lovelace Institute, *An Eye on the Future*, [Ada Lovelace Eye on the Future], (2025), online: <https://www.adalovelaceinstitute.org/report/an-eye-on-the-future/>.

- 47 United Kingdom, Prime Minister’s Office, *The King’s Speech 2026: Background Briefing Notes* (13 May 2026) at 68–69.
- 48 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>. For an industry perspective on the potential uses and benefits of ALPRs, see Scylla AI, *8 Reasons to Use Intelligent Licence Plate Recognition Systems*, online: <https://www.scylla.ai/8-reasons-to-use-intelligent-licence-plate-recognition-systems/> (Accessed March 2025).
- 49 See generally, New York University Policing Project, “Automated Licence Plate Readers” [Policing Project ALPRs], online: <https://www.policingproject.org/automated-licence-plate-readers>.
- 50 See generally, Flock Safety, “Why Flock”, online: <https://www.flocksafety.com/blog/why-flock>.
- 51 UBC AI in Policing at 34.
- 52 IPC ALPR Guidance.
- 53 DeFlock.
- 54 Office of the Inspector General of the Los Angeles Police Commission, *LAPD Review of the Department’s ALPR System and Use in the Field*, (July 10, 2026) [LAPD ALPR Report] at 2, online: https://www.oig.lacity.org/_files/ugd/b2dd23_781bdb1b27314ec4acc45f4b821320d8.pdf.
- 55 See generally, Flock Safety, “Licence Plate Readers”, online: <https://www.flocksafety.com/products/license-plate-readers>.
- 56 Flock Safety, “Why Flock”, online: <https://www.flocksafety.com/blog/why-flock>.
- 57 Toronto Police Service, *Automatic License Plate Reader Technology in TPS Vehicles*, online: <https://www.tps.ca/use-technology/automatic-licence-plate-reader/> (Accessed September 2026).
- 58 Toronto Police Service, “Automatic Licence Plate Recognition”, online: <https://www.tps.ca/use-technology/automatic-licence-plate-reader/> (Accessed September 14, 2026).
- 59 Staff Sergeant Jeff Bassingthwaite, Toronto Police Service, “Tricked-Out-Ride: Outfitting Cars with Computers, Cameras and Integrating ALPR” (4th Annual Police Tech Conference and Expo Mississauga, November 11 2025), slide deck on file with the LCO.
- 60 Ottawa Police Service, “Road Safety, Automatic License Plate Recognition” (accessed September 14, 2026), online: <https://www.ottawapolice.ca/en/sections-and-units/operations-and-support/road-safety-unit/#AutomaticLicencePlateRecognition>.
- 61 LAPD ALPR Report.
- 62 Los Angeles Times, “LAPD suspends use of Flock surveillance cameras over privacy issues” (July 11, 2026), online: <https://www.latimes.com/california/story/2026-07-11/lapd-suspends-use-of-flock-surveillance-cameras-over-privacy-issues>.
- 63 Predictive policing is discussed in the LCO’s Criminal AI Project Issue Paper. See also generally, 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>; Andrew Guthrie Ferguson, *Your Data Will Be Used Against You: Policing in the Age of Self-Surveillance* (NYU Press, March 2026), online: <https://nyupress.org/9781479838295/your-data-will-be-used-against-you/>; 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>; 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>.
- 64 EUROPOL at 15.
- 65 Ferguson 2019 at 491.

- 66 Ferguson 2019 at 491.
- 67 To Surveil and Protect at 41.
- 68 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.
- 69 To Surveil and Protect at 45-46.
- 70 Bureau of Justice Assistance at 7-9.
- 71 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.
- 72 See generally, LCO Police AI Issue Paper and NAS Predictive Policing at 3-4.
- 73 To Surveil and Protect at 47.
- 74 UBC AI in Policing at 19.
- 75 EUROPOL at 17.
- 76 UBC Police AI Report at 20.
- 77 UBC Police AI Report at 47.
- 78 Royal Canadian Mounted Police, National Technology Onboarding Program, *Transparency Blueprint: Snapshot of Operational Technologies*, [RCMP Transparency Blueprint] (2024), online: <https://rcmp.ca/en/corporate-information/publications-and-manuals/national-technology-onboarding-program-transparency-blueprint> at 15.
- 79 RCMP Transparency Blueprint at 16.
- 80 Atlas of Surveillance. See also 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.
- 81 Scott Thompson, *The Existing and Emergent State of UAV/RPAS/Drones Surveillance Capacities and Law Enforcement* [IPC Drone Survey] (2025), online: <https://www.ipc.on.ca/en/resources/research-hub/drones-surveillance-capacities-and-law-enforcement> at 10.
- 82 See generally UBC Police AI Report at 29-33. See also 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> and American Civil Liberties Union, *ACLU White Paper on Police Department's Use of AI to Draft Police Reports*, (2024), online: <https://www.aclu.org/documents/aclu-on-police-departments-use-of-ai-to-draft-police-reports>.
- 83 UBC Police AI Report at 30.
- 84 Ottawa Police Service, "Camera Technology", online: <https://www.ottawapolice.ca/en/community-safety-and-crime-prevention/camera-technology/> (Accessed September 14, 2026).
- 85 See generally UBC Police AI Report at 17-19.
- 86 UBC Police AI Report at 64. See also Government of Canada, "Algorithmic Impact Assessment Results – Griffeye Tool", online: <https://open.canada.ca/data/en/dataset/89898244-aaae-4591-ba9b-fe5cd81d5924/resource/dd50ce04-3150-4f26-b8ab-0ad067489593>.
- 87 UBC Police AI Report at 64.
- 88 SoundThinking Inc., *ShotSpotter Frequently Asked Questions*, online: <https://www.soundthinking.com/faqs/shotspotter-faqs/> (Accessed September 12, 2026).
- 89 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/>.
- 90 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>.

- 91 Policing Project How Police Use AI.
- 92 The Law Commission of Ontario has written an extensive analysis of American bail algorithms. 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>.
- 93 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.
- 94 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>.
- 95 Policing Project How Police Use AI. See also Ada Lovelace Eye on the Future at 24.
- 96 Canadian Lawyer Magazine, “AI on trial: 388 decisions track the rise of AI references across Canada’s courts- Federal Courts, Part 1” (March 20 2026), online: https://www.canadianlawyermag.com/cl-plus/data-reports/ai-on-trial-388-decisions-track-the-rise-of-ai-references-across-canadas-courts-federal-court/393875?_hsmi=410518162; and Canadian Lawyer Magazine, “AI on trial: 388 decisions track the rise of AI references across Canada’s courts- Federal Courts, Part 2” (March 20 2026), online: https://www.canadianlawyermag.com/cl-plus/data-reports/ai-on-trial-388-decisions-track-the-rise-of-ai-references-across-canadas-courts-provincial-courts/393876?_hsmi=410518162.
- 97 Damien Charlotin, “AI Hallucination Cases” (updated September 21 2026), online: https://www.damiencharlotin.com/hallucinations/?q=&sort_by=-date&states=Canada&period_idx=0.
- 98 See generally, Alissa Marque, Heydari, New York University Policing Project, *AI and Prosecution: Mapping the Current and Future Roles of Artificial Intelligence in Prosecution*, (2024), online: <https://www.policingproject.org/misc-articles/ai-in-prosecution>.
- 99 Consultation notes on file with the LCO.
- 100 Public Prosecution Service of Canada, “2026-27 Departmental Plan” (modified March 13 2026), online: https://www.ppsc-sppc.gc.ca/eng/pub/dp-pm/2026_2027/index.html.
- 101 Consultation notes on file with the LCO.
- 102 La Presse, “Un juge a-t-il succombé à la tentation de l’IA?” (March 6 2026), online: <https://www.lapresse.ca/actualites/justice-et-faits-divers/2026-03-06/fausse-jurisprudence-vrai-malaise/un-juge-a-t-il-succombe-a-la-tentation-de-l-ia.php>.
- 103 Office of the Commissioner for Federal Judicial Affairs Canada, “Repository Of Artificial Intelligence (AI) Initiatives In Canadian Courts And Tribunals” (modified May 14 2026), online: <https://www.fja.gc.ca/COVID-19/Repository-of-AI-Initiatives-in-Courts-and-Tribunals-Repertoire-dinitatives-IA-dans-les-tribunaux-eng.html>.
- 104 Legal Aid BC, “Court Services Branch rough transcripts survey” (June 19 2025), online: <https://legalaaid.bc.ca/lawyers/news/court-services-branch-rough-transcripts-survey>. See also Office of the Commissioner for Federal Judicial Affairs Canada, “Repository Of Artificial Intelligence (AI) Initiatives In Canadian Courts And Tribunals” (modified May 14 2026), online: <https://www.fja.gc.ca/COVID-19/Repository-of-AI-Initiatives-in-Courts-and-Tribunals-Repertoire-dinitatives-IA-dans-les-tribunaux-eng.html>.
- 105 Office of the Commissioner for Federal Judicial Affairs Canada, “Repository Of Artificial Intelligence (AI) Initiatives In Canadian Courts And Tribunals” (modified May 14 2026), online: <https://www.fja.gc.ca/COVID-19/Repository-of-AI-Initiatives-in-Courts-and-Tribunals-Repertoire-dinitatives-IA-dans-les-tribunaux-eng.html>.
- 106 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>.
- 107 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>.

- 108 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.
- 109 Some have proposed a role for AI in more accurately assessing testimony or submissions. See 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>.
- 110 Presentation of Gerald Chan, “Use of AI Tools by Legal Counsel” to the Association of Ontario Judges, Joint Annual General Meeting of the Ontario Court of Justice (Niagara, May 21 2026), notes on file with LCO.
- 111 See generally, the LCO’s third Criminal AI Issue Paper, *AI and the Assessment of Risk in Bail and Sentencing* (2025), online: <https://lco-cdo.org/en/publications/ai-in-criminal-justice-paper-3-ai-and-the-assessment-of-risk-in-bail-sentencing-and-recidivism/>.
- 112 Canadian HR Reporter, “AI bot sends confidential info to Ontario hospital patients after recording doctors’ meeting: IPC” (November 21 2025), online: <https://www.hrreporter.com/focus-areas/automation-ai/ai-bot-sends-confidential-info-to-ontario-hospital-patients-after-recording-doctors-meeting-ipc/393766>. See also Auditor General of Ontario, *Use of Artificial Intelligence in the Ontario Government* (2026), online: https://www.auditor.on.ca/en/content/specialreports/specialreports/en26/2026_AI_EN.pdf.
- 113 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>.
- 114 See LCO Police AI Issue Paper.
- 115 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>.
- 116 Consultation notes on file with the LCO.
- 117 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>.
- 118 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 monitors, 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 iAcuity, *Speed vs Scrutiny: How AI is Revolutionizing Crime Analysis*, (2024), online: <https://www.iacuityfintech.com/speed-vs-scrutiny-how-ai-is-revolutionizing-crime-analysis/>.
- 119 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>.
- 120 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 relevant information based on predefined criteria or patterns. [Footnotes omitted.] EUROPOL at 20.

- 121 EUROPOL at 28-29.
- 122 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>.
- 123 See LCO Police AI Issue Paper.
- 124 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>.
- 125 See generally UBC Police AI Report at 13-53.
- 126 Law Commission of Ontario, *Accountable AI*, (2022) [Accountable AI], online: <https://www.lco-cdo.org/en/our-currentprojects/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-currentprojects/ai-adm-and-the-justice-system/> and 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>.
- 127 See LCO Accountable AI at 40-55 for a discussion of AI and human rights.
- 128 For an extensive discussion of the AI data bias and issues, see LCO American Lessons at 20-26.
- 129 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 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), at 3, online: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>. NIST also identified concerns regarding false negatives false positives, gender, and age. See also See UBC Police AI Report at 15.
- 130 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.
- 131 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>.
- 132 See UBC Police AI Report at 15 and accompanying notes discussing the early research.
- 133 Metropolitan Police, *Live Facial Recognition: Annual Report* (September 2025), online: <https://news.met.police.uk/documents/live-facial-recognition-annual-report-2025-dot-pdf-451727-at-15>.
- 134 Marion Oswald et al, PROBABLE Futures, *Government consultation on a new legal framework for law enforcement use of biometrics, facial recognition and similar technologies* (February 10, 2026), online: https://research.northumbria.ac.uk/probablefutures/?page_id=2572 at 11. See also Ada Lovelace Eye on the Future at 20: “In short, the National Physical Laboratory (NPL) study does not confirm LFR is generally safe to use.”
- 135 Ottawa FRT Initiative at 3.

- 136 See generally UBC Police AI Report at 23-24 and 27. The National Academy of Sciences report cited above includes an extensive discussion of predictive policing and bias. See 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.”
- 137 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.
- 138 OHRC Eliminating Racial Profiling at s. 4.2.6.1. 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.
- OHRC Eliminating Racial Profiling at s. 4.2.6.2.
- 139 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/>.
- 140 See generally LCO American Lessons at 20-25.
- 141 INCLO Challenging FRT at 22.
- 142 Office of the Privacy Commissioner of Canada, *Police use of Facial Recognition Technology in Canada and the Way Forward* [Privacy Commissioners Way Forward] (June 10 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/.
- 143 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>.
- 144 Law Commission of Ontario, *Law Enforcement Use of Facial Recognition Technology: Vancouver Roundtable Report* (2025), online: <https://www.lco-cdo.org/CrimAI>.
- 145 Met LFR Report at 5.
- 146 See the discussion and citations in the text box “How FRT is Used in the UK” in Section 2.1. See also Big Brother Watch, “Stop Facial Recognition”, online: <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/> (Accessed September 14, 2026).
- 147 BBC, “Police to trial handheld facial recognition devices” (March 2, 2026), online: <https://www.bbc.com/news/articles/cly2ml86x8go>.
- 148 See generally, OPC Way Forward, Privacy Commissioners Joint Clearview AI Investigation and 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.
- 149 CBC News Edmonton, “Edmonton police emails, documents provide new information on Canada-first AI facial recognition bodycam project” [CBC News Edmonton] (April 13, 2026), online: <https://www.cbc.ca/news/canada/edmonton/edmonton-police-emails-documents-provide-new-information-on-canada-first-ai-facial-recognition-bodycam-pilot-9.7157991>.

- 150 CBC News Edmonton.
- 151 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. For example, the IPC Mugshot Guidance report sets out detailed guidance addressing pre-implementation issues, operational considerations, and program review and evaluation. IPC Mugshot Guidance at 4-33.
- 152 *R. v. Bykovets* (2024 SCC 6) [Bykovets], online: <https://www.canlii.org/en/ca/scc/doc/2024/2024scc6/2024scc6.html>.
- 153 Bykovets.
- 154 See generally, DeFlock.
- 155 The NYU Policing Project identifies several ALPR risks, including privacy; false positives; data sharing; surveillance of protests; and the need for auditing, transparency and enforcement. New York University Policing Project, “A Brief Guide to Licence Plate Readers”, online: <https://www.policingproject.org/automated-license-plate-readers>. See generally, DeFlock, “What is an ALPR?”, online: <https://deflock.org/what-is-an-alpr>.
- 156 LAPD ALPR Report.
- 157 Information and Privacy Commissioner of Ontario, *Guidance on Police Use of Remotely Piloted Aircraft Systems (Drones) in Ontario*, (2026) [IPC Drones], online: <https://www.ipc.on.ca/en/resources/guidance-police-use-remotely-piloted-aircraft-systems-drones-ontario> at 2.
- 158 See generally, 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> and UBC Police AI Report at 18-19 and 20.
- 159 TechnologyReview.com, “How LLMs could supercharge mass surveillance in the US” [LLM Supercharge], (April 21 2026), online: <https://www.technologyreview.com/2026/04/21/1135919/ai-surveillance-privacy-llms-bulk-data/>.
- 160 New York Times, “Twelve Million Phones, One Dataset, Zero Privacy” (December 19 2019), online: <https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html>.
- 161 MIT Technology Review, “How LLMs could supercharge mass surveillance in the US” (April 21 2026), online: <https://www.technologyreview.com/2026/04/21/1135919/ai-surveillance-privacy-llms-bulk-data/>.
- 162 Washington Post, “The powerful tools in ICE’s arsenal to track suspects — and protesters” [Washington Post ICE], (January 29 2026), online: <https://www.washingtonpost.com/technology/interactive/2026/ice-surveillance-immigrants-protesters>.
- 163 Washington Post ICE
- 164 404Media.co, “A Texas Cop Searched License Plate Cameras Nationwide for a Woman Who Got an Abortion” (May 29 2025) [404 Media] online: <https://www.404media.co/a-texas-cop-searched-license-plate-cameras-nationwide-for-a-woman-who-got-an-abortion/>.
- 165 404Media.
- 166 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. See also INTERPOL’s “Transparency Principles” in INTERPOL, *A Policy Framework for Responsible Limits on Facial Recognition* [INTERPOL Policy Framework] (2021), online: <https://unicri.org/A-Policy-Framework%20for-Responsible-Limits-on-Facial-Recognition> at 15-16.
- 167 AI disclosure and transparency issues are discussed extensively in the LCO Criminal AI project papers. See particularly Issue Paper 4, *AI at Trial and On Appeal*.
- 168 See the LCO’s American Lessons report for a good summary of these issues.
- 169 International Network of Civil Liberties Organizations, “Policing FRT: the rights, risks and harms”, online: <https://inclo.net/pillars/surveillance-and-digital-rights/principles-for-use-of-frt/policing-frt-the-rights-risks-and-harms/>.

- 170 Washington Post, “Police seldom disclose use of facial recognition despite false arrests” [Washington Post FRT] (October 6 2024), online: <https://www.washingtonpost.com/business/2024/10/06/police-facial-recognition-secret-false-arrest/>.
- 171 Washington Post FRT.
- 172 See generally, OPC Way Forward and Privacy Commissioners Joint Clearview AI Investigation].
- 173 Government of Canada AI Register, Records 747-760, accessed August 18, 2026. Online <https://open.canada.ca/data/en/dataset/fcbc0200-79ba-4fa4-94a6-00e32facea6b/resource/369f6f34-148a-42ed-b581-8c164e941a89>.
- 174 Royal Canadian Mounted Police, *RCMP Publishes Transparency Blueprint: Snapshot of Operational Technologies* [RCMP Transparency Blueprint] (September 2024), online: <https://rcmp.ca/en/news/2024/09/rcmp-publishes-transparency-blueprint-snapshot-operational-technologies>.
- 175 TPS Use of AI Policy.
- 176 OPC Police FRT Guidance at paras 124-129.
- 177 IPC FRT Mugshot Guidance at 12-13.
- 178 David Freeman Engstrom & Daniel E. Ho, *Algorithmic Accountability in the Administrative State* ((2020) Yale J on Reg 800) at 821, online: <https://www.yalejreg.com/print/algorithmic-accountability-in-the-administrative-state/>.
- 179 These issues are described in several LCO Criminal AI project papers, including the Introduction, Police AI Issue Paper, and AI at Trial and Appeal.
- 180 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.
International Criminal Police Organization (INTERPOL), *Responsible AI Principles* (2024) [INTERPOL Responsible AI Principles] (2024), at 12, online: <https://www.interpol.int/en/How-we-work/Innovation/Artificial-Intelligence-Toolkit>.
- 181 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>.
- 182 See, for example, INCLO Challenging FRT at 14-15.
- 183 INTERPOL Responsible AI Principles at 13.
- 184 INTERPOL Responsible AI Principles at 13.
- 185 Benjamin Perrin, Geoffrey Liew and Isabell Sweeney, *AI & Policing: Knowledge Synthesis Report on the Governance & Use of Artificial Intelligence by Police in Canada*” (2026), online: https://commons.allard.ubc.ca/fac_pubs/2832/ at 1-2.
- 186 For a discussion of “diffused” risks in the UK, see generally, Ada Lovelace Eye on the Future.
- 187 CBC News Edmonton, “Edmonton police emails, documents provide new information on Canada-first AI facial recognition bodycam project” [CBC News Edmonton] (April 13, 2026), online: <https://www.cbc.ca/news/canada/edmonton/edmonton-police-emails-documents-provide-new-information-on-canada-first-ai-facial-recognition-bodycam-pilot-9.7157991>.
- 188 CBC News Edmonton.
- 189 Royal Canadian Mounted Police, “Body Worn Cameras”, online: <https://rcmp.ca/en/body-worn-cameras#s7>. (Accessed September 15, 2026).
- 190 *State v. Loomis*, 881 N.W.2d 749 (Wisc. 2016) [*Loomis*].
- 191 *Loomis* at para 34.
- 192 LCO American Lessons at 35-37.

- 193 See generally, LCO Criminal AI Project Introduction at 20-24 and more specifically in each LCO Criminal AI Project Background Paper.
- 194 Many of these initiatives are recounted in LCO Criminal AI Project Introduction at 32-38.
- 195 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 (2024)* [EU AI Act], 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>.
- 196 EU AI Act, Chapter II, Article 5, s. 1(h).
- 197 EU AI Act, Chapter II, Article 5, s.2.(b).
- 198 EU AI Act, Chapter II, Article 5, s.3.
- 199 EU AI Act, Chapter II, Article 5, s.4.
- 200 EU AI Act, Chapter II, Article 5, s.1(d).
- 201 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).
- 202 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.*
- See: EU AI Act, Chapter III, Annex III.
- 203 EU AI Act, Chapter III, Articles 8-17.
- 204 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>.
- 205 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.
- 206 Executive Order M-24-10 at 21-24.
- 207 Executive Order M-24-10 at 31.

- 208 The list of AI systems included in M-24-10 included:
- 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.
- See: M-24-10 at 32.
- 209 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/>.
- 210 AI Laws By State, “Police & Facial Recognition AI Tracker” (online: <https://www.aillawsbystate.com/tools/facial-recognition-tracker>) (Accessed September 15, 2026). See also other 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/>.
- 211 The LCO can provide a compendium upon request.
- 212 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.
- 213 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>.
- 214 Each of these are explored in more detail in the discussion below.
- 215 Tech Policy Press, “Status of State Laws on Facial Recognition Surveillance”, (January 6, 2025), online: <https://www.techpolicy.press/status-of-state-laws-on-facial-recognition-surveillance-continued-progress-and-smart-innovations/>.
- 216 Airsight, “Drone Laws”, online: <https://www.airsight.com/learn/airspace-security/drone-laws-rules-and-regulations>. (Accessed August 2026.)
- 217 See also, Cleveland.com, “What we learned about Ohio’s new police drone rules and when warrants aren’t required” (September 18, 2026), online: <https://www.cleveland.com/metro/2026/09/what-we-learned-about-ohios-new-police-drone-rules-and-when-warrants-arent-required.html>.
- 218 Cleveland Division of Police, General Police Order [Cleveland Drone Policy], online: https://www.documentcloud.org/documents/25418225-gpo-40607-approved-by-cpc-112024_final-draft/, II. Prohibited Use, C. 2.
- 219 Cleveland Drone Policy, II. Prohibited Use, B.
- 220 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. 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>.

- 221 New York Police Department, Facial Recognition Technology Policy, P.G. 212-129, [NYPD FRT Policy] (2020), online: <https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page>.
- 222 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>.
- 223 NYU Policing Project FRT Resources.
- 224 NYU Policing Project, "Police Disclosure of AI", online: <https://www.policingproject.org/governing-ai-articles/2025/9/8/police-disclosure-of-ai>.
- 225 NYU Policing Project, "Automated License Plate Readers – Policy and Legislative Resources", online: <https://www.policingproject.org/police-disclosure-of-ai>.
- 226 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.
- 227 AI Taxonomy at 94.
- 228 AI Taxonomy at 89.
- 229 AI Taxonomy at 92-94.
- 230 See generally, DeFlock.
- 231 See generally, DeFlock, "What is an ALPR?" See also LAPD ALPR report.
- 232 ACLU You Are Being Tracked.
- 233 DeFlock, "City Council."
- 234 Jesus Jimenez and David Ovalle, "In Red States, Law-and-Order Republicans Turn Against Flock Cameras", New York Times, Sept 5, 2026, [NYT Red States], online at <https://www.nytimes.com/2026/09/05/us/red-states-republicans-flock-cameras.html>.
- 235 CBS 12 News WPEC, "Governor DeSantis calls Flock license plate readers "out of control."" [CBS 12 News] (August 26, 2026), online: <https://www.youtube.com/shorts/m1lItxEuS38>.
- 236 NYT Red States.
- 237 Big Brother Watch, "Stop Facial Recognition", online: <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/> (Accessed September 14, 2026).
- 238 See, for example, Equality and Human Rights Commission, "Met Police's use of facial recognition tech must comply with human rights law, says regulator" (August 20, 2026), online: <https://www.equalityhumanrights.com/met-polices-use-facial-recognition-tech-must-comply-human-rights-law-says-regulator?return-url=https%3A%2F%2Fwww.equalityhumanrights.com%2Fsearch%3Fkeys%3Dfacial%2B>; Liberty, "Liberty responds to Oxford Street Facial Recognition" (August 12, 2026), online: <https://www.libertyhumanrights.org.uk/issue/oxford-street-facial-recognition-plans/>; and The Guardian, "Essex police pause facial recognition camera use after study finds racial bias" (March 20, 2026), online: <https://www.theguardian.com/technology/2026/mar/19/essex-police-pause-facial-recognition-camera-use-study-racial-bias>; and PROBable Futures, *Government consultation on a new legal framework for law enforcement use of biometrics, facial recognition and similar technologies* (February 10, 2026), at 11, online: https://research.northumbria.ac.uk/probablefutures/?page_id=2572.
- 239 For an extensive critique of the UK biometric regulatory landscape, see Ada Lovelace Institute, *An Eye on the Future* [Ada Lovelace Eye on the Future], (2025), online: <https://www.adalovelaceinstitute.org/report/an-eye-on-the-future/>.
- 240 UK Government, *Consultation on a new legal framework for law enforcement use of biometrics, facial recognition and similar technologies*, (December 4, 2025), online: <https://www.gov.uk/government/consultations/legal-framework-for-using-facial-recognition-in-law-enforcement/consultation-on-a-new-legal-framework-for-law-enforcement-use-of-biometrics-facial-recognition-and-similar-technologies-accessible>.

- 241 United Kingdom, Prime Minister's Office, *The King's Speech 2026: Background Briefing Notes* (13 May 2026) at 68–69.
- 242 UK Government, "PoliceAI to speed up investigations and fight crime" (June 10, 2026), online: <https://www.gov.uk/government/news/policeai-to-speed-up-investigations-and-fight-crime>.
- 243 *Ibid.*
- 244 *Ibid.*
- 245 *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>.
- 246 For a discussion of AIDA and responsible criminal AI governance, see LCO Criminal AI Issue Papers – Introduction at 42–43.
- 247 Government of Canada, Canada's *National Artificial Intelligence Strategy: AI for All* [Canada National AI Strategy] (2026), online: https://ised-isde.canada.ca/site/ised/en/canadas-national-artificial-intelligence-strategy-ai-all#_Toc75.
- 248 Canada National AI Strategy at 14.
- 249 Canada National AI Strategy.
- 250 UBC Police AI Report.
- 251 *Safe Social Media Act*, Bill C-34, 1st Sess, 45th Parl, 2026 (first reading 10 June 2026).
- 252 *Protecting Privacy and Consumer Data Act*, Bill C-36, 1st Sess, 45th Parl, 2026 (first reading 15 June 2026).
- 253 Canada, *Directive on Automated Decision-Making* [Canada ADM Directive], 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>.
- 254 See Accountable AI at 57–66 and Regulating AI at 17–49.
- 255 See generally, Accountable AI at 56–66.
- 256 Government of Canada AI Register, Records 747–760, accessed August 18, 2026. Online <https://open.canada.ca/data/en/dataset/fcbc0200-79ba-4fa4-94a6-00e32facea6b/resource/369f6f34-148a-42ed-b581-8c164e941a89>.
- 257 *Enhancing Digital Security and Trust Act*, S.O. 2024, c. 24, [EDSTA], online: <https://www.ontario.ca/laws/statute/24e24>.
- 258 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>.
- 259 EDSTA at ss. 5(1–6), 6(2), 7, 8.
- 260 EDSTA s. 5(1) states that its provisions respecting AI systems "applies to such public sector entities as may be prescribed if they use or intend to use an artificial intelligence system in prescribed circumstances." This section includes two important 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 the legislation. 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 EDSTA governance or requirements.

- 261 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/>.
- 262 Government of Ontario, Ministry of Public and Business Service Delivery and Procurement, *Responsible Use of AI Directive*, December 1, 2024 [Ontario AI Directive].
- 263 The Ontario AI Directive is discussed at length in the LCO Criminal AI Project Introduction.
- 264 RCMP, “National Technology Onboarding Program”, online: <https://rcmp.ca/en/specialized-policing-services/technical-operations/national-technology-onboarding-program>.
- 265 RCMP Transparency Blueprint.
- 266 See generally the program of the 2026 CACP Data and AI Leadership Summit, online: https://www.cacp.ca/cgi/page.cgi/CACP_Data_AI_Leadership_Summit.html.
- 267 See generally, Peel Regional Police Service, “Privacy and Technology”, online: <https://rcmp.ca/en/specialized-policing-services/technical-operations/national-technology-onboarding-program>; Durham Regional Police Service Board, “Use of Artificial Intelligence”, online: <https://durhampoliceboard.ca/policies-and-bylaws/>; York Regional Police, “Facial Recognition Technology”, online: <https://www.yrp.ca/explore/our-work/facial-recognition>; Ottawa FRT Initiative.
- 268 LCO consultations, notes on file.
- 269 TPS AI Policy, “Guiding Principles.”
- 270 TPS AI Policy, “Policy of the Board.”
- 271 Office of the Privacy Commissioner of Canada, Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d’accès à l’information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta (February 2, 2021), online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/>.
- 272 OPC Way Forward.
- 273 IPC FRT Mugshot Guidance.
- 274 *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>.
- 275 Information and Privacy Commissioner of Ontario, *Guidance on Police Use of Remotely Piloted Aircraft Systems (Drones) in Ontario*, (2026) [IPC Drones], online: <https://www.ipc.on.ca/en/resources/guidance-police-use-remotely-piloted-aircraft-systems-drones-ontario> at 2.
- 276 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>.
- 277 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://coursuperieuredubec.ca/fileadmin/cour-superieure/Communiqués_et_Directives/Montreal/Avis_a_la_Commune_juridique-Utilisation_intelligence_artificielle_EN.pdf.
- 278 Federal Court Practice Direction.

- 279 Canadian Judicial Council, *Guidelines for the Use of Artificial Intelligence in Canadian Courts* (Sept. 2024) [CJC Guidelines], online: <https://cjc-ccm.ca/en/news/canadian-judicial-council-issues-guidelines-use-artificial-intelligence-canadian-courts>.
- 280 CJC Guidelines at 6.
- 281 CJC Guidelines at 8-9.
- 282 Consultations with the LCO, notes on file.
- 283 This issue was discussed at both LCO Roundtables in Vancouver and Toronto. Reports available at <https://www.lco-cdo.org/CrimAI>.
- 284 Law Commission of Ontario, *AI and Systemic Oversight Mechanisms in Criminal Justice* (April 2025) at 10, online: <https://www.lco-cdo.org/wp-content/uploads/2025/04/LCO-AI-in-Criminal-Justice-Paper-5-Systemic-Oversight-1.pdf>. With respect to the limited jurisdiction of courts to address policies in other sectors, see LCO Issue Paper 4, *AI at Trial and On Appeal*, at Section 2.2.
- 285 LCO submission to Ontario consultation.
- 286 In section 4.2, this paper outlines a series of federal responses to high risk AI systems, including the *Artificial Intelligence and Data Act* (AIDA), the *Canada National AI Strategy* and the federal *Automated Decision-making Directive*. As discussed, these initiatives share a common concern for governing high risk AI systems. These initiatives are also alike in that they don't establish authority to govern the use of AI in criminal justice.
- 287 Enacted in 2024, the EU AI Act imposes a consistent set of baseline laws governing AI in both the public and private sectors. The AI Act also includes detailed provisions governing AI in criminal justice. In the United States, several jurisdictions have established statutory frameworks governing criminal AI systems. And as outlined in section 4.1, the UK recently committed to establish a new legal framework to underpin law enforcement use of FRT, and to create a single, expert regulatory body to provide independent advice and oversight of regulated AI systems. See generally: 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 (2024)* [EU AI Act], online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689>; and in the UK, Prime Minister's Office, "The King's Speech 2026" (May 13 2026) at 30-33, 124, 126, online: https://assets.publishing.service.gov.uk/media/6a18713db95db968c8f3bbfd/The_King_s_Speech_2026_-_background_briefing_notes.pdf.
- 288 The Honourable François-Philippe Champagne, Letter to the Standing Committee on Industry and Technology (undated October 2023), at 8, online: <https://www.ourcommons.ca/DocumentViewer/en/44-1/INDU/related-document/12600809>.
- 289 See UBC AI & Criminal Justice Initiative, *Draft Principles on the Governance and Use of AI by Police in Canada, 2026* (September 9 2026), online: <https://canlii.ca/t/7nvmp>.
- 290 LCO consultations, notes on file.
- 291 See Council of Europe, *HUDERIA Methodology and Model For Assessing The Risks And Impacts Of AI Systems From The Perspective Of Human Rights, Democracy And The Rule Of Law* (February 25 2026) at 2 and 7, online: <https://www.coe.int/en/web/artificial-intelligence/huderia-risk-and-impact-assessment-of-ai-systems>.
- 292 *ibid.*
- 293 See for example discussion of the TPS AI Policy above.
- 294 Note, for example, that the Edmonton and Ottawa privacy assessments may not be complete assessments of broader impacts on criminal law rights and legal procedure.

- 295 The limited reliability and validity of facial recognition systems – and the unlikelihood of satisfying evidentiary admissibility standards – have been cited by AI vendors including Axon as a rationale for withholding deployment of the technology in Canada. However, vendor self-assessment of the performance of these technologies is claimed to be tilting in favor of their use. See Presentation of Ryan Fritsch, “AI in Criminal Justice” (Canadian Association for the Civilian Oversight of Law Enforcement (CACOLE) 2026 National Conference (Saskatoon, June 3 2026)), notes on file with the LCO.
- 296 *Courts of Justice Act* (R.S.O. 1990, c. C.43), online: <https://www.ontario.ca/laws/statute/90c43>. See also Ontario Superior Court of Justice, “Memorandum of Understanding between the Chief Justice of the Superior Court of Justice of Ontario and the Attorney General of Ontario” (May 5 2008), online: <https://www.ontariocourts.ca/scj/about-the-court-2/jurisdiction/structure-and-governance-of-the-court/mou/>.
- 297 Ontario Superior Court of Justice, “Memorandum of Understanding between the Chief Justice of the Superior Court of Justice of Ontario and the Attorney General of Ontario” (May 5 2008), online: <https://www.ontariocourts.ca/scj/about-the-court-2/jurisdiction/structure-and-governance-of-the-court/mou/>.
- 298 See for example: O. Reg. 400/23: Collection Of Identifying Information In Certain Circumstances- Prohibition And Duties; O. Reg. 391/23: Use Of Force And Weapons; O. Reg. 90/24: General Matters Under The Authority Of The Minister; O. Reg. 406/23: Discipline. Regulations under the *Community Safety and Policing Act, 2019* are available online: <https://www.ontario.ca/laws/statute/19c01>. Regulations under the *Missing Persons Act, 2018* are available online: <https://www.ontario.ca/laws/statute/18m03>.
- 299 See for example: See generally, OPC Way Forward, Privacy Commissioners Joint Clearview AI Investigation and 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.
- 300 See TPS AI Policy; RCMP Technology Blueprint.
- 301 Information and Privacy Commissioner of Ontario, “Letter to Toronto Police Services Board re: Update on the Implementation of the Board’s Policy on Use of Artificial Intelligence Technology in relation to the facial recognition mugshot database program and other AI technologies used by the Toronto Police Service” (January 10 2024), online: <https://www.ipc.on.ca/sites/default/files/legacy/2024/01/2024-01-10-submission-to-the-january-11-2024-toronto-police-services-board-public-meeting-ai-policy-and-the-toronto-fr-mugshot-database-program-e.pdf>.
- 302 *Ibid.*
- 303 See TPS, “Artificial Intelligence Registry” (undated) with risk assessment inventory, online: <https://www.tps.ca/police-reform/artificial-intelligence/>.
- 304 In either circumstance, a lack of formalized transparency reporting means there may be little enforcement or follow-through. For example, Ontario’s Information and Privacy Commissioner raised several concerns with the format, timing, and extent of an initial “AI inventory” report delivered internally to the Toronto Police Services Board in January, 2024. Concerns were also raised with the way AI assessment was conducted and conclusions about the appropriate risk-level assigned to technologies including automated license plate recognition systems. It is unclear if TPS investigated or responded to these concerns, and if any corresponding changes were made in policy or practice. It is clear that the impugned risk assessments were not reclassified.
- 305 Toronto AI Policy.
- 306 European Commission, “Strengthening Europe’s Tech Sovereignty” (June 3 2026), online: <https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty>.
- 307 The strategy commits the EU to develop everything from open-source computer operating systems to independent payment and credit card systems, as well as AI foundation models and chip fabrication. European Commission, “Strengthening Europe’s Tech Sovereignty” (June 3 2026), online: <https://digital-strategy.ec.europa.eu/en/policies/eu-tech-sovereignty>.

- 308 The Guardian, “Anthropic to disable its most advanced AI models after US order limiting foreign access” (June 13 2026), online: <https://www.theguardian.com/technology/2026/jun/13/anthropic-disable-advanced-ai-models-us-government-order>.
- 309 TheConversation.com, “Sovereign AI? Anthropic shutdown reveals Canada’s weakness” (June 17 2026), online: <https://theconversation.com/sovereign-ai-anthropic-shutdown-reveals-canadas-weakness-285473>. See also: The Globe and Mail, “Lost access to Anthropic’s AI models highlights risk of relying on U.S. tech, Canadian experts say” (June 14 2026), online: <https://www.theglobeandmail.com/business/article-anthropic-fable-mythos-ai-offline-canada-risks/>.
- 310 Los Angeles Police Commission, Office of the Inspector General, “Review Of The Department’s ALPR System And Use In The Field” (July 10 2026), at 13-14, online: https://www.oig.lacity.org/_files/ugd/b2dd23_781bdb1b27314ec4acc45f4b821320d8.pdf.
- 311 Los Angeles Police Commission, Office of the Inspector General, “Review Of The Department’s ALPR System And Use In The Field” (July 10 2026), at 6, 20, 95-96, online: https://www.oig.lacity.org/_files/ugd/b2dd23_781bdb1b27314ec4acc45f4b821320d8.pdf.
- 312 Los Angeles Police Commission, Office of the Inspector General, “Review Of The Department’s ALPR System And Use In The Field” (July 10 2026), at 20, online: https://www.oig.lacity.org/_files/ugd/b2dd23_781bdb1b27314ec4acc45f4b821320d8.pdf.
- 313 Los Angeles Police Commission, Office of the Inspector General, “Review Of The Department’s ALPR System And Use In The Field” (July 10 2026), at 23, online: https://www.oig.lacity.org/_files/ugd/b2dd23_781bdb1b27314ec4acc45f4b821320d8.pdf.
- 314 See “What is digital sovereignty?” in Government of Canada, *Digital Sovereignty: A Framework to improve digital readiness of the Government of Canada* (November 2025), online: <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/digital-sovereignty-framework-improve-digital-readiness.html>.
- 315 Canada, Department of Innovation, Science and Economic Development, *Canada’s National Artificial Intelligence Strategy: AI for All* (June 2026), online: <https://ised-isde.canada.ca/site/ised/sites/default/files/documents/ai-strategy-en.pdf>.
- 316 See, for example, the overall vision of the *Strategy* that commits “to develop a responsible, safe, and sovereign AI industry” on the basis that “Prosperity and sovereignty in this era belong to nations that can leverage trust to adopt, build, and govern AI on their own terms”. In this vision, benefits flow from “technological infrastructure over which they [Canadians] have a meaningful degree of sovereign control.” Specific commitments will “build sovereign Canadian AI foundations in compute, data, talent, and infrastructure, ensuring Canadians can trust that the systems they adopt are built and governed on Canadian terms”. However, none of these commitments are specific to criminal justice. In fact, among five identified “Priority Sectors,” criminal justice is not included.
Canada, Department of Innovation, Science and Economic Development, *Canada’s National Artificial Intelligence Strategy: AI for All* (June 2026), at 4-6, online: <https://ised-isde.canada.ca/site/ised/sites/default/files/documents/ai-strategy-en.pdf>.
- 317 Canada, House of Commons, Bill C-36, *An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts* (1st Reading June 15 2026), at s. 63(4-5), online: <https://www.parl.ca/DocumentViewer/en/45-1/bill/C-36/first-reading>.
- 318 C-36 includes some provisions that speak to digital sovereignty. For example, C-36 “introduces rules governing cross-border data transfers” such that: “Organizations routing Canadian personal data to foreign processors or affiliates will face new due diligence obligations, including conducting privacy impact assessments and implementing measures to mitigate risk before data is disclosed or transferred. A review of data-sharing agreements and vendor contracts is advisable now.” See: INQ Law, “Major Changes in Proposed Replacement for PIPEDA: What Bill C-36 Means for Your Organization” (June 16 2026), online: <https://www.inq.law/post/major-changes-in-proposed-replacement-for-pipeda-what-bill-c-36-means-for-your-organization>.

- 319 Canada, House of Commons, Bill C-36, *An Act to enact the Protecting Privacy and Consumer Data Act, to amend the Personal Information Protection and Electronic Documents Act and to make amendments to other Acts* (1st Reading June 15 2026), at s. 63(4-5), online: <https://www.parl.ca/DocumentViewer/en/45-1/bill/C-36/first-reading>. For a discussion of the proposed right to an explanation of automated decision making see Theresa Scassa, “Bill C-36’s proposed right to an explanation of automated decision-making” (August 20 2026), online: <https://teresascassa.substack.com/p/bill-c-36s-proposed-right-to-an-explanation>.
- 320 Auditor General of Ontario, *Use of Artificial Intelligence in the Ontario Government* (2026), online: https://www.auditor.on.ca/en/content/specialreports/specialreports/en26/2026_AI_EN.pdf.
- 321 Auditor General of Ontario report May 2026.
- 322 Auditor General of Ontario report May 2026.
- 323 Auditor General of Ontario report May 2026.
- 324 UBC AI & Criminal Justice Initiative, *Draft Principles on the Governance and Use of AI by Police in Canada, 2026* (September 9 2026), online: <https://canlii.ca/t/7nvmp>.
- 325 For example, the EU AI Act establishes a standing Advisory Forum (Article 67) and a Scientific Panel (Article 68), while open public consultations were conducted on defining “high risk” AI uses under the European Commission’s public consultation framework (online at: https://commission.europa.eu/about/service-standards-and-principles/transparency/consultations_en). In the UK, a consultative AI White Paper proposed five clear principles for existing UK regulators to follow, and set out expectations for responsible AI. Consultations were subsequently reported in UK Department for Science, Innovation & Technology, “A pro-innovation approach to AI regulation: government response” (updated February 6 2024), online: <https://www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response#executive-summary>.
- 326 INTERPOL cites significant public consultations in development of their Artificial Intelligence Toolkit. See: INTERPOL, “Artificial Intelligence Toolkit” (undated), online: <https://www.interpol.int/How-we-work/Innovation/Artificial-Intelligence-Toolkit>.
- 327 International Association of Chiefs of Police, *Implications Associated with Police Use of Artificial Intelligence* (2025) at p 5, as cited and discussed in Perrin LCO, *Draft Policing Principles*.
- 328 For example, Canada’s Treasury Board Secretariat asserts in the Directive on Automated Decision Making that “Information about the efficacy, fairness, and transparency of an AI system should be publicly available.” See: Treasury Board, *Directive on Automated Decision-Making* (modified 24 June 2025) at s. 6.5, online: <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592>, as cited and discussed in Perrin LCO, *Draft Policing Principles*.
- 329 “Unacceptable Risks,” the EU AI Act establishes categories for “high risk”, “limited risk”, and “Minimal or Low Risk” AI systems. See: EU AIA at Articles 5, 6 and 50, online: <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-5>.
- 330 TPS AI Policy.
- 331 Many of these are discussed above in Section 4.2, “Responsible Criminal AI in Canada.”
- 332 See: EU AIA at Articles 5, 6 and 50, online: <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-5>.
- 333 TPS Use of AI Policy.
- 334 LCO consultations, notes on file.
- 335 EU AI Act, art 5(1)(d).
- 336 EU AI Act, art 5(1)(e).
- 337 EU AI Act, art 5(1)(g).
- 338 EU AI Act, arts 5(1)(h), 5(2)-(7).
- 339 Toronto Police Service Board, *Use of Artificial Intelligence Technology* [TPSB, *Use of AI Policy*] (28 February 2022; updated 11 January 2024), online: <https://tpsb.ca/home/about/policies-by-laws/board-policies/use-of-artificial-intelligence-technology/>.

- 340 EDSTA s. 5(6).
- 341 AIDA s. 17(1).
- 342 The list in Chapter 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.
- 343 EU AI Act, Chapter III, arts 8-17.
- 344 Effectively, this enshrines the kind of additional provincial and federal consultation the LCO suggests above, and may be exemplified by the decision of the Supreme Court in *R. v. Spencer* (2014 SCC 43). In that case, the court interpreted the PIPEDA prohibition on corporations disclosing personal info to law enforcement as having an exception, but also requiring separate specific legislative authorization to rely on that exception.
- 345 See for example Axon’s product Auto-Transcribe, which is described as a tool that “transforms the entire evidence management process [f]rom report writing with Draft One to streamlined evidence search and audio redaction, fast, dependable transcripts lay the foundation for future AI innovations across the Axon ecosystem”, one which “enhances efficiency, saving agencies critical time during evidence review.” Axon.com, “Auto-Transcribe” (accessed May 15 2026), online: <https://www.axon.com/products/auto-transcribe>.
- 346 Auditor General report.
- 347 Maura Grossman, Presentation to the Atlantic Criminal Court Judges Annual Conference (September 24 2026), notes on file with the LCO.
- 348 For instance, popular AI scribe systems are known to intentionally obscure the editing trail or prompts used to generate a police report, making it harder to test the evidence and the account of events. Over time, these practices can also impair the ability of a police officer testify, as erroneous reports are relied on and generate false memories and characterization of events. Furthermore, recent US studies show a tendency among police to under-report the use of AI, furthering the potential for harm and misconduct. Without proper disclosure and assessment, AI systems will not be effectively subject to testing through a criminal justice proceeding. See: ArsTechnica.com, “Cops’ favorite AI tool automatically deletes evidence of when AI was used” (July 10 2025), online: <https://arstechnica.com/tech-policy/2025/07/cops-favorite-ai-tool-automatically-deletes-evidence-of-when-ai-was-used/>; Taurus Myhand, “Once the Jury Sees It, The Jury Can’t Unsee It: The Challenge Trial Judges Face When Authenticating Video Evidence in the Age of Deepfakes” (29 Widener L. Rev. 171 (2023)); and, Washington Post, “Police seldom disclose use of facial recognition despite false arrests: A Post investigation found that many defendants were unaware of the technology’s role in linking them to crimes, leading to questions of fairness” (October 6 2024), online: <https://www.washingtonpost.com/business/2024/10/06/police-facial-recognition-secret-false-arrest/>.
- 349 See Presentation of Dirk Niles, Peel Police Service, “Artificial Intelligence Policies, Procedures, and Governance in Practice: Community-Based Real-World Application of AI in Policing” (Canadian Association for the Civilian Oversight of Law Enforcement (CACOLE) 2026 National Conference (Saskatoon, June 3 2026)), notes on file with the LCO.
- 350 LCO consultations, notes on file.
- 351 Government of Canada, “Government of Canada AI Register” (updated April 28 2026), online: <https://open.canada.ca/data/en/dataset/fcbc0200-79ba-4fa4-94a6-00e32facea6b>.

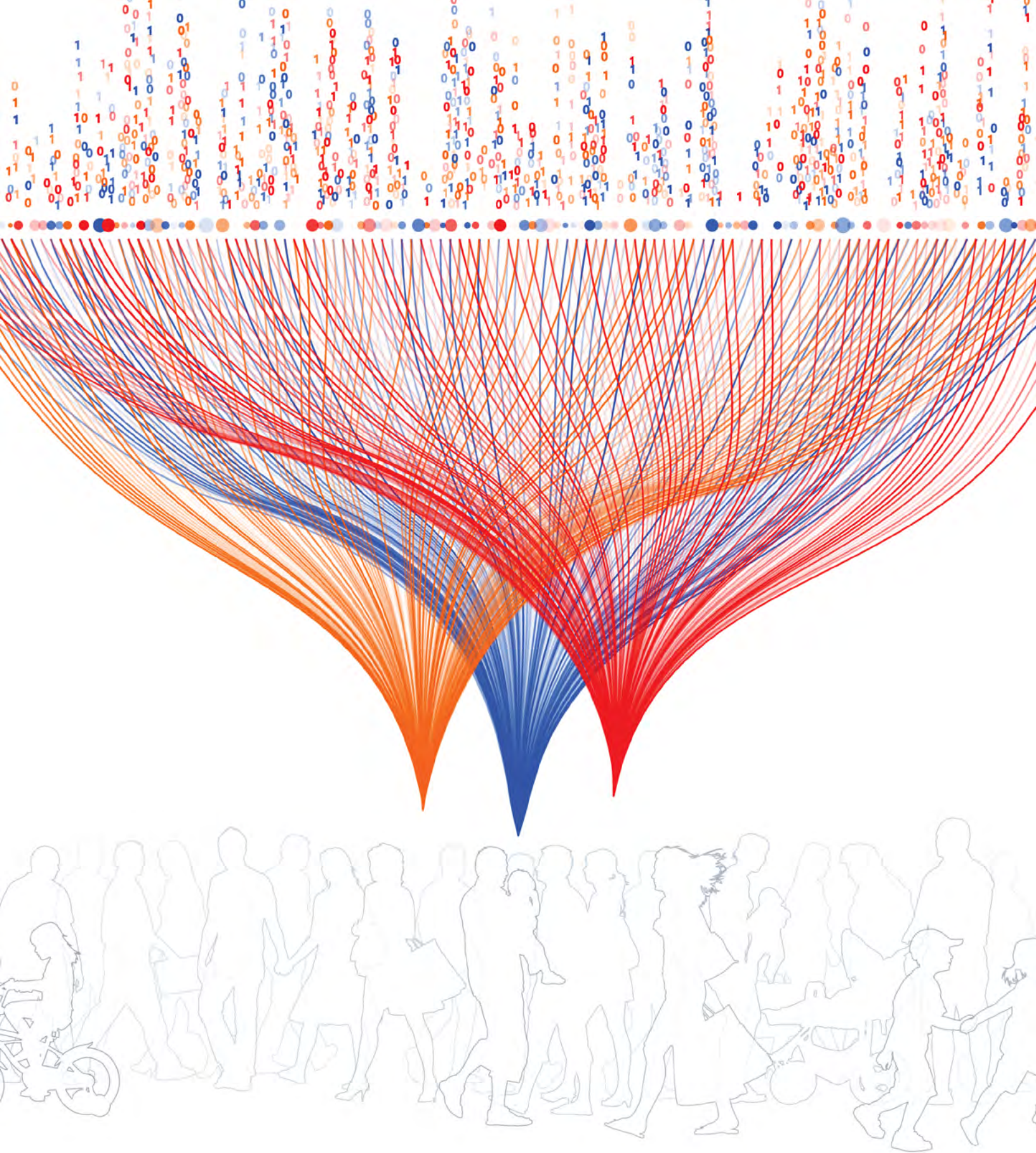
- 352 For the RCMP see “Algorithmic Impact Assessments Results- Voice 2 Text application” (December 23 2024), online: <https://open.canada.ca/data/en/dataset/7612202f-1530-41ce-80c7-6e121f5fcadc>; and “Algorithmic Impact Assessment Results- Griffeye Tool” (November 21 2024), online: <https://open.canada.ca/data/en/dataset/89898244-aaae-4591-ba9b-fe5cd81d5924>.
- 353 See for example: Connecticut: https://portal.ct.gov/das/knowledge-base/articles/bits/ai-inventory?language=en_US; New York Focus, “New York Is Struggling to Track Its Own AI Use” (July 30 2026), online: <https://nysfocus.com/2026/07/30/new-york-ai-systems-inventory-findings>; Texas Observer, “Texas’ AI-Powered Surveillance Arsenal Has Ballooned. Proposed Laws Provide Few Guardrails” (March 31 2025), online: <https://www.texasobserver.org/texas-dps-surveillance-arsenal-artificial-intelligence-lege/>; California: <https://www.cdt.ca.gov/technology-innovation/hrads-login/faqs/>;
- 354 See European Commission, “Article 71: EU database for high risk AI systems listed in Annex III” (June 13 2024), online: <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-71>. For sensitive AI system used by law enforcement see European Commission, “Article 49: Registration” (June 13 2024), online: <https://ai-act-service-desk.ec.europa.eu/en/ai-act/article-49>.
- 355 Government of Ontario, “Artificial Intelligence (AI) in Ontario” (updated July 14 2026), online: <https://www.ontario.ca/page/artificial-intelligence-ai-ontario>.
- 356 Ministry of Public and Business Service Delivery, “Artificial Intelligence (AI) use cases in the Ontario Public Service” (updated June 9 2026), online: <https://data.ontario.ca/dataset/artificial-intelligence-ai-use-cases-in-the-ontario-public-service>.
- 357 For example, other known and reported uses of AI in Ontario public service include inmate risk classification systems, FRT systems, AI scribes, and potential reliance on federal uses of AI in immigration cases. See: BreachMedia, “Lawsuit says AI tool disproportionately places Black prisoners in maximum security in Ontario” (July 19 2026), online: <https://mashable.com/tech/lawsuit-says-ai-tool-disproportionately-places-ontario-black-prisoners>; Auditor General of Ontario, *Use of Artificial Intelligence in the Ontario Government* (2026), online: https://www.auditor.on.ca/en/content/specialreports/specialreports/en26/2026_AI_EN.pdf; 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>; and Toronto Star, “Canada rejected her permanent residence application. Her job duties were made up — by Immigration’s AI reviewer” (May 6 2026), online: https://www.thestar.com/news/canada/canada-rejected-her-permanent-residence-application-her-job-duties-were-made-up-by-immigrations-ai-reviewer/article_3f1ea5be-0b3d-4541-ac00-0a1b8484d877.html.
- 358 At the moment, the public registry only contains three examples of AI use from across the entire Ontario Public Service: a general purpose “generative AI assistant”; a tool for listing statutory requirements across all Ontario legislation and regulations; and a chatbot to assist social assistance staff in applying legislation and policies. The registry discloses eight basic categories of information for each registered AI use case, including:
- The Ministry responsible
 - A paragraph describing the use case
 - How the “human in the loop” uses the tool (described in a sentence); and
 - A sentence about the data used.
- See: Ministry of Public and Business Service Delivery, “Artificial Intelligence (AI) use cases in the Ontario Public Service” (updated June 9 2026), online: <https://data.ontario.ca/dataset/artificial-intelligence-ai-use-cases-in-the-ontario-public-service>.
- 359 Ministry of Public and Business Service Delivery, “Artificial Intelligence (AI) use cases in the Ontario Public Service” (updated June 9 2026), online: <https://data.ontario.ca/dataset/artificial-intelligence-ai-use-cases-in-the-ontario-public-service>.
- 360 Office of the Auditor General of Ontario, “Performance Audit: Use of Artificial Intelligence in the Ontario Government” (2026), at 3, online: https://www.auditor.on.ca/en/content/specialreports/specialreports/en26/2026_AI_EN.pdf.

- 361 Office of the Auditor General of Ontario, “Performance Audit: Use of Artificial Intelligence in the Ontario Government” (2026), at 3, online: https://www.auditor.on.ca/en/content/specialreports/specialreports/en26/2026_AI_EN.pdf.
- 362 TPS Use of AI Policy.
- 363 Toronto Police Service, “Artificial Intelligence” (undated), online: <https://www.tps.ca/police-reform/artificial-intelligence/>.
- 364 See See TPS, “Artificial Intelligence Registry” (undated) with risk assessment inventory, online: <https://www.tps.ca/police-reform/artificial-intelligence/>.
- 365 Ontario Ministry of Public and Business Service Delivery and Procurement, “AI use cases in the OPS” (updated June 9 2026), online: <https://data.ontario.ca/dataset/artificial-intelligence-ai-use-cases-in-the-ontario-public-service/resource/b8778f78-f1dc-4f95-9bd1-2420bb4cbc11>.
- 366 See the discussion above in Section 2.7.
- 367 See the discussion in Sections 2.11 and Section 6 at Recommendations 21-24.
- 368 See Canadian Judicial Council, *Guidelines for the Use of Artificial Intelligence in Canadian Courts* (1st Edition, September 2024), online: <https://cjc-ccm.ca/sites/default/files/documents/2024/AI%20Guidelines%20-%20FINAL%20-%202024-09%20-%20EN.pdf>.
- 369 Amy Salyzyn, “Shadow AI: A Growing Problem for Canadian Courts” (August 26 2026), online: <https://www.slaw.ca/2026/08/26/shadow-ai-a-growing-problem-for-canadian-courts/>.
- 370 Amy Salyzyn, “Shadow AI: A Growing Problem for Canadian Courts” (August 26 2026), online: <https://www.slaw.ca/2026/08/26/shadow-ai-a-growing-problem-for-canadian-courts/>.
- 371 LCO consultations, notes on file with the LCO.
- 372 See Government of Ontario, “Crown Prosecution Manual” (updated January 31 2024), online: <https://www.ontario.ca/document/crown-prosecution-manual>.
- 373 Access to this database is limited to the European Commission and designated national authorities. Examples of law enforcement related AI systems deemed for registration in secure, non-public section of the registry include AI systems:
- to assess the risk of a natural person becoming the victim of criminal offences;
 - in support of law enforcement authorities as polygraphs or similar tools;
 - to evaluate the reliability of evidence in the course of the investigation or prosecution of criminal offences;
 - to assess personality traits and characteristics or past criminal behaviour of natural persons or groups;
- for the profiling of natural persons in the course of the detection, investigation or prosecution of criminal offences.
- 374 European Commission, “Annex III” (June 13 2024), at s. 6, online: <https://ai-act-service-desk.ec.europa.eu/en/ai-act/annex-3>.
- 375 Ontario, “Ontario’s Trustworthy Artificial Intelligence (AI) Framework” (updated December 1 2025), online: <https://www.ontario.ca/page/ontarios-trustworthy-artificial-intelligence-ai-framework>.
- 376 Presentation of Kurt Martin, Edmonton Police Service, “Edmonton Police Service: BWV and DEMS Implementation” (Canadian Association for the Civilian Oversight of Law Enforcement (CACOLE) 2026 National Conference (Saskatoon, June 3 2026)), notes on file with the LCO.
- 377 Taylor Lambert, CBC News Edmonton, “Edmonton police emails, documents provide new information on Canada-first AI facial recognition bodycam project” (April 13, 2026), online at <https://www.cbc.ca/news/canada/edmonton/edmonton-police-emails-documents-provide-new-information-on-canada-first-ai-facial-recognition-bodycam-pilot-9.7157991>. According to the Edmonton police, officers will not get alerts or notifications about facial resemblance while on duty. If a person is within four metres of a bodycam, their face is detected and the data is sent to the cloud to compare against the EPS database of persons of interest. If it’s not a match, then the facial data is immediately discarded. CBC, “Edmonton Police Service partners with US company to test use of facial-recognition bodycams” (December 2, 2025), online at <https://ca.news.yahoo.com/edmonton-police-partners-u-company-043758681.html>.
- 378 Presentation of Kurt Martin, Edmonton Police Service, “Edmonton Police Service: BWV and DEMS Implementation” (Canadian Association for the Civilian Oversight of Law Enforcement (CACOLE) 2026 National Conference (Saskatoon, June 3 2026)), notes on file with the LCO.

- 379 Tracey Nagai, Global News, “Need to do things differently’: Alberta police services look to AI for future” (February 26, 2026), online at <https://globalnews.ca/news/11708183/need-to-do-things-differently-alberta-police-services-look-to-ai-for-future/>.
- 380 Citizen Lab, “Edmonton Police Trial AI Facial Recognition Bodycams”, online: <https://citizenlab.ca/edmonton-police-trial-ai-facial-recognition-bodycams/>.
- 381 CBC News, “Alberta privacy commissioner, police at odds over pilot of facial recognition technology,” (December 3, 2025), online: <https://www.cbc.ca/news/canada/edmonton/edmonton-alberta-police-privacy-commissioner-ai-bodycams-9.7001945>.
- 382 Office of the Inspector General of the Los Angeles Police Commission, *LAPD Review of the Department’s ALPR System and Use in the Field*, (July 10, 2026) [LAPD ALPR Report] at 2, online: https://www.oig.lacity.org/_files/ugd/b2dd23_781bdb1b27314ec4acc45f4b821320d8.pdf. See also: Futurism.com, “LAPD Abandons Flock Contract After Making a Horrifying Discovery” (July 13 2026), online: <https://futurism.com/future-society/lapd-abandons-flock-contract-false-alarm> noting that as implemented by the LAPD, the Flock ALPR system “carry an error rate of 32.3 percent, effectively giving officers a one-in-three chance at pulling an innocent person over.”
- 383 LCO consultations, notes on file.
- 384 European Commission, “European AI Office” (updated September 8 2026), online: <https://digital-strategy.ec.europa.eu/en/policies/ai-office>.
- 385 European Commission, “European AI Office” (updated September 8 2026), online: <https://digital-strategy.ec.europa.eu/en/policies/ai-office>.
- 386 See European Commission, “AI Act Scientific Panel” (updated June 1 2026), online: <https://digital-strategy.ec.europa.eu/en/policies/ai-scientific-panel>; and European Commission, “AI Act Advisory Forum” (updated June 12 2026), online: <https://digital-strategy.ec.europa.eu/en/policies/ai-advisory-forum>.
- 387 Gov.UK, “PoliceAI to speed up investigations and fight crime” (June 10 2026), online: <https://www.gov.uk/government/news/policeai-to-speed-up-investigations-and-fight-crime>.
- 388 Gov.UK, “PoliceAI to speed up investigations and fight crime” (June 10 2026), online: <https://www.gov.uk/government/news/policeai-to-speed-up-investigations-and-fight-crime>.
- 389 Futurism, “Cop Accused of Using AI to Fake Evidence” (June 18 2026), online: <https://futurism.com/artificial-intelligence/cop-ai-fake-evidence-uk>.
- 390 A more detailed discussion is in LCO, *Issue Paper 2: Use of AI by Law Enforcement* (April 2025) at section 3.4, online: <https://lco-cdo.org/en/publications/ai-in-criminal-justice-paper-2-use-of-ai-by-law-enforcement/>.
- 391 See the discussion above in Section 2.7.
- 392 This issue was discussed at both LCO Roundtables in Vancouver and Toronto. Reports available at <https://www.lco-cdo.org/CrimAI>. These issues were further discussed at a second roundtable in Vancouver: UBC AI & Criminal Justice Initiative and Law Commission of Ontario, “AI & Policing Symposium Report” (September 9 2026), online: <https://canlii.ca/t/7nvmn>.
- 393 LCO consultations repeatedly discussed how AI systems may rely on a range of underlying models and techniques of varying strengths, weakness, capabilities and task appropriateness. Consultees noted that AI systems are often frequently updated, changing the performance characteristics of the product. AI development is also largely unregulated. AI testing is in its infancy, including independent scientific validation of the validity of an AI system (that it does what it claims to do) and the reliability of AI systems (that similar variables result in similar outputs). AI testing is often done by vendors and in lab-like conditions, undermining claims and often not reflecting diminished performance in real-world use cases, such as the example of the LAPD Inspector General Report.

- 394 LCO consultations repeatedly discussed how oversight and validation of AI systems is often shifted onto individual officials who are undermined and unqualified to confirm recommendations and results. Participants shared concerns that AI products almost always come with a disclaimer that a “human in the loop” has to “review”, “confirm” or “certify” results. The view was expressed that this lets an AI vendor or service provider avoid accountability (in court or otherwise) and externalize product design deficiencies, errors, and liability onto individual officials. Simultaneously, such designees are routinely prone to human frailties including automation bias, poor or no training, time and performance pressures, a lack of control or meaningful critical knowledge of how an AI system operates, and perverse incentives (such as number of authorizations issued per day). These failures were both confirmed and strongly criticized among participants in the LCO and UBC Faculty of Law joint Vancouver Symposium. A recent major conference of police and police oversight agencies from across Canada confirmed a widely held view that the “human in the loop” can’t be a final *event* in a chain of evidence, but rather has to be operationalized as a continuous *process* of oversight and verification throughout the chain of evidence. The very visible systemic results of these failures have also been widely reported in US, UK and Canadian media. See for example: See: The Guardian, “Tennessee grandmother jailed after AI facial recognition error links her to fraud” (March 12 2026), online: <https://www.theguardian.com/us-news/2026/mar/12/tennessee-grandmother-ai-fraud>; NBC News, “Detroit woman sues city after being falsely arrested while pregnant due to facial recognition technology” (August 6 2023), online: <https://www.nbcnews.com/news/us-news/detroit-woman-sues-city-falsely-arrested-8-months-pregnant-due-facial-rcna98447>; and on the fallibility of judges as a check and balance, see Reuters, “Two federal judges say use of AI led to errors in US court rulings” (October 23 2025), online: <https://www.reuters.com/sustainability/society-equity/two-federal-judges-say-use-ai-led-errors-us-court-rulings-2025-10-23/>; and in Canada see La Presse, “Un juge a-t-il succombé à la tentation de l’IA?” (March 6 2026), online: <https://www.lapresse.ca/actualites/justice-et-faits-divers/2026-03-06/fausse-jurisprudence-vrai-malaise/un-juge-a-t-il-succombe-a-la-tentation-de-l-ia.php>.
- 395 Several notable examples bear mentioning. For instance, a recent public presentation by judges of Ontario’s Court of Appeal, Superior Court, and Court of Justice discussed a case in which a litigant used AI to fabricate a formal letter from the Toronto Police Service, and sought to admit the letter into evidence. The ruse was only caught because the AI misspelled “Police” in the generated logo. See: LexisNexis Canada, “Artificial Intelligence and the Ontario Courts: Current State and Perspectives” (online webinar, June 18 2026), online: <https://canada.lexisnexis.com/l/1079963/2026-06-22/3q33cb>.
- There is also concern that the casual ease with which AI tools produce convincing results may tempt officials and undermine public confidence in justice institutions. Recently, for instance, Vancouver police released a public relations photo to promote the seizure of a small amount of street drugs, cash, and paraphernalia. The image, however, was quickly identified as including obvious flaws introduced by AI. Public outcry was vociferous and evidenced a deep distrust that police would take such a casual approach to manipulating or faking key evidence to persuade the public. One commenter bluntly asked: “Hey so are we faking evidence now?” See: CTVNews Vancouver, “Vancouver police explain ‘made with AI’ image of seized drugs, cash” (June 24 2026), online: <https://www.ctvnews.ca/vancouver/article/vancouver-police-explain-made-with-ai-image-of-seized-drugs-cash/>.
- Similar events have happened in other jurisdictions. Police in the UK are reportedly “investigating one law enforcement officer who’s alleged to have used generative AI to create evidential material in a number of cases.” See: CTVNews Vancouver, “Vancouver police explain ‘made with AI’ image of seized drugs, cash” (June 24 2026), online: <https://www.ctvnews.ca/vancouver/article/vancouver-police-explain-made-with-ai-image-of-seized-drugs-cash/>.
- 396 See Ontario Court Civil Rules Committee, “Consultation On Proposals For Rules Of Civil Procedure Relating To Evidence And Artificial Intelligence” (July 2025). For the LCO’s detailed response to the proposed rules, see Law Commission of Ontario, “Letter to Courts of Ontario Artificial Intelligence Subcommittee of the Civil Rules Committee re: Consultation on proposals for Rules of Civil Procedure relating to evidence and Artificial Intelligence” (September 15 2025), online: <https://www.lco-cdo.org/wp-content/uploads/2025/10/CRC-AI-Evidence-LCO-Submission-Final-September-15-2025.pdf>; and Law Commission of Ontario, “Letter to Courts of Ontario Artificial Intelligence Subcommittee of the Civil Rules Committee re: AI and Bias – Additional Submissions” (December 1 2025), at 2, on file with the LCO. The draft rule is in Ontario Civil Rules Committee Artificial Intelligence Sub-Committee, “The Proposed Rules from the AI Subcommittee for the Civil Rules Committee – Final Draft” (undated), on file with the LCO.

- 397 For a helpful summary of development see National Law Review, “AI-Generated Deepfakes in Court: An Emerging Threat to Evidence Authenticity?” (June 11 2025), online: <https://natlawreview.com/article/ai-generated-deepfakes-court-emerging-threat-evidence-authenticity>.
- 398 CCC 482(2-3).
- 399 See LCO Issues Paper 3, AI and the Assessment of Risk in Bail, Sentencing and Recidivism, available at: <https://www.lco-cdo.org/CrimAI>.
- 400 *R v Julian* (1972 CarswellNS 17 (CA)) at para 5; *Toronto Star Newspapers Ltd v Canada* ([2010] 1 SCR 721) at para 28 which states “there are practically no prohibitions as regards to the evidence the prosecution can lead to show cause why the detention of the accused in custody is justified.” See also: *Criminal Code* (RSC 1985, c C-46) at ss. 518(1)(d)(e).
- 401 Washington Post, “Police seldom disclose use of facial recognition despite false arrests” (October 6 2024), online: <https://www.washingtonpost.com/business/2024/10/06/police-facial-recognition-secret-false-arrest/>. The investigation described the scope of the problem: “Hundreds of Americans have been arrested after being connected to a crime by facial recognition software... but many never know it because police seldom disclose their use of the controversial technology. Police departments in 15 states provided The Post with rarely seen records documenting their use of facial recognition in more than 1,000 criminal investigations over the past four years. According to the arrest reports in those cases and interviews with people who were arrested, authorities routinely failed to inform defendants about their use of the software — denying them the opportunity to contest the results of an emerging technology that is prone to error, especially when identifying people of color. In fact, the records show that officers often obscured their reliance on the software in public-facing reports, saying that they identified suspects “through investigative means” or that a human source such as a witness or police officer made the initial identification.”
- 402 Washington Post, “Police seldom disclose use of facial recognition despite false arrests” (October 6 2024), online: <https://www.washingtonpost.com/business/2024/10/06/police-facial-recognition-secret-false-arrest/>.
- 403 A summary of these and other funding programs is found in LCO Criminal AI Issue Paper, *AI and Systemic Oversight Mechanisms*.
- 404 See: Ontario, Centre of Forensic Sciences, online: <https://www.ontario.ca/page/centre-forensic-sciences>.
- 405 See: Ontario, Centre of Forensic Sciences, online: <https://www.ontario.ca/page/centre-forensic-sciences>.
- 406 See: Ontario, Centre of Forensic Sciences, online: <https://www.ontario.ca/page/reporting-forensic-examination-results-and-opinions>.
- 407 Recently for example Anthropic.ai implemented a digital watermark to its AI products, see: Forbes, “Claude Is Now Putting Invisible Watermarks In AI-Generated Text—Here’s What That Means” (August 14 2026), online: <https://www.forbes.com/sites/anishasircar/2026/08/13/claude-will-now-leave-a-watermark-on-everything-it-writes-what-does-that-mean/>. Following Executive Orders from the Biden White House, leading AI vendors committed to developing watermarking technology for AI. See: Reuters, “OpenAI, Google, others pledge to watermark AI content for safety, White House says” (July 21 2023), online: <https://www.reuters.com/technology/openai-google-others-pledge-watermark-ai-content-safety-white-house-2023-07-21/>.
- 408 See for example: *R. v. Gerezghier* (2024 BCSC 780), online: <https://canlii.ca/t/k4pdr>, and the associated remedy ruling in *R. v. Gerezghier* (2024 BCSC 1255), online: <https://canlii.ca/t/k5s8m>. See also: *R. v. Medow* (2025 ONCJ 661), online: <https://canlii.ca/t/kh447>.



Law Commission of
Ontario
Commission du droit
de l'Ontario

2030 Ignat Kaneff Building
Osgoode Hall Law School, York University
4700 Keele Street, Toronto, Ontario, Canada M3J 1P3