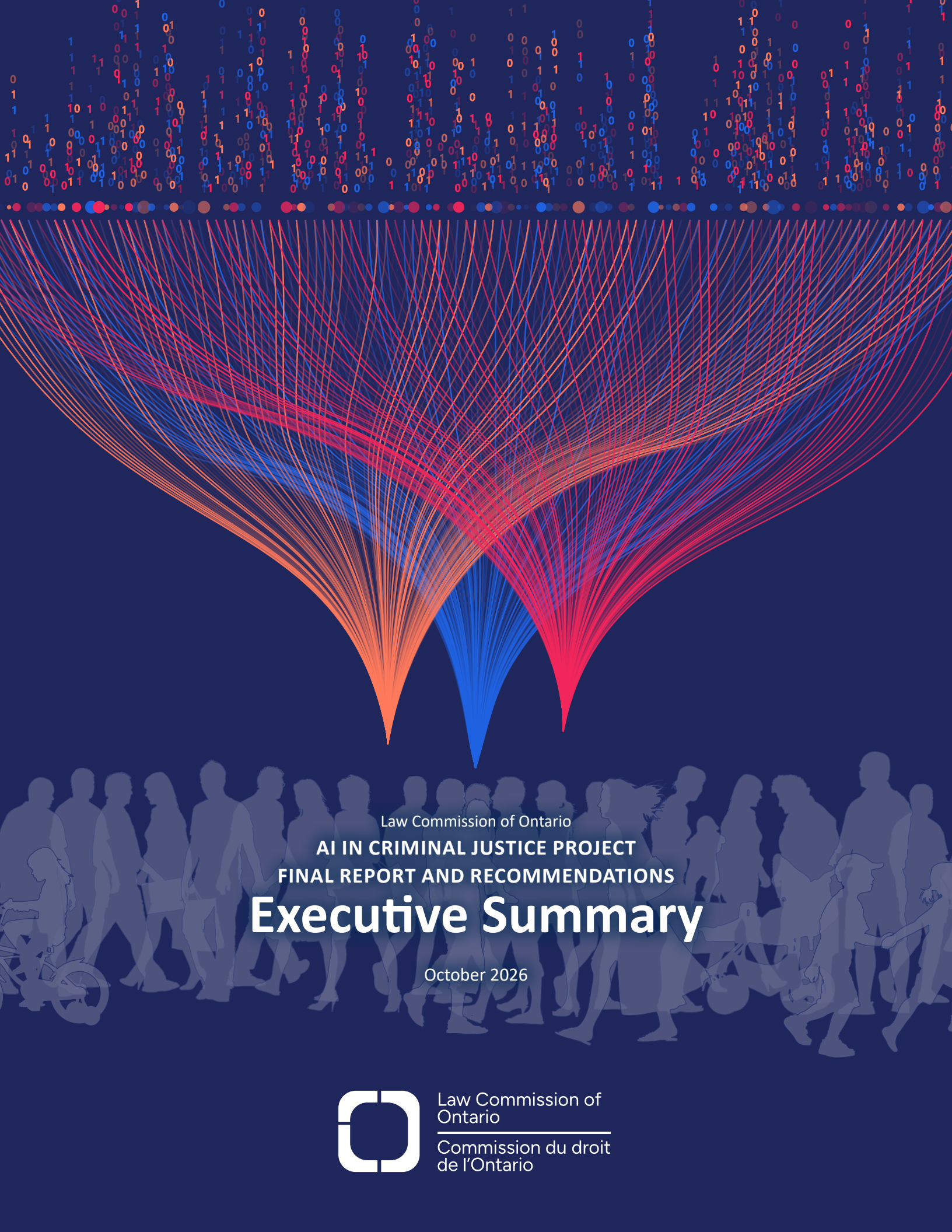




Law Commission of Ontario

AI IN CRIMINAL JUSTICE PROJECT
FINAL REPORT AND RECOMMENDATIONS

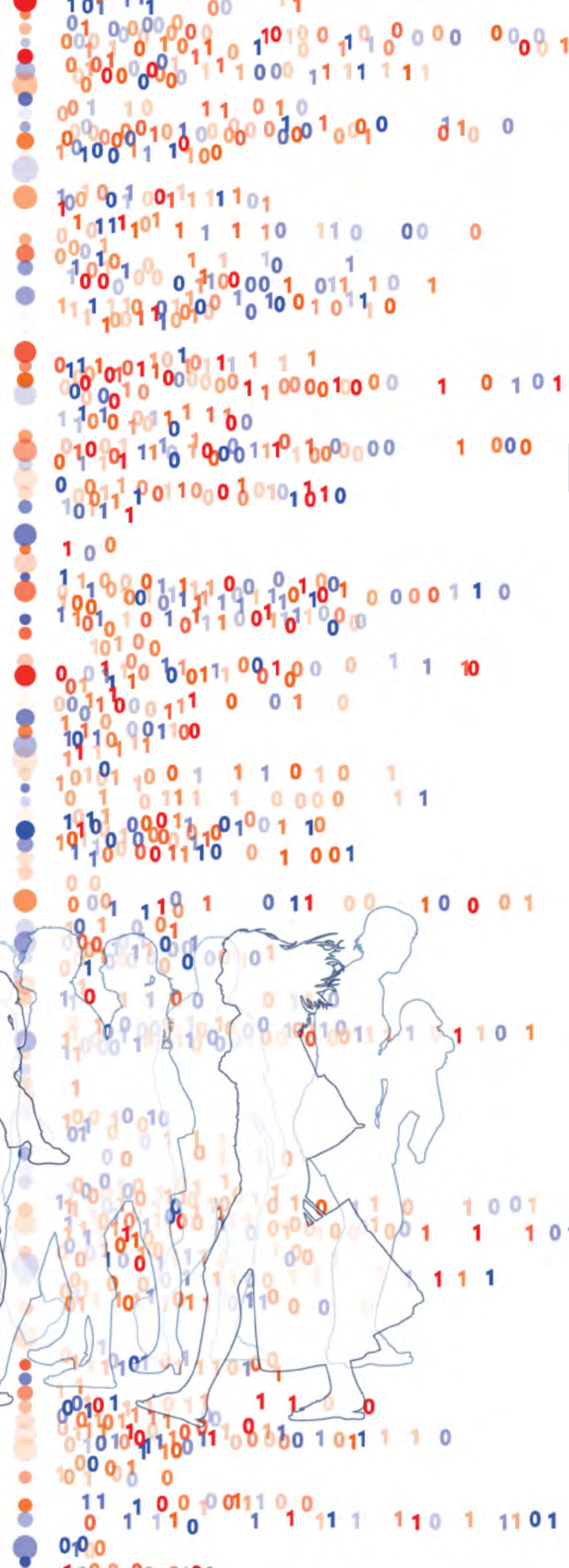
Executive Summary

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.

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.

More information about the LCO and this project is available at: <https://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

Disclaimer

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

Project Lead and Contact

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

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://lco-cdo.org>

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

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

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.



Law Commission of Canada
Commission du droit du Canada

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 of AI in the Canadian criminal justice system.

In April 2025, the LCO released a project introduction 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](#)

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

In addition to the project Issue Papers, the LCO convened two half-day roundtable events to consider key criminal justice AI issues, including a June 2025 [Vancouver Roundtable on the Use of Facial Recognition Technology by Law Enforcement](#) and an August 2025 [Toronto Roundtable on AI Evidence in Criminal Justice](#).

[Project Advisory Committee members](#) and [Issue Paper authors](#) include representatives from governments, police services, Crowns, the criminal defence bar, legal aid, courts administration, human rights and privacy commissions, civil society and public interest organizations, and academics.

The project included extensive consultations and engagements across the provincial and Canadian criminal justice system. In total, more than 1,400 people participated in more than 30 public discussions, workshops, conferences and public lectures across Canada.

The LCO also 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.

All project materials are available on the LCO's AI in Criminal Justice [webpage](#).



Introduction

This is the Executive Summary of the *Final Report and Recommendations* of the Law Commission of Ontario (LCO)'s [Artificial Intelligence in Criminal Justice Project](#) (the "Criminal AI project").

AI is increasingly used in criminal justice systems in Canada and worldwide to aid investigations, analyze evidence, conduct risk assessments, 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, AI report-writing and many more.

Many AI technologies can 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 procedure, 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 2024.¹ Criminal AI tools are also deployed widely in the US, including a network of up to 140,000 ALPRs.²

In these examples and others, criminal AI systems are alternately praised for improving public safety and criticized for mass surveillance, bias, violation of procedural rights, errors and hallucinations. In response, 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.

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

Adoption of responsible criminal AI governance in Canada appears slower also. To date, no Canadian government has enacted laws or regulations governing the use of AI by Canadian police or criminal courts. That said, many Canadian police services and other criminal justice institutions have developed AI self-governance policies.

The LCO believes that criminal AI systems introduce new and complex risks that could expose an unprecedented number of Ontarians to police surveillance, privacy violations, racial bias and other risks and harms.

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. The LCO and others believe the provincial response to these risks must be coordinated and systemic to ensure systems are legal, beneficial and have public trust.

The LCO's 29 recommendations would embed responsible AI principles and policies throughout Ontario's 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 full text of the LCO's Criminal AI Project Final Report and Recommendations are available [here](#).

Criminal AI in Canada

The extent of AI use by police and other criminal justice institutions in Canada is not known. The UBC Police AI Report, police service disclosures and media reports suggest the following Canadian police services have used or are using the following AI systems:³

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

Automated Licence Plate Readers

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

Object Recognition and Video Analytics

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

Predictive Policing

- Calgary Police Service
- Vancouver Police Service
- Saskatoon Police Service

Autonomous Robots, Drones and Vehicles

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

Gunshot Detection

- Toronto Police Service

Open Source and Social Media Monitoring

- Calgary Police Service
- RCMP

AI-Assisted Police Reports

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



Criminal AI Systems and Their Potential

Section 2 of the *Final Report* discusses the most common criminal justice AI systems used in the US, UK and Canada. Most are police systems; however, AI is also used by prosecutors, courts and others.⁴

The LCO's research and consultations demonstrate that, depending on how they are deployed, AI systems have significant potential to improve public safety and the criminal justice system. 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 large datasets or documents.
- Analyze evidence.
- Predict the location of future crimes or perpetrators.
- Prepare police reports, transcribe or translate recordings.

Three of the best known or most common police AI systems include:

Facial Recognition Technology (FRT)

FRT compares a "faceprint" or probe image against a reference image in a database and makes a prediction about whether the images match. There are many types and variations of FRT, including systems used for suspect identification, missing person or human trafficking investigations, child sexual abuse investigations, crowd surveillance and identity verification.

There are important legal and operational differences between FRT systems. For example, live FRT scans images from live camera feeds to identify or track individuals in real time. In contrast, retroactive FRT is used to identify individuals from previously recorded images or videos.

The most extensive FRT deployment may be in the UK, where a large-scale, national live FRT system is currently being implemented. The UK uses live FRT mobile vans and fixed cameras to scan crowds and match faces against a specific police watchlist in real time.⁵ FRT is reportedly used by almost 1,000 law enforcement agencies in the US.⁶

It is unknown how many police in Canada are using FRT due to the lack of mandatory disclosure of policing AI systems. 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.⁷

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. The Edmonton system is notable: Edmonton police have begun testing body cameras equipped with FRT trained to detect the faces of about 7,000 people police say have serious criminal warrants or who are flagged as potential safety risks.

Automated Licence Plate Readers (ALPRs)

ALPRs and vehicle surveillance systems use mobile or fixed cameras to detect information about vehicles, such as a vehicle's license plate number and other information. ALPRs have been described as "vehicle fingerprints." ALPRs assist police to quickly find stolen vehicles and unlicensed, prohibited, suspended and/or uninsured drivers. ALPRs can also be used to track individuals.

The scale of ALPR surveillance is unprecedented: The Los Angeles Police Department scanned more than 210 million license plates in two months in 2025.⁸

It is not clear how widely ALPRs are deployed in Ontario or Canada. The Toronto Police Service states it uses ALPRs to "receive real-time alerting in patrol vehicles to arrest wanted criminals, recover stolen vehicles and locate missing persons that are on various hotlists." The Toronto Police Service reports that its ALPRs can scan more than 1.25 million licence plates every day.⁹

Predictive Policing

Predictive policing is a generic name for police AI systems that process and analyze large and complex datasets much more quickly than humans. Predictive policing has many applications but is commonly understood as AI systems that try to predict or 'forecast' future crime, including 1) location-based systems that identify where and when potential criminal activity might occur, and 2) person-based systems that identify individuals who are likely to be involved in future crimes.

Predictive policing has been used extensively across the US. Canadian police that have used or tested predictive policing include the Vancouver (GeoDASH) and Calgary Police Departments (Palantir Gotham).

Other AI Systems Used by Police

Other AI systems used or considered by police include open-source intelligence and social media intelligence; drones; AI-assisted police reports; evidence management; gunshot detection, bail and sentencing algorithms; and biometric inferencing.

Criminal Courts, Crowns and Defence Counsel

Police are not the only criminal justice institution or actor using AI. Prosecutors can use AI to help manage digital evidence, automate redactions, streamline document generation and analyze forensic evidence. Courts have used AI to aid in writing judgements; for legal research, drafting, and translation; to generate transcripts; and to help litigants complete and file forms. Lawyers and unrepresented litigants may use AI systems for legal research and writing; to draft pleadings and submissions; to evaluate evidence; to test testimony; or to summarize transcripts, analyze expert reports and prepare cross-examination.



Criminal AI Harms and Risks

Section 3 of the *Final Report* discusses criminal AI's risks and potential harms.¹⁰

Legal Risks

Bias and Discrimination

Many FRT systems have been shown to be biased and discriminatory. Many advocates believe that FRT bias is conclusive proof that FRT systems should be banned in whole or in part. Others believe that FRT bias is a diminishing issue and that better training data or systems can mitigate errors.

Many predictive policing systems have also been proven to be biased and discriminatory, leading to the withdrawal of many systems in the face of legal challenges and public outcry. There have been significant bias concerns about other criminal AI systems, especially bail/sentencing algorithms.

Privacy and Surveillance

Privacy and surveillance risks are one of most widely discussed risks of criminal AI systems, particularly FRT systems. Privacy and surveillance risks can vary widely depending on how FRT systems are used. For example, 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 dedicated investigative or mugshot database.

The deployment of FRT in the UK example illustrates the privacy risks of FRT deployed at scale. In the UK, police services have used live FRT vans and static FRT to surveil millions of people, including more than 3 million people in London in a single year.¹¹ UK live FRT surveils people in criminal "hot spots", in major shopping districts, on trains and subways, at sporting events and music festivals, and other locations.

Canadian police FRT systems have also been criticized on privacy and surveillance grounds, including use of the ClearviewAI by the RCMP and the Edmonton Police Service's piloting of FRT body cameras.

ALPRs have been heavily criticized for privacy violations and for promoting mass surveillance. Police use of drones also raises important privacy and surveillance issues, as have criminal AI systems, such as video analytics, social media monitoring and predictive policing.

Disclosure and Transparency

Disclosure and transparency are fundamental elements of legal and public accountability, especially in the context of criminal prosecutions. Criminal AI systems have been criticized for 1) lack of transparency or public disclosure about the existence of an AI system, and 2) lack of disclosure to an accused during an investigation or prosecution.

In Canada, there is no comprehensive disclosure of police or other criminal justice AI systems. The RCMP and Toronto Police Service have organizational policies requiring disclosure of their AI systems. These policies are not consistent.

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.”¹² 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.

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. FRT and predictive policing systems in particular have been subject to strident criticisms of their training data. The accuracy, reliability, and validity of FRT systems can also be influenced depending on how and when it is used. INTERPOL notes, for example, that “...the accuracy of [FRT systems]...varies widely depending on the quality of the image fed into the system.”¹³

After reviewing the evidence of police AI testing, the UBC AI & Criminal Justice Project concluded:

*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.*¹⁴

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.

First, there are many laws and regulators governing criminal AI systems in Ontario, 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 police regulations, directives or policies.
- Policies or guidance from police boards, police services and provincial agencies.
- Decisions and policies from courts, privacy and human rights commissions, law societies and others.

Second, there is a wide, diverse, and decentralized provincial network of institutions who could be involved in operating, overseeing, litigating or adjudicating criminal AI issues Ontario, including:

- All 53 police services in Ontario.
- Police service boards, municipalities, and regional governments.
- The provincial Ministry of the Solicitor General and Ministry of the Attorney General.
- The Inspector General of Policing and Law Enforcement Complaints Agency.
- Crown Attorneys.
- Criminal judges sitting on both the Ontario Court of Justice and Superior Court.
- Criminal defence counsel, duty counsel and Legal Aid Ontario.
- Justices of the Peace.

The combination of multiple laws, multiple actors/institutions and complex technologies could result in ad hoc, inconsistent or improper governance of criminal FRT systems, especially if and when these systems are deployed at scale across Ontario.

The LCO also frequently heard about the risks and challenges of deploying or governing AI within 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 management, evidence management, digital sovereignty evaluation, and more. These are complicated and expensive tasks, potentially out of reach for all but the largest and best resourced criminal justice institutions.

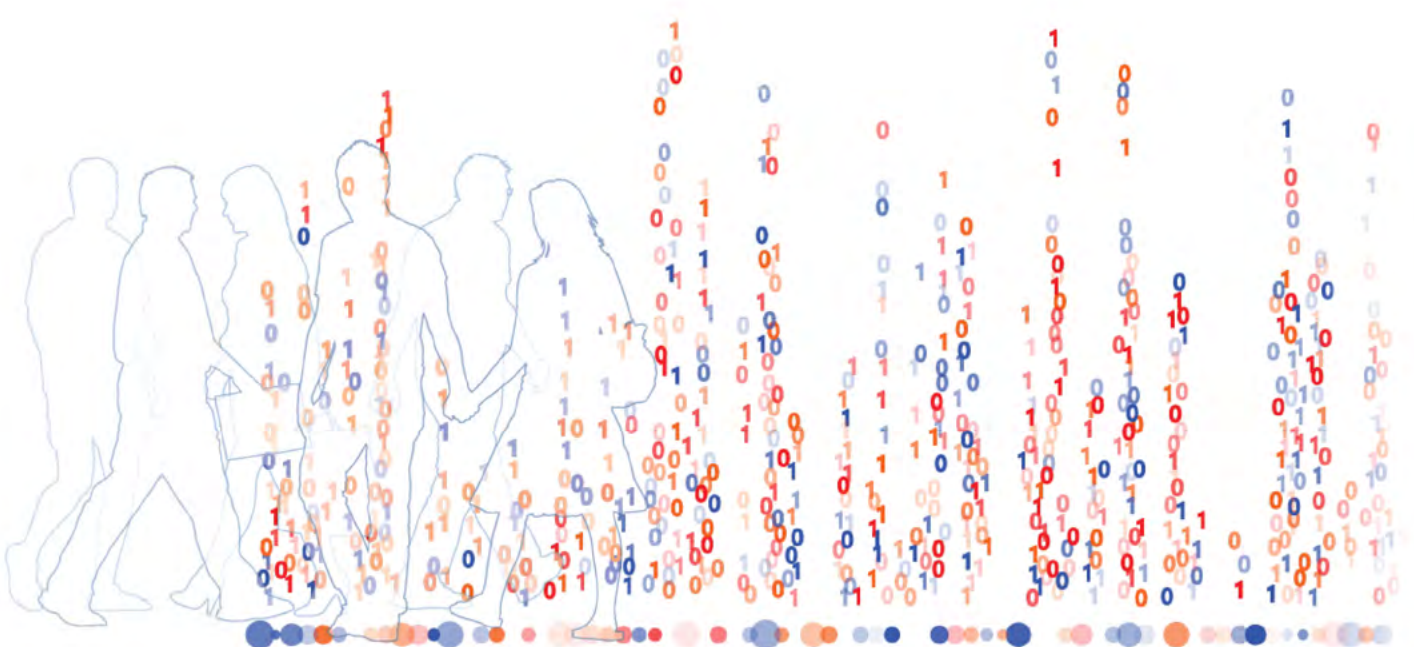
Our consultations and research revealed sophisticated efforts within and between many Canadian police organizations to address institutional issues proactively, including impressive initiatives by the RCMP, Toronto Police Service and Canadian Association of Chiefs of Police (CACP). This approach, while commendable, brings risks and inefficiencies. For example, many organizations discussed the need to develop common or consistent criminal AI impact assessments, compliance or procurement policies. Many consultees also stated institutions were trying to solve the same problem at the same time.

Administration of Justice and Access to Justice Risks

The risks described above create complex new administration of justice and access to justice risks. For example, it is not clear that courts have the capacity or tools to address the complex and systemic statistical, technical, policy and legal issues that will arise in criminal cases involving AI evidence.

Equally important, it will be very difficult for most criminal defendants (particularly those represented by legal aid or who are self-represented) to mount an effective challenge to the complex statistical, technical and legal issues raised by AI systems, especially in bail or sentencing hearings.

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.





Responsible Criminal AI

Section 4 of the *Final Report* reviews responsible criminal AI internationally and in Canada.¹⁵

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.

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.

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 restricted use 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.

The European Union Artificial Intelligence Act

The most important international AI governance statute is the European Union's *Artificial Intelligence Act* (EU AI Act).¹⁶ 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 perhaps 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 a partial ban on real time mass FRT and biometric surveillance¹⁷ and a partial ban on predictive policing.¹⁸ Both prohibitions are subject to several exceptions. 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.¹⁹ In the event police or governments deploy these systems, the EU AI Act requires many oversight and mitigation requirements.

United States

The US federal government has seen dramatic shifts in responsible criminal AI rules and policies. The Biden Administration established a comprehensive responsible criminal AI framework, including detailed requirements for up to 18 criminal justice “rights-impacting” AI systems used by U.S. departments and agencies.²⁰ In January 2025, these requirements were rescinded by the Trump Administration.

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 2026.²¹ These laws 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.

Drone regulation is also common, with as many as 18 US states passing legislation requiring police agencies to obtain a search warrant to use drones for surveillance or to conduct a search.²²

There is a currently a national controversy in the US regarding ALPRs, where the pushback against “Flock” cameras (named after 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 to with federal officials, including immigration authorities.

DeFlock, an American ALPR advocacy organization, reports that 153 cities have cancelled or rejected ALPR contracts or deactivated cameras since 2021, including more than 50 in August 2026 alone.²³ The Republican Governor of Florida recently called the use of ALPRs in Florida “out of control”²⁴ 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 AI surveillance state where everything we’re doing is being tracked at all times.”²⁵

United Kingdom

The expansion of FRT in the UK has been rapid and controversial, and it has been described as “spiralling out of control.”²⁶ Many critics, including the UK’s Equality and Human Rights Commissioner, have noted the risks of privacy violations, racial bias and police harassment. Critics also state that rapid FRT deployment is proceeding in the absence of a statutory and policy framework.

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.”²⁷ 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.”²⁸

Canada

In contrast to the EU, US and UK, there are no dedicated federal or provincial statutes, regulations or policies governing criminal AI systems in Canada.

Federal Government

There is no federal legislation governing criminal AI systems in Canada. The failed 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,²⁹ but would not have directly regulated the use of AI in the public sector or criminal justice system. Nor have there been AI-specific amendments to the *Criminal Code of Canada* or other relevant federal legislation.

In May 2026, the federal government introduced *Canada's National Artificial Intelligence Strategy: AI for All*.³⁰ However, the *Strategy* did not establish trustworthy AI in criminal justice. Nor does the *Strategy* appear to promote responsible criminal AI through the regulation of private sector firms providing criminal AI systems as *AIDA* might have.

Since the *Strategy* was announced, the federal government has introduced two new AI-related bills, Bill C-34 (the *Safe Social Media Act*)³¹ and Bill C-36 (the *Protecting Privacy and Consumer Data Act*) which update private sector privacy laws.³² Neither Bill addresses responsible criminal AI.

The most important federal responsible AI initiative is the 2021 federal Automated Decision-making Directive (federal ADM Directive) and Algorithmic Impact Assessment (AIA).³³ The federal ADM Directive and AIA do not explicitly apply to federal law enforcement agencies. However, the RCMP has voluntarily complied, posting 14 reports to the Government of Canada AI Register.³⁴

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 Government of Ontario passed the *Enhancing Digital Security and Trust Act, 2024 (EDSTA)* in November 2024.³⁵ 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."³⁶ *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.³⁷ *EDSTA* does not apply to AI used in Ontario's criminal justice system.

The provincial government followed *EDSTA* with its "Responsible Use of Artificial Intelligence Directive" in December 2024, but it does not explicitly apply to AI systems used by Ontario police or in Ontario's criminal courts.³⁸

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 (NTOP) and Transparency Blueprint are sophisticated initiatives that incorporate many responsible criminal AI principles.

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").³⁹ Several other Ontario police services have adopted limited AI policies, including services in Peel, Durham, York and Ottawa.

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 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

Privacy Commissioners

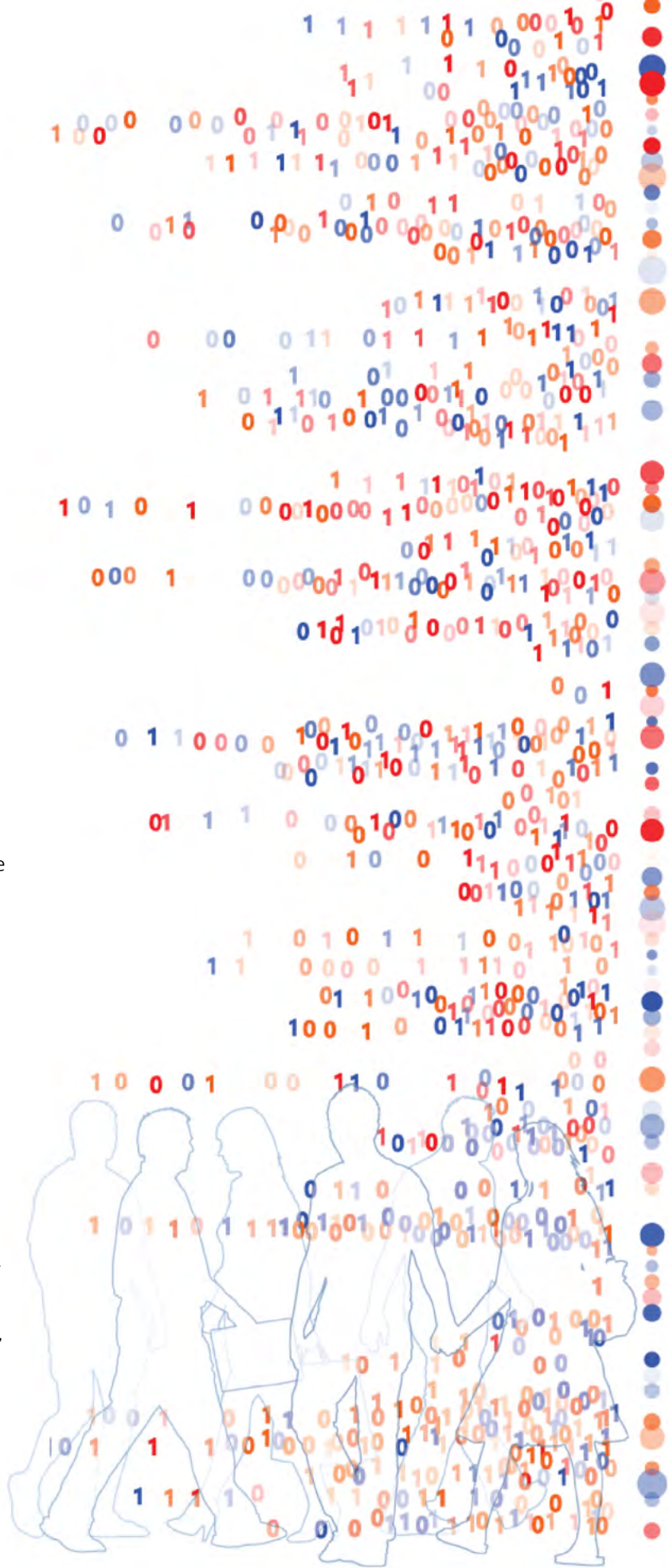
Canadian Privacy Commissioners have taken a prominent and important leadership role in promoting responsible criminal AI in Canada. To date, Privacy Commissioners have completed at least six investigations, reports or guidance documents on FRT and other AI issues in Canadian policing.

Courts

The most significant development in court-based responsible AI policy in Canada is a proposed new Rule of Civil Procedure in Ontario. In 2025 and 2026, the Ontario Civil Rules Committee Artificial Intelligence Sub-Committee (“Civil Rules Sub-Committee”) proposed a new Rule governing AI evidence in civil proceedings in Ontario. This rule could be an important precedent for rules in criminal justice.

Other Criminal Justice Institutions

In addition to police Privacy Commissioners and courts, there are many other departments, boards, agencies and organizations potentially using, regulating or adjudicating AI systems in Ontario’s criminal justice system. 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.





Gaps, Risks and Opportunities in the Canadian Criminal Justice System

Section 5 of the *Final Report* summarizes the LCO's analysis of the legal and governance landscape governing provincial criminal AI systems. Our research and consultations confirm that there are still wide and consequential gaps in the framework governing criminal AI systems in Ontario, including:

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

These gaps will be significantly worsened if and when more Ontario police services and other criminal justice institutions adopt AI. The result will be unacceptable legal risks, inefficiencies, barriers to responsible AI adoption and missed opportunities to improve public safety.

Failure to regulate criminal justice AI systems could mean FRT, ALPRs, predictive policing and other technologies could be introduced in Ontario without appropriate “guardrails” or accountability requirements. The potential harm to criminal defendants, criminal courts and public trust is foreseeable and significant. The lack of consistent AI disclosure, bias, or risk assessment requirements will also mean that police, governments, counsel, and courts will struggle to determine the appropriate uses and limits of criminal justice AI systems.

Notwithstanding this analysis, there are many reasons to be optimistic. The LCO found a near-universal desire amongst criminal justice system stakeholders for a proactive and collaborative strategy to address criminal AI governance issues in Canada. LCO consultations also found widespread agreement on a set of core principles for achieving responsible AI 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.



LCO Recommendations

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. The recommendations are based on precedents, practices and strategies already in place in Canada and other jurisdictions or currently in development by Canadian law enforcement, governments or other justice institutions.

The full text of the LCO’s Criminal AI Project recommendations are available [here](#).

Recommendations 1-3: Provincial Criminal AI Framework

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

- Public disclosure of criminal AI systems.
- Risk criteria identifying prohibited, high risk, restricted use and low risk uses.
- A dedicated and mandatory impact assessment.
- A duty to evaluate AI systems against Canadian law and for lawful authority and purpose.
- Procedural protections.
- Support for criminal justice AI pilots.
- Mandatory and ongoing auditing and evaluation requirements.
- Procurement standards and policies governing responsible software practices.
- An independent supervisory body.
- Guarantees for judicial independence and investigative privilege.

A provincial framework will promote responsible criminal AI adoption across Ontario; improve the province’s ability to promote, evaluate and oversee AI systems; and establish a transparent and comprehensive provincial agenda.

Recommendation 4: Provincial Criminal Justice AI Legislation

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

- A precautionary principle.
- The duty to prioritize compliance with fundamental Canadian rights, law and values.
- Mandatory risk categories.
- Public disclosure, risk assessment, legal safeguards and auditing requirements.

Recommendation 4 addresses the need for provincial consistency and baseline requirements. Provincial legislation will bring coherence and coordination to what is now a decentralized and disorganized network. The need for provincial coordination is growing as more Ontario police services and other institutions begin to use AI.

Recommendation 4 also establishes governing rules commensurate with the legal rights and risks at stake. AI in the criminal justice system affects some of the 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.

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.

Fortunately, Ontario has already established the precedent of framework AI legislation. *EDSTA* establishes provincial authority to regulate AI use across most of Ontario's public sector. Recommendation 4 would establish legislative AI governance in criminal justice. It would be puzzling if AI in most of Ontario's public sector was subject to AI legislation, but the highest risk criminal justice systems were not.

There are many international precedents for establishing framework legislation to govern AI systems.

Recommendation 4 also includes a precautionary principle and a requirement to give priority to assess criminal AI systems for conformity with Canadian criminal law. Together, these provisions 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.

Over 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. 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.

Recommendation 5-7: Provincial Reporting and Oversight

LCO Recommendations 5-7 establish provincial responsible criminal AI reporting and oversight regime.

There are many statutes, regulations and policies in Ontario ensuring public reporting and transparency in provincial law enforcement, including the *Community Safety and Policing Act, 2019*. These provisions are essential to good governance, effective oversight and public trust in law enforcement, especially in high risk contexts. Province-wide reporting obligations also promote consistent, comprehensive evidence-based reports, rules and enforcement.

In contrast, there is no comprehensive public disclosure about 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.

Recommendations 5-7 establish the critical infrastructure needed to support an effective criminal AI reporting and public accountability regime in Ontario. These recommendations promote evidence-based criminal AI governance. They also support responsible AI adoption and public trust and accountability.

Recommendation 5 would centralize criminal AI expertise within two independent oversight agencies, the Inspector General of Policing and the Law Enforcement Complaints Agency. This will promote their capacity to oversee AI systems, to investigate complaints and to report on systemic issues.

Recommendation 5 is an interim measure. It anticipates Recommendation 6, which would establish the authority to create a dedicated provincial supervisory authority for AI systems in criminal justice, which is also discussed in Recommendation 19.

Recommendation 7 supports these objectives by requiring 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 would protect digital sovereignty in Ontario's criminal AI systems. It would also establish 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. Additional provisions are discussed in Recommendation 18.

Recommendation 9: Public Engagement

LCO 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 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.

The LCO's recommendations reflect several principles and objectives widely supported in our consultations, including:

- The governance of criminal AI systems must be based on risk.
- It is a priority to identify and mitigate the risks of high-impact criminal AI systems.
- Risk management supports responsible criminal AI, legal accountability and public trust.
- 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/interoperability between organizations.
- Risk management should be supported by centralized expertise, monitoring and certification.
- Public engagement is necessary.

Recommendations 10 and 11 establish the baseline or prerequisites of this framework. Recommendations 12 to 15 address specific issues.

Recommendation 10 would legislate four categories of criminal AI risk: Prohibited, High Risk, Restricted Use and Low Risk. These categories are consistent with the risk categories in the EU *AI Act* and other international legislation and frameworks. These categories are also consistent with established Canadian AI risk categories, including those included the federal ADM Directive, *EDSTA* and, most importantly, the Toronto Police Use of AI Policy.⁴⁰

These categories were widely supported in our consultations as reflecting an appropriate sliding-scale of AI system capabilities, risks and mitigation measures. These categories have been recently adopted in a draft Canadian Association of Chiefs of Police AI guidance framework.

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. As a result, Recommendation 11 commits the province to public consultations on important AI risk management issues.

Recommendations 12 to 15: Risk Criteria, Practices and Mitigation

Broadly speaking, Recommendations 12 to 15 “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 and low risk, and 2) the measures to mitigate that risk.

The LCO is confident Recommendations 12-15 are coherent and sound. The recommendations reflect a combination of current or emerging standards and practices in responsible criminal AI governance in Canada and internationally. That said, these recommendations are inclusive rather than conclusive. The LCO recommends provincial consultations to ensure the best decision-making and to promote public accountability and trust.

Recommendation 12: Prohibited AI Systems

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 specific circumstances, including the EU *AI Act*.

The most important Canadian example of AI prohibitions and “red lines” in policing is the Toronto Police Service Use of AI Policy. This policy identifies a wide range of prohibited “extreme risk technologies” which “may not be considered for adoption,” including:

1. Any application where there is no qualified “human-in-the-loop”.
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 to 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.
7. Where training or transactional data is known or thought to be illegally sourced, or where it is from an unknown source.⁴¹

The authority to legislatively prohibit certain kinds of AI systems is also included Ontario's *EDSTA*⁴²

Recommendation 13: High Risk AI 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.

The TPS Use of AI Policy includes several examples of pre-emptively designated “high risk technologies”, making them subject to higher oversight requirements, 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.
7. Where a system cannot be fully explainable in its behaviour.⁴³

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.⁴⁴

Recommendation 13's 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 of exemptions, emergencies and exigent circumstances under the prohibited and high risk assessment categories. The LCO did not make recommendations on these issues in the Final Report. The LCO believes there is a need to consider these issues further.

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

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 undermining public confidence in the criminal justice system.

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

Recommendation 16: Public Criminal AI Registry

Recommendation 16 would establish a comprehensive public registry of AI systems used in Ontario's criminal justice system. Recommendation 16 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 criminal AI risk assessment tool. Common risk assessment criteria, categories, and mitigation measures would ensure a consistent approach to reliable AI across different 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 would commit the province to establish a dedicated supervisory body for AI systems in criminal justice. The LCO believes a Supervisory Authority could centralize expertise, eliminate duplicate assessments, certify AI technology for provincial use, provide ongoing monitoring, provide independent AI expert witnesses and opinions, and promote public accountability and engagement. 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 address both the shared jurisdiction in these matters between the provincial government, federal government and various Rules committees, and the need for dedicated evidentiary rules at different stages of the criminal justice process.

The LCO and stakeholders agree that AI evidence has the potential to significantly benefit police investigations, reduce expenditures and improve public safety. At the same time, AI tools and evidence also have potentially serious risks. The LCO's analysis addresses two emerging classes of AI evidence: 1) acknowledged AI evidence, and 2) unacknowledged AI evidence, including deepfakes.

Examples of acknowledged AI evidence include:

- AI tools approved for investigative use.
- AI scribes used to transcribe or describe video and audio or 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.

Consultees generally agreed that AI evidence raises the following issues:

- 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.
- In many cases, it appears the “human in the loop” responsible for AI evidence may not have the training, resources or independence to properly assess the system.
- 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.
- Proceedings with lower evidentiary thresholds are less likely to effectively test AI systems. For example, the rapid pace, high pressure and reduced evidentiary threshold in bail hearings means that AI evidence is unlikely to be reviewed appropriately.
- Access to AI experts is challenging.
- Courts may need to consider many different AI tools simultaneously.
- Regulation by litigation is unlikely to be effective.

- Deepfakes are an emerging problem.

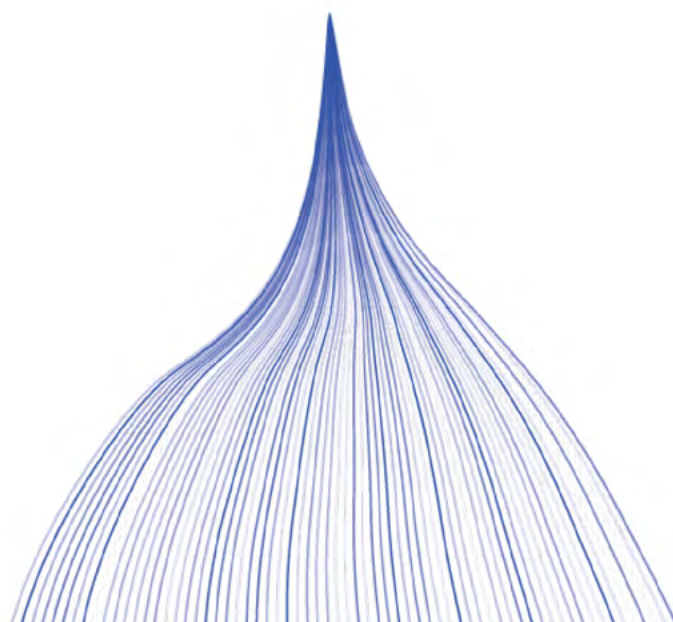
Stakeholders acknowledged that criminal evidence law is flexible and routinely adapted to novel technologies. They believed, however, that existing provisions in the *Canada Evidence Act* and *Ontario Evidence Act* governing electronic or business records were not well-suited for AI evidence.

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.

The LCO and consultees further agreed that the proposed AI evidence rules developed by the Ontario Civil Rules Sub-Committee are an important precedent for equivalent rules in the criminal justice system. These rules would have to be adapted to criminal proceedings.

To address these issues, Recommendations 21-23 set out a series of proposals to establish dedicated committees to study and recommend detailed AI rules in criminal proceedings. Certain key requirements should be the foundation for this work, including a requirement mandating disclosure at different stages of criminal proceedings and consideration of the threshold for evidentiary admissibility, reliability and bias of AI evidence.

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



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.

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.

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. Recommendation 26 would establish an AI Centre of Excellence within LAO.

Recommendation 27 would establish a dedicated LAO external advisory committee with a mandate to meet regularly and advise LAO's board and management on AI issues.

Access to Experts and Forensic Tools

Recommendations 28-29 are transitional recommendations. Pending creation of the proposed criminal AI Supervisory Authority, these recommendations call for much-needed litigation resources to be made available more immediately through the Centre of Forensic Sciences (CFS).

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. 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 deepfake evidence and documents.

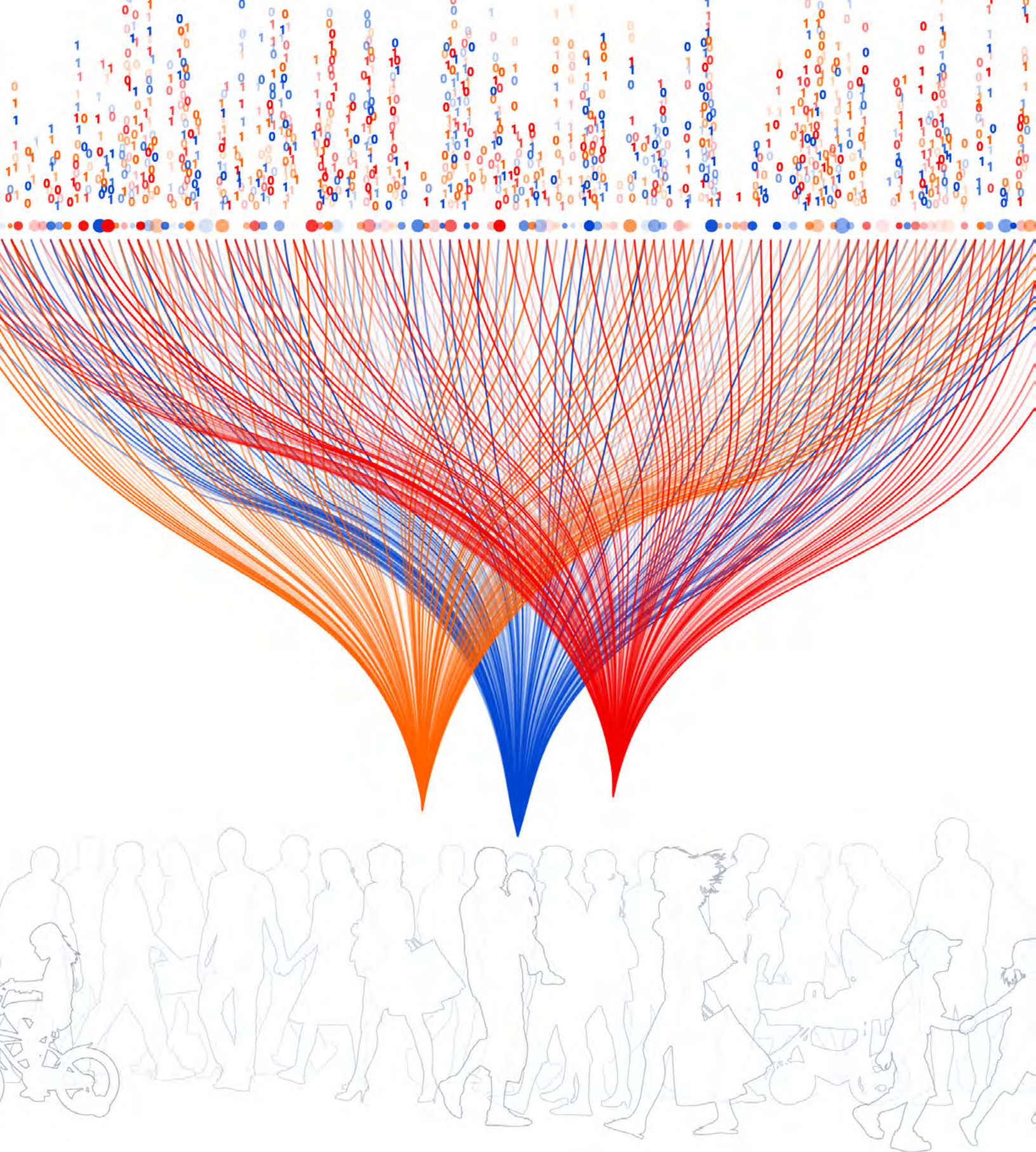


Endnotes

- 1 UK Parliament, “Facial recognition technology in policing” [UK Parliament FRT] (April 8 20260, online: <https://post.parliament.uk/facial-recognition-technology-in-policing/>).
- 2 See generally, DeFlock, an American “open-source project mapping licence plate readers” [DeFlock], online: <https://deflock.org/>. (Accessed September 14, 2026).
- 3 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>.
- 4 See Section 2 of Law Commission of Ontario, *AI in Criminal Justice: Final Report and Recommendations* [LCO Final Criminal AI Report] (2026), online: <https://lco-cdo.org/en/projects/ai-in-criminal-justice/> for a comprehensive discussion of these issues.
- 5 See the text box “How FRT is Used in the UK” in Section 2 of the LCO Final Criminal AI Report for further information.
- 6 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 enforcement and government agencies across the United States as of September 2026. [Atlas of Surveillance] Online: <https://atlasofsurveillance.org/atlas>.
- 7 UBC Police AI Report at 14.
- 8 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/audit-and-complaint-reports>.
- 9 Toronto Police Service, “Automatic Licence Plate Recognition”, online: <https://www.tps.ca/use-technology/automatic-licence-plate-reader/>. (Accessed September 14, 2026),
- 10 See Section 3 of the LCO Final Criminal AI Report for a comprehensive discussion of these issues.
- 11 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.
- 12 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/>.
- 13 International Criminal Police Organization (INTERPOL), *Responsible AI Principles* (2024) [INTERPOL Responsible AI Principles] (2024), online: <https://www.interpol.int/en/How-we-work/Innovation/Artificial-Intelligence-Toolkit> at 13.
- 14 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.
- 15 See Section 4 of the LCO Final Criminal AI Report for a comprehensive discussion of these issues.
- 16 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>.
- 17 EU AI Act, Chapter II, Article 5, s. 1(h).
- 18 EU AI Act, Chapter II, Article 5, s.1(d).
- 19 See: EU AI Act, Chapter III, Annex III.
- 20 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>

- 21 The LCO can provide a compendium upon request.
- 22 Airsight, “Drone Laws”, online: <https://www.airsight.com/learn/airspace-security/drone-laws-rules-and-regulations>. (Accessed August 2026.)
- 23 DeFlock, “City Council.”
- 24 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/m1l1txEuS38>.
- 25 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>.
- 26 Big Brother Watch, “Stop Facial Recognition”, online: <https://bigbrotherwatch.org.uk/campaigns/stop-facial-recognition/>. (Accessed September 14, 2026.)
- 27 United Kingdom, Prime Minister’s Office, *The King’s Speech 2026: Background Briefing Notes* (13 May 2026) at 68–69.
- 28 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>.
- 29 *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>.
- 30 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>.
- 31 *Safe Social Media Act*, Bill C-34, 1st Sess, 45th Parl, 2026 (first reading 10 June 2026).
- 32 *Protecting Privacy and Consumer Data Act*, Bill C-36, 1st Sess, 45th Parl, 2026 (first reading 15 June 2026).
- 33 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>.
- 34 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>.
- 35 *Enhancing Digital Security and Trust Act*, S.O. 2024, c. 24, [EDSTA], online: <https://www.ontario.ca/laws/statute/24e24>.
- 36 Government of Ontario, Consultation on proposed legislation: Strengthening Cyber Security and Building Trust in the Public Sector Act, 2024 (2024).
- 37 EDSTA at ss. 5(1-6), 6(2), 7, 8.
- 38 Government of Ontario, Ministry of Public and Business Service Delivery and Procurement, *Responsible Use of AI Directive*, December 1, 2024 [Ontario AI Directive].
- 39 Toronto Police Service, “Use of Artificial Intelligence Technology” (introduced February 28 2022, updated January 11 2024), online: <https://tps.ca/home/about/policies-by-laws/board-policies/use-of-artificial-intelligence-technology/> [TPS Use of AI Policy].
- 40 TPS Use of AI Policy.
- 41 TPS Use of AI Policy.
- 42 EDSTA s. 5(6).
- 43 TPS Use of AI Policy.
- 44 EU AI Act, Chapter III, Annex III.



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