

Law Commission of Ontario

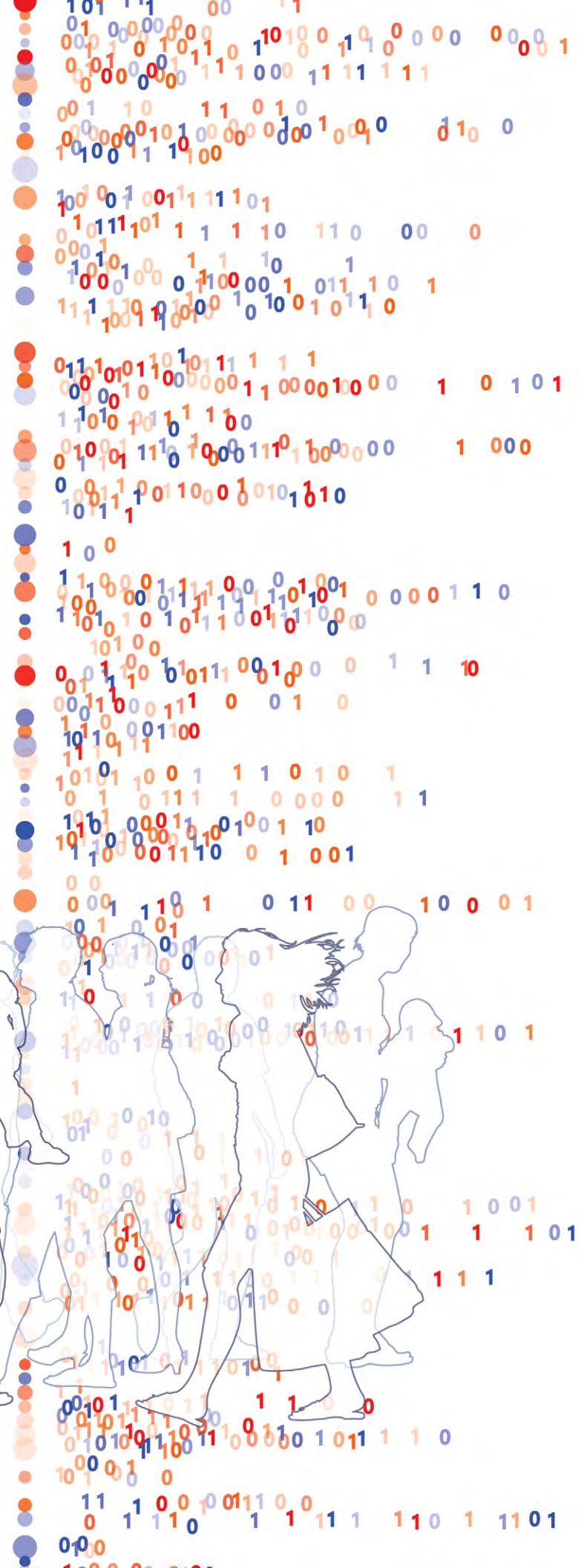
**AI IN CRIMINAL JUSTICE PROJECT | ANNEX A**

# Executive Summary and Consultation Questions

April 2025



LAW COMMISSION OF ONTARIO  
COMMISSION DU DROIT DE L'ONTARIO



---

## About The Law Commission of Ontario

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

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

Recent LCO reports and submissions addressing AI issues include:

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

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

## Contact

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

Tel: (416) 650-8406

E-mail: [LawCommission@lco-cdo.org](mailto: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)

Twitter: [@LCO\\_CDO](https://twitter.com/LCO_CDO)

YouTube: [@lawcommissionofontario8724](https://www.youtube.com/channel/UC8724lawcommissionofontario)

## Funders

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



## The LCO AI in Criminal Justice Project

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

Project materials are available online:

<https://www.lco-cdo.org/CrimAI>.

## Series Editors

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

## Student Researchers

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

## External Advisory Committee

**Alpha Chan**, Chief Information Security Officer,  
Toronto Police Services

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

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

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

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

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

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

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

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

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

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

**Michael Swinburne**, Senior Policy Advisor, Canadian  
Human Rights Commission

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

## Disclaimer

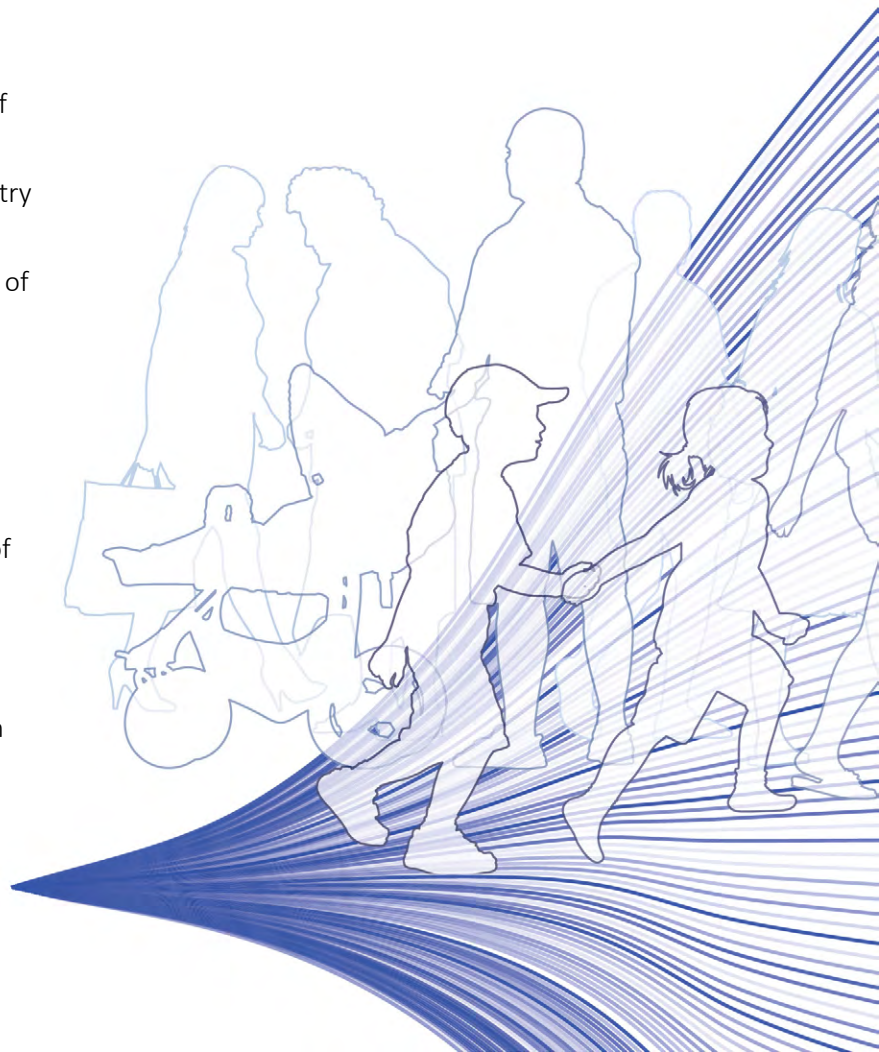
The analysis, findings, and recommendations in this paper do not necessarily represent the views of the LCO's funders, supporters, Advisory Committee members, or Issue Paper authors.

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

## Citation

Law Commission of Ontario, *Executive Summary and Consultation Questions, AI in Criminal Justice Project* (April 2025).

Layout and Design by [12thirteen](#).





# Contents

<b>1. The LCO AI in Criminal Justice Project.....</b>	<b>6</b>
<b>2. About the LCO.....</b>	<b>8</b>
<b>3. AI in Criminal Justice: Uses and Benefits.....</b>	<b>9</b>
<b>4. AI in Criminal Justice: Risks and Issues .....</b>	<b>11</b>
<b>5. AI Benefits and Risks in Context .....</b>	<b>13</b>
<b>6. Overview of Criminal AI Project Issue Papers .....</b>	<b>14</b>
<b>7. Trustworthy Criminal AI .....</b>	<b>16</b>
<b>8. Trustworthy AI in Canadian Criminal Justice .....</b>	<b>17</b>
Existing Laws and Policies.....	17
Federal AI Legislation, Government Directives and Policies .....	18
AI Legislation, Government Directives, and Policies in Ontario.....	19
Guidance From Canadian Privacy Commissioners and Courts .....	21
<b>9. Conclusion .....</b>	<b>22</b>
<b>10. Next Steps and Contacts.....</b>	<b>24</b>
<b>Appendix A – Consolidated Consultation Questions.....</b>	<b>25</b>
1. Provincial Standards.....	25
2. Prohibited Uses and Risk Criteria.....	25
3. Bias, Privacy and Procedural Fairness.....	26
4. Disclosure .....	26
5. Impact Assessments.....	26
6. Bail and Sentencing Risk Assessments .....	27
7. AI Litigation .....	27
8. Public Engagement .....	28
9. Access to Justice.....	28
10. Institutional Capacity .....	28
11. Systemic Oversight.....	28
<b>Endnotes .....</b>	<b>29</b>



# 1. The LCO AI in Criminal Justice Project

The Law Commission of Ontario’s (LCO) [AI in Criminal Justice Project](#) is a groundbreaking survey and analysis of artificial intelligence (AI) in the Canadian criminal justice system.

This project is a unique collaboration of leading practitioners and experts from across Canada. Authors and advisors include representatives from governments, police services, Crowns, defence counsel, courts, legal aid, human rights commissions, civil society organizations and academics.

The project includes an Introduction and four project Issue Papers. Each Issue Paper considers the use of AI in a distinct phase of the criminal justice process, including:

- Use of AI by Law Enforcement.
- AI and the Assessment of Risk in Bail, Sentencing, and Recidivism.
- AI at Trial and on Appeal.
- AI and Systemic Oversight Mechanisms.

The project is organized around four key themes or topics:

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

- What AI tools are being used and could be used at each stage of Canadian criminal justice?
- What are the benefits and risks of these technologies?
- What legal issues are likely to arise at each stage, particularly in relation to the *Charter of Rights and Freedoms*, procedural fairness, evidence law, and criminal common law?
- What is the state of Canadian law and procedures to address these issues, and what proactive steps might be identified and taken to align practices and standards systemically?

Second, the project asks who is likely to be affected by AI in the criminal justice system.

Third, the project surveys and analyzes recent international and Canadian “trustworthy criminal AI” initiatives.

Finally, the project tries to foreshadow or predict what could happen if action is not taken.

The LCO's Criminal AI Issue Papers are designed to facilitate discussion and consultation. We have learned that "trustworthy criminal AI" depends on complex legal, technical and operational considerations. We have also learned that broad collaborations and consultations are crucial. Accordingly, each Issue Paper includes questions for Canadian criminal AI policymakers and stakeholders. These questions are summarized in [Appendix A](#) to this Executive Summary. In this manner, the LCO hopes the papers will become a catalyst for a wider Canadian discussion about these important and timely issues.

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

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



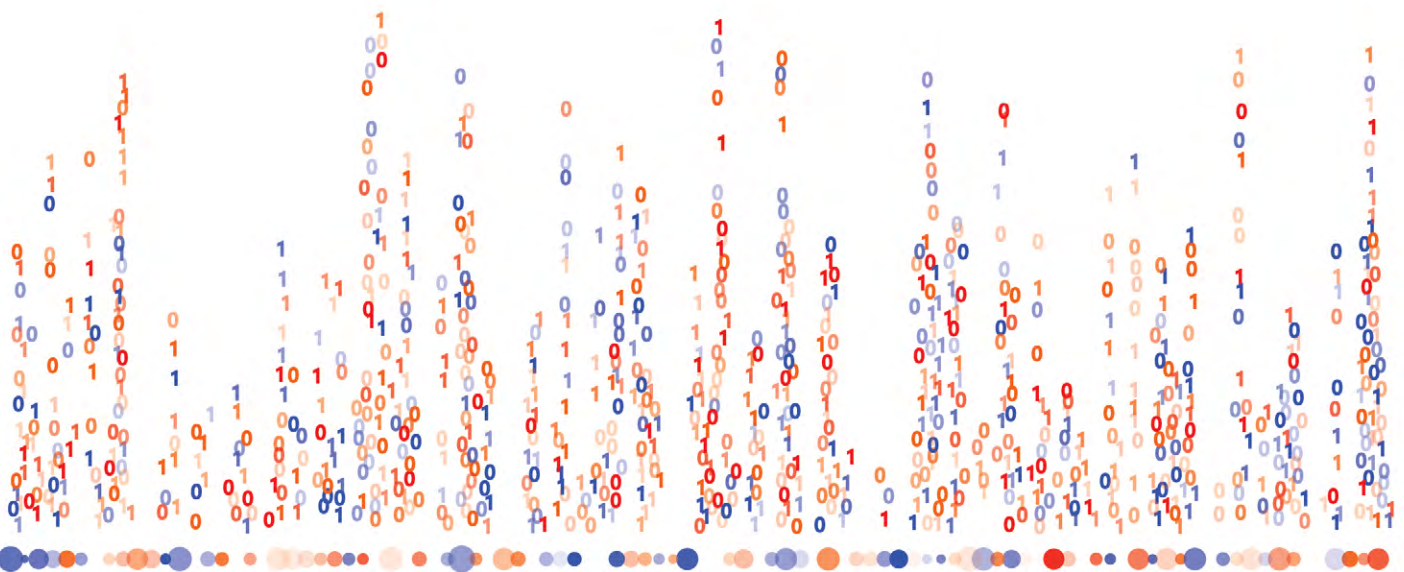


## 2. About the LCO

The Law Commission of Ontario is Ontario's leading law reform agency. The LCO provides independent, balanced, and authoritative advice on complex and important legal policy issues. 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. More information about the LCO is available [here](#).

This project is one of several LCO projects addressing AI issues in the Canadian justice system. Previous projects and reports include:

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





## 3. AI in Criminal Justice: Uses and Benefits

Across the world, the criminal justice system has been at the forefront of the adoption of AI. Criminal jurisdictions outside of Canada employ AI to improve police investigations, analyze evidence, assist judicial decision-making, improve data analysis and target resources. AI technologies used in criminal justice today include predictive policing, facial recognition and biometric surveillance, social media analysis, licence plate readers, bail and sentencing algorithms and many other applications. Many of these systems have reportedly been used in Canada as well. Notable criminal justice AI systems include:

### 1. Predictive Analytics/Predictive Policing<sup>1</sup>

Predictive policing is a generic name for AI technology that processes and analyses large and complex datasets much more quickly than humans. Professor Andrew Ferguson, a leading US scholar on predictive policing, writes of the promise of

*...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.<sup>2</sup>*

Predictive policing is commonly understood as AI systems that try to forecast future crime, including:<sup>3</sup>

- Location-based systems that predict where and when criminal activity might occur.
- Person-based systems that predict who is likely to be involved in future criminal activity.

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.<sup>4</sup> 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).<sup>5</sup>

## 2. Facial Recognition and Biometrics<sup>6</sup>

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.<sup>7</sup>*

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

Many police services believe FRT and other biometric technologies have significant potential to improve public safety, police investigations and efficiency. For example, INTERPOL has stated that

*...computer vision and biometrics have emerged as game-changers for law enforcement...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.<sup>8</sup>*

FRT and biometric systems can be used for many purposes and in many contexts, including:

- To support criminal investigations, including terrorist threats; investigations for missing persons children, human trafficking or sexual exploitation; public order events; etc.
- To scan mugshot databases.
- To provide surveillance in public, private or secure spaces.
- For real-time personal identification through police body cams or drone videos.
- To analyze images or video collected by third parties.<sup>9</sup>

FRT is widely deployed by law enforcement agencies in the United States and internationally.<sup>10</sup> The best-known FRT system in Canada is the RCMP's since-discontinued use of Clearview AI, an Internet image-scraping program.<sup>11</sup> The Toronto Police Services also uses FRT in limited circumstances.<sup>12</sup>

## 3. Bail and Sentencing Algorithms<sup>13</sup>

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, where they quickly emerged as the “favored reform” to advance the American “bail reform” movement.<sup>14</sup> According to the Center on Court Innovation, a New York-based non-profit research organization, “[t]he appeal of pretrial risk assessment—especially in large, overburdened court systems—is of a fast and objective evaluation, harnessing the power of data to aid decision-making.”<sup>15</sup>

## 4. Other AI Systems Used in Criminal Justice<sup>16</sup>

Other AI-enabled technologies discussed in the Criminal AI Issue Papers include:

- Automatic licence plate readers.
- Drones.
- Gunshot detection systems.
- Open-source intelligence (OSINT) and social media intelligence (SOCINT) systems.
- AI-generated evidence.



## 4. AI in Criminal Justice: Risks and Issues

Many reports document how AI systems such as biometric surveillance, predictive policing, and bail and sentencing algorithms are risks to human rights, civil liberties, privacy protections and procedural fairness. These reports also discuss how the risks of these systems fall disproportionately on low-income, Indigenous, racialized or otherwise vulnerable communities and individuals. Notable AI risks in the criminal justice system include:

### 1. Bias and Discrimination

Data bias and discrimination issues in criminal justice AI systems are well-known and widely-acknowledged.<sup>17</sup> For example, studies of FRT systems “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.”<sup>18</sup> Many predictive policing and bail/sentencing algorithms have also been shown to be biased and discriminatory.<sup>19</sup>

Concerns about bias have led to many proposals to strictly regulate criminal justice AI systems.<sup>20</sup>

### 2. Privacy and Surveillance

Privacy and surveillance risks are widely acknowledged in criminal AI systems, particularly FRT systems.<sup>21</sup> Privacy risks in other criminal justice AI systems can include:

- Social media monitoring systems that can reduce privacy in online communications.
- Automatic licence plate readers that can track an individual’s movements.
- Drones that surveil individuals or events or are used to collect information about bystanders who are not connected to a law enforcement investigation.<sup>22</sup>

As with FRT, privacy risks have also led to many proposals to regulate or ban criminal AI applications.<sup>23</sup>

### 3. Disclosure and Transparency

Criminal AI systems are frequently criticized for their lack of disclosure and transparency, including<sup>24</sup>

- Lack of disclosure about the existence of an AI system generally or to the individual affected.
- Lack of disclosure of key elements of an AI system, such as its training data.
- Lack of disclosure about how an AI system makes decisions.

The RCMP's use of Clearview AI is the best-known Canadian AI disclosure controversy.<sup>25</sup>

### 4. Opacity/Lack of Explainability

Criminal 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.”<sup>26</sup> As a result, even simple algorithmic systems can become “black boxes.”

### 5. Data Accuracy, Reliability, and Validity

FRT, predictive policing and other criminal justice AI systems have been subject to strident criticisms about the accuracy, reliability and validity of their training data.<sup>27</sup>

### 6. Effective Oversight

Criminal AI systems raise several oversight risks, including:

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

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

### 7. Miscarriages of Justice/Access to Justice

Any of the risks above could lead to miscarriages of justice for individual accused, including risks of false arrest; false imprisonment; and risks to *Charter* rights, privacy, and procedural fairness.

Criminal AI systems also raise systemic access to justice concerns, including how criminal accused (particularly accused represented by legal aid or who are self-represented) will be able to effectively challenge AI systems.





## 5. AI Benefits and Risks in Context

When assessing criminal AI benefits and risks, it is important to account for the variations within and between criminal AI systems. These variations can have wide ranging implications for public safety, police investigations, and individual rights. 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. There are also many variations within and between predictive policing systems.<sup>28</sup>

It is also important to note that criminal AI technologies are not static. For example, a recent U.S. National Academy of Sciences report notes that predictive policing is evolving and that many of the early predictive policing systems “have come and gone” in the face of significant criticisms.<sup>29</sup>





## 6. Overview of Criminal AI Project Issue Papers

The LCO Criminal AI Project includes an Introduction and four specific Issue Papers. Each Issue Paper considers the use of AI in a distinct phase of the criminal justice process.

All project Issue Papers are available on the LCO project [website](#).

### **Paper 1: Introduction to the LCO Criminal AI Project**

The first paper is an introduction and summary to the LCO Criminal AI project. This paper was written by LCO Executive Director, Nye Thomas.

This paper identifies AI systems currently used in criminal justice and summarizes their respective benefits and risks. The paper also summarizes criminal AI governance initiatives internationally and in Canada. The paper concludes with an assessment of “trustworthy criminal AI” in Canada and Ontario.

### **Paper 2: Use of AI by Law Enforcement**

The second LCO Criminal AI Project paper considers the use of AI by law enforcement. This paper was written by LCO Counsel, Ryan Fritsch.

This paper discusses the broad range of AI-enabled technologies used by law enforcement internationally and within Canada, including FRT, predictive policing, object recognition, AI generated evidence and others. The paper considers the potential benefits and risks of these systems and how they raise novel legal, societal and constitutional issues.

The paper also considers the how AI could influence the Crown’s assessment of charges and the advice function between Crowns and law enforcement, including questions about AI admissibility, disclosure requirements and privacy issues.

### Paper 3: AI and the Assessment of Risk in Bail, Sentencing, and Recidivism

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

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

The paper also considers the unique nature of bail hearings, which tend to be quicker and informal, and sentencing and post-sentencing hearings, in which the presumption of innocence is no longer operative.

### Paper 4: AI at Trial and on Appeal

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

AI raises novel issues that are fundamental to ensure fair trial process and protection of liberty and constitutional rights. Trials and appeals ensure a fair and transparent proceeding by relying on the *Charter of Rights and Freedoms*; common law principles guiding case interpretation and procedural fairness; and evidence law. The introduction of AI—both as evidence and in analytical tools employed by litigants and officers of the court—raises new concerns about disclosure, admissibility, bias and access to justice that are not directly addressed by existing legislation and case law.

### Paper 5: AI and Systemic Oversight Mechanisms

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

Without robust legal, regulatory, and policy frameworks, the criminal law process is limited in its ability to oversee the use of AI by state actors and mitigate potential abuses. While federal Bill C-27 and Ontario’s *EDSTA* contain some important regulatory measures, their application to criminal law is limited. Key issues include the lack of access to remedies for rights breaches, the lack of independent oversight bodies, and the relatively narrow understanding of privacy rights reflected in current legislation and case law. New and proposed legislation from jurisdictions such as the EU and the US may offer guidance; however, these approaches also have gaps. This paper also explores how AI is sure to test rights to a full defence and access to justice, including adequate time and funding to defense counsel to challenge the use of AI in bail or sentencing, or the admission of AI evidence at trial.





## 7. Trustworthy Criminal AI

The potential benefits, risks, and harms of AI in criminal justice are widely acknowledged by governments, police services, prosecutors, defence counsel, academics and NGOs around the world.<sup>30</sup> This acknowledgement has led to a wide range of laws, policies and frameworks based on the principle that AI benefits depend on dedicated and sophisticated rules minimizing risks and harms.

There is a broad range and diversity of trustworthy criminal AI initiatives in Europe and the United States. For example, the European Union’s *Artificial Intelligence Act* (EU AI Act) includes prohibitions on several criminal AI systems, including real time biometric surveillance and certain predictive policing systems.<sup>31</sup> The EU AI Act also identifies several AI tools in “law enforcement” and the “administration of justice” as being presumptively high-risk and thus subject to more detailed regulatory requirements.<sup>32</sup> In the United States, detailed criminal justice AI legislation, executive orders, policies, and rules have been adopted or proposed by the federal government, states, municipalities, police services and NGOs.<sup>33</sup>

The overarching theme of these initiatives is that consistent and comprehensive rules are needed to ensure criminal AI systems are beneficial, legal and accountable. That said, the substance and form of these initiatives varies significantly and can include:

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

The LCO does not believe any single precedent or framework can or should be adopted in Canada or Ontario. Trustworthy criminal AI laws and policies must be tailored to our laws, criminal justice system and institutions. The LCO believes Canadian policymakers and stakeholders can learn important lessons from the experience of other jurisdictions.



## 8. Trustworthy AI in Canadian Criminal Justice

### Existing Laws and Policies

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

The LCO and our authors have concluded that, while existing legal rules and procedures have many strengths, they do not establish trustworthy criminal AI in Canada. This is because:

- AI raises novel, complex and consequential issues at each stage of a criminal proceeding.
- Improperly designed or operated AI systems could have profound implications for liberty interests, constitutional rights, privacy, criminal procedure, court efficiency, access to justice and public trust in the Canadian criminal justice system.

- There is a need for AI accountability at each stage of the criminal justice system.
- “Regulation by litigation” is unlikely to effectively address the systemic and complex challenges of criminal AI systems.
- It is not clear that agencies and courts will be able to determine or apply consistent AI disclosure obligations, bias and privacy testing, reliability criteria, etc.

The LCO and our authors are concerned these issues will spread and compound across the wide, diverse, and decentralized network of institutions and actors involved in developing, operating, litigating or overseeing AI in Canada's and Ontario's criminal justice system.

## Federal AI Legislation, Government Directives and Policies

There are three initiatives at the federal level relevant to criminal AI systems.

### 1. The Federal Artificial Intelligence and Data Act (AIDA)

In June 2022, the federal Minister of Industry, Science and Economic Development (ISED) introduced the draft *Artificial Intelligence and Data Act* (AIDA) as part of Bill C-27.<sup>34</sup>

Like the EU *AI Act*, *AIDA* proposed a risk-based approach to AI governance. Unlike the EU *AI Act*, however, *AIDA* did not directly regulate the use of AI in the public sector or criminal justice system. Rather, *AIDA* would have applied to private sector organizations responsible for the “development, deployment, use or making available of AI systems.”<sup>35</sup> Nor did *AIDA* originally include explicit bans or prohibitions on AI systems that have unacceptable risks.

Upon introduction, *AIDA* was heavily criticized for its lack of detail, consultations and important trustworthy AI protections.<sup>36</sup> The federal government responded, in part, by proposing several amendments, including a proposed list of “classes of systems that would be considered high impact”, including three relevant to criminal justice (some biometric systems, AI systems used by courts, and AI systems “to assist a peace officer...”).<sup>37</sup> The federal government’s proposed amendments did not assuage *AIDA*’s critics, who continued to criticize the legislation.<sup>38</sup>

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

### 2. The Federal Automated Decision-making Directive

In 2021, the federal government enacted the Automated Decision-making Directive (federal ADM Directive) and its companion Algorithmic Impact Assessment (AIA). The federal ADM Directive and AIA apply to a broad range of federal technology systems, not just AI systems.<sup>39</sup>

The LCO has written at length about federal ADM Directive and AIA.<sup>40</sup> We have praised both as leading examples of tools and strategies that incorporate procedural fairness protections into the design and operation of automated government decision-making.<sup>41</sup> The Federal ADM Directive and AIA do not apply to federal law enforcement agencies.<sup>42</sup>

The federal government is currently undertaking its fourth review of the federal ADM Directive and AIA.<sup>43</sup> This review could include proposals to strengthen the federal ADM Directive’s human rights provisions and more explicit criteria addressing prohibited or banned federal AI systems. This revision will not apply the federal ADM Directive and AIA to federal law enforcement agencies.

### 3. RCMP

In response to the Office of the Privacy Commissioner’s special report on the RCMP’s use of Clearview AI, the RCMP created the National Technologies Onboarding Program (NTOP).<sup>44</sup> NTOP is an internal program to evaluate RCMP technology systems. The RCMP says AI and privacy intrusive technologies are NTOP’s highest priorities.<sup>45</sup>

The NTOP’s first transparency report, *Transparency Blueprint: Snapshot of Operational Technologies*, was released in September 2024.<sup>46</sup> The *Transparency Blueprint* outlines how the RCMP is implementing a more proactive approach to technology assessment and transparency, including AI systems. The RCMP states NTOP had evaluated 28 technologies as of September 2024.<sup>47</sup>

## 4. Assessing Federal Initiatives to Promote Trustworthy Criminal AI

Had it passed, a revised *AIDA* would have included limited provisions to promote trustworthy AI in Canada. The addition of prescribed “high impact” AI systems in biometrics, courts and policing would have been helpful additions to the legislation. Other positive aspects of *AIDA* included publication and plain language notice requirements, mandatory bias and mitigation requirements, and notable penalties for non-compliance. Nevertheless, an amended *AIDA* would still not have established trustworthy criminal AI in federal law enforcement or the criminal justice system.

The federal ADM Directive and AIA remain leading examples of how to ensure procedure fairness in public sector AI systems. The current review of the federal ADM Directive and AIA could make these instruments even stronger. These proposals, while welcome, would still not apply the federal ADM Directive and AIA to federal law enforcement agencies.

The federal government’s inaction in this area is disappointing. It has been approximately five years since the enactment of the first federal ADM Directive, yet there is still no dedicated federal legislation, directive, or policy establishing trustworthy criminal AI for federal criminal justice institutions or actors, include federal law enforcement agencies. The lack of federal action contrasts unfavourably with the EU and US, both of which have taken important steps to address the unique and serious risks of criminal AI.

The RCMP’s NTOP program and recent *Transparency Blueprint* are sophisticated initiatives that incorporate many of the trustworthy criminal AI principles. However, neither NTOP nor the *Transparency Blueprint* appear to include detailed information on prohibited uses, risk categories or mitigation requirements. The LCO hopes these issues will be addressed in future RCMP policies.

## AI Legislation, Government Directives, and Policies in Ontario

There are three initiatives in Ontario relevant to criminal AI systems.

### 1. *Enhancing Digital Security and Trust Act, 2024*

The Government of Ontario passed the *Enhancing Digital Security and Trust Act, 2024 (EDSTA)* in November 2024.<sup>48</sup> 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.”<sup>49</sup>

The LCO has written at length about *EDSTA* and Bill 194, the Bill that introduced the legislation.<sup>50</sup> We have concluded the legislation fails to establish a comprehensive trustworthy AI for public sector AI systems in Ontario due to its lack of protections for human rights, disclosure requirements, risk categories, and other provisions. *EDSTA* does not apply to AI used in Ontario’s criminal justice system.<sup>51</sup>

### 2. 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.<sup>52</sup> 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’s early analysis is that the Ontario AI Directive has several significant gaps or uncertainties.<sup>53</sup> 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.

### 3. Toronto Police Service Board “Use of AI Technology Policy”

The most significant criminal AI policy in Canada is the Toronto Police Services Board’s (TPSB) “Use of AI Technology Policy” (“TPS AI Policy”).<sup>54</sup>

The TPS AI Policy incorporates many trustworthy criminal AI principles. For example, the TPS AI Policy:

- Acknowledges 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].”<sup>55</sup>
- Requires technology to adhere to detailed guiding principles, including legality, fairness, reliability, justifiability, personal and organizational accountability, transparency, privacy and meaningful engagement.<sup>56</sup>
- Includes explicit risk criteria, including “Extreme Risk Technologies” which may not be considered for adoption, including AI systems that result in “mass surveillance defined as monitoring of a population or a significant component of a population...” and “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.”<sup>57</sup>
- Includes obligations regarding purpose limitations, data requirements, disclosure requirements, approval and reporting procedures, impact assessments, and public engagement strategies.

The TPS issued its first public disclosure report in January 2024. This report disclosed that the TPS uses five AI-enabled systems. The TPS also self-assessed the risk level of each system. An FRT system that automates mugshot identification was the only system classified as “high-risk”.<sup>58</sup>

At least one other police service in Ontario has adopted an AI policy. In October 2024, the Durham Regional Police Services Board adopted a “Use of Artificial Intelligence” Policy.<sup>59</sup> This policy includes several trustworthy criminal AI principles but is less detailed and prescriptive than the TPS AI Policy. For example, the Durham policy does not include risk categories or prohibited “Extreme Risk Technologies.”

### 4. Assessing Provincial Initiatives to Promote Trustworthy Criminal AI

The provincial government has taken important first steps to promote trustworthy AI across Ontario’s public sector. To date, this commitment has not extended to AI systems used in provincial law enforcement or the provincial criminal justice system. As a result, there is no dedicated legislation, directive or policy establishing trustworthy AI in Ontario criminal justice system.

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

The Ontario AI Directive is more comprehensive than *EDSTA*, but there are many outstanding questions. Critically, the Ontario AI Directive does not apply to any police service in Ontario.

The most significant trustworthy criminal AI policy in Ontario is the TPS AI Policy. The TPS AI Policy is a sophisticated document that incorporates many criminal trustworthy AI principles identified by the LCO and other jurisdictions. That said, the TPS AI Policy has structural limitations as a trustworthy criminal AI governance instrument:

First, the TPS AI Policy is not legally binding. It does not create a legal accountability regime, remedial provisions or penalty provisions for non-compliance.

Second, the TPS AI Policy is self-regulating. It does not create an independent oversight body or external review mechanism. As a result, the TPS has been criticized for interpreting the TPS AI Policy loosely.<sup>60</sup>

Third, and most importantly, the TPS AI Policy is an administrative policy governing a single police service in Ontario. It does not establish a provincial AI standard for either policing generally or any other part of Ontario’s criminal justice system.

From a provincial perspective, the TPS AI Policy demonstrates the difficulty and risks of relying on individual police services and boards to regulate policing AI systems: There are 53 police services in Ontario. To date, it appears only two services have adopted dedicated AI policies. This means that 51 police services in Ontario *are not* subject to AI prohibitions, risk criteria, disclosure and consultation requirements, etc. As a result, one or more of the 51 remaining police services in Ontario could adopt “Extreme Risk” AI systems (such as real time FRT or predictive policing) without effective guardrails, accountability requirements or public disclosure. This is a worst-case scenario, but not an impossible one.

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

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

## Guidance From Canadian Privacy Commissioners and Courts

A final source of trustworthy criminal AI policies are Canadian Privacy Commissioners and courts.

Canadian Privacy Commissioners have taken a prominent and important leadership role in promoting trustworthy criminal AI in Canada. To date, Privacy Commissioners in Canada have completed at least five studies or reports of FRT in Canadian policing.<sup>61</sup> These reports offer detailed guidance on how police services can use AI systems while respecting privacy rights. The LCO expects Canadian Privacy Commissioners will continue to address criminal justice AI issues in the future.

In addition to the Privacy Commissioners, several Canadian courts have adopted AI policies. For example, the Federal Court has adopted policies to guide the use of AI by the court and to direct the use of AI by parties and professionals appearing before the court.<sup>62</sup> Courts in Alberta, Manitoba, and Quebec have adopted similar policies.<sup>63</sup> Finally, the Canadian Judicial Council has produced a thoughtful set of *Guidelines for the Use of Artificial Intelligence in Canadian Courts*.<sup>64</sup> These guidelines emphasize the need to maintain and respect judicial independence if and when courts implement AI systems.

Guidance from Privacy Commissioners and courts are important efforts to establish trustworthy AI principles in their respective domains. They do not, however, establish comprehensive accountability for criminal AI systems either nationally or provincially.



## 9. Conclusion

There have been many positive developments in AI governance at the federal and provincial level in Canada. To their credit, several Canadian police services, Privacy Commissioners and others have taken important initiatives to address criminal AI risks. Unfortunately, there are still wide and consequential gaps in the legislative or legal framework governing criminal AI systems, including:

- **Lack of mandatory and consistent disclosure requirements.** At present, the overwhelming majority of police services in Ontario could implement predictive policing, FRT or other forms of AI without having to disclose those systems publicly.
- **Lack of criminal AI prohibitions, “guardrails” or consistent risk criteria.** In Ontario, there are no legal “guardrails” prohibiting or regulating the highest risks criminal AI systems, such as real time mass surveillance and predictive policing. Nor are there transparent and consistent risk categories to consistently identify criminal AI risks and mitigation strategies.
- **Lack of mandatory impact assessments.** There is no provincial obligation for any actor in the criminal justice system to assess the impact of an AI system on *Charter* rights, human rights, privacy or procedural justice.
- **Lack of criminal procedural protections.** In Canada (and by extension, Ontario), there are no explicit procedural protections governing police or court use of high-risk criminal AI systems, such as warrant requirements for high-risk AI systems. There are also no policies or programs to ensure the right to a full defence, effective legal representation or access to justice.
- **Lack of mandatory obligation to test, audit or evaluate criminal AI systems.** An AI system could be implemented in Ontario’s criminal justice system without a duty to audit or evaluate its accuracy, bias, validity, reliability, admissibility or effectiveness.
- **Lack of obligation to undertake public consultations.** But for the Toronto Police Service, there is no obligation in Ontario to consult publicly on AI systems used in criminal justice.

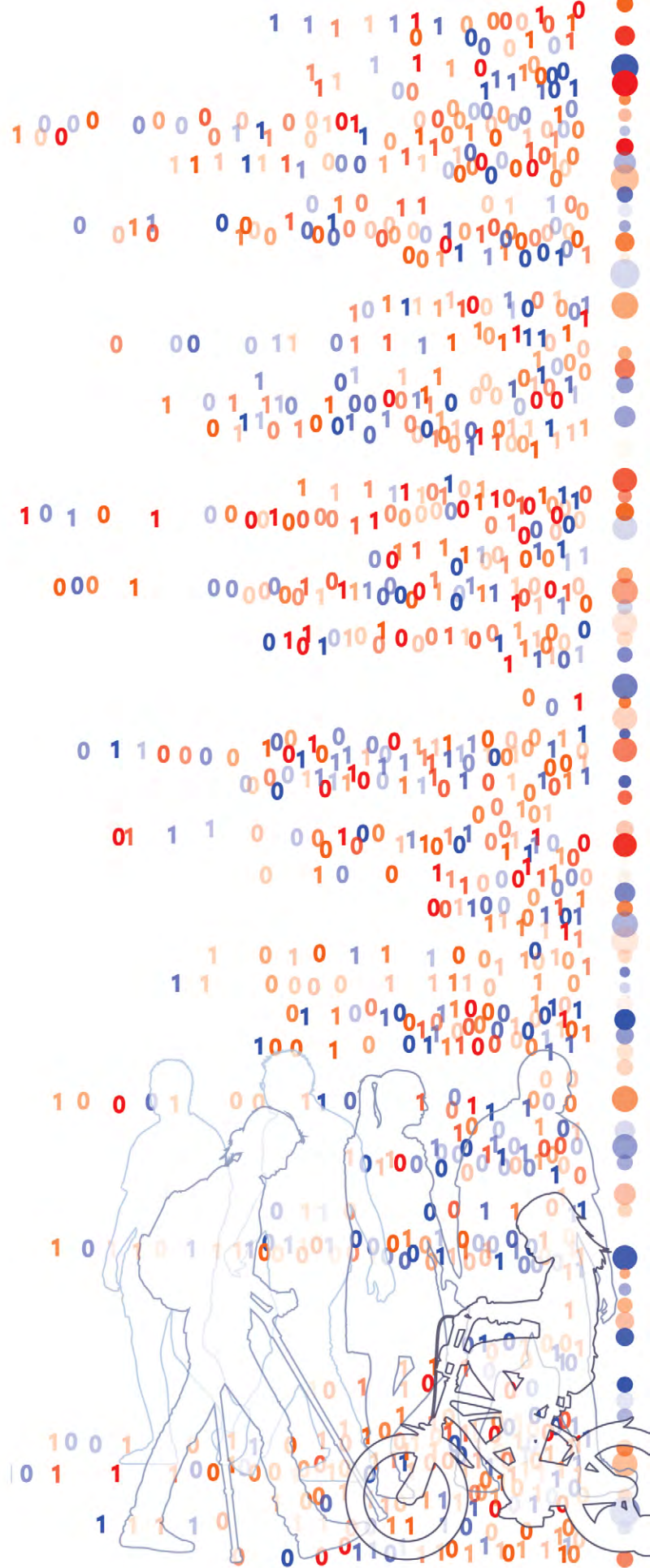
The LCO acknowledges that these are comparatively early days for criminal AI regulation in Ontario and across Canada. The federal Directive and AIA, *EDSTA*, the Ontario AI Directive, and TPS AI Policies were all adopted within the last few years. That said, Canadian and provincial policymakers are far behind their international counterparts in establishing governance tools to address this fast moving technology.

It is not too early to ask what could happen if governments do not regulate criminal justice AI systems. This is not a hypothetical question. Criminal AI systems have been used in other jurisdictions for several years. Policymakers thus have a detailed record of well-documented and widely publicized risks and harms, including:

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

Absent proactive steps, these risks and consequences are both foreseeable and significant.

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





## 10. Next Steps and Contacts

One of the important lessons of this project is that whether AI in criminal justice is harmful or beneficial depends on a complex, interdependent series of technical, operational, policy and legal choices. A second important lesson is that broad collaborations and consultations are crucial. Given the issues at stake, no one organization or stakeholder can or should act unilaterally.

The LCO is confident that provincial policymakers and stakeholders are committed to addressing these issues thoughtfully and collaboratively. To this end, the LCO will be organizing project consultations over the next several months.

Individuals or organizations interested in collaborating with the LCO are encouraged to contact Ryan Fritsch, the LCO's Criminal AI Project Lead, at [rfritsch@lco-cdo.org](mailto:rfritsch@lco-cdo.org).

Details of our consultation plans, Criminal AI Issue Papers and additional information is available on the LCO AI in Criminal Justice [website](#).

The LCO can also be contacted at:

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

Tel: (416) 650-8406

E-mail: [LawCommission@lco-cdo.org](mailto:LawCommission@lco-cdo.org)

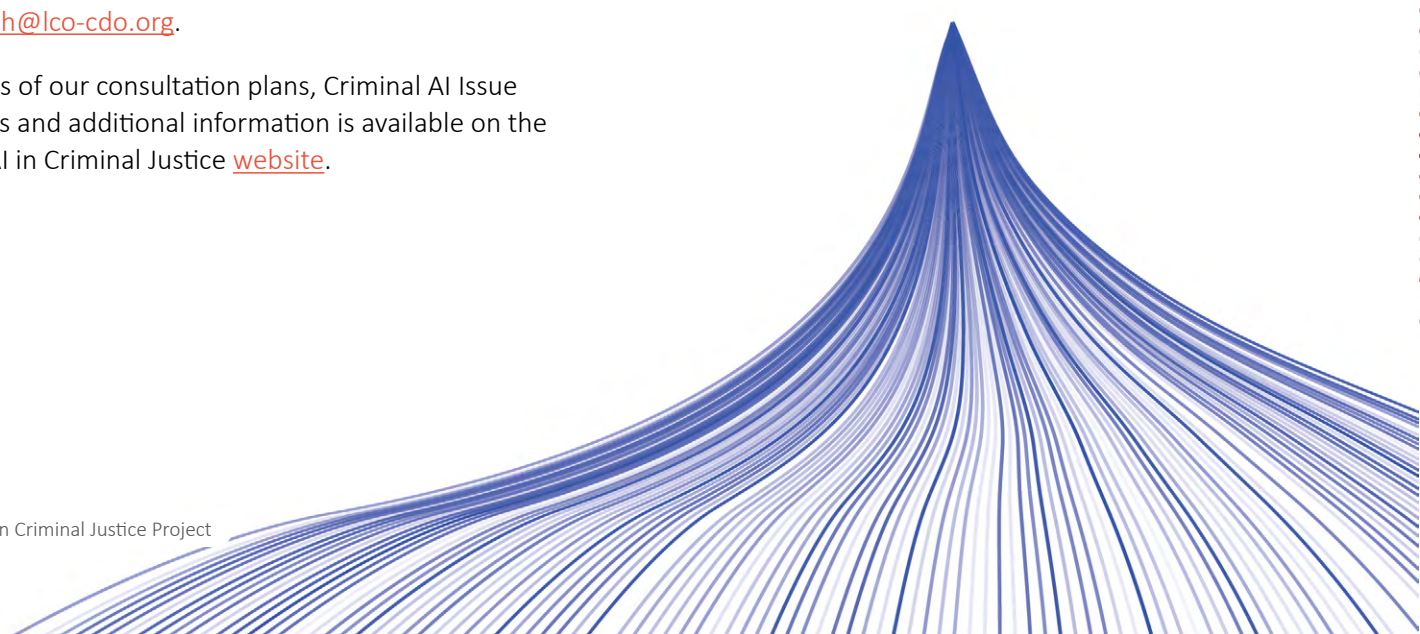
Web: <https://www.lco-cdo.org>

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

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

Twitter: [@LCO\\_CDO](https://twitter.com/LCO_CDO)

YouTube: [@lawcommissionofontario8724](https://www.youtube.com/channel/UC8724lawcommissionofontario)



## Appendix A

# Consolidated Consultation Questions

The questions below reflect key themes and issues in the LCO Criminal AI Issue Papers. The questions are provided as prompts for public discussion and consultation. In addition to the consolidated questions below, each Issue Paper includes detailed questions about the issues raised in each paper.

### 1. Provincial Standards

The Issue Papers suggest the need for provincial rules establishing key trustworthy criminal AI rules and criteria. The Issue Papers suggest many potential models, including:

- Federal legislation or regulations (*Criminal Code*, federal ADM Directive?).
- Provincial legislation or regulation (*EDSTA*, policing legislation, Ontario AI Directive?).
- Criminal justice institutional policies (Police, courts, Crown Policy Manual?).

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

### 2. Prohibited Uses and Risk Criteria

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

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

*If you agree some systems or uses should be prohibited or identified as “high-risk”:*

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

### 3. Bias, Privacy and Procedural Fairness

Trustworthy criminal AI initiatives consistently include principles or detailed rules to ensure these systems do not discriminate and protect privacy and procedural fairness. The components of these initiatives vary, but can often include:

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

The Issue Papers also note the variations within and between criminal AI systems have important implications for their risks and effect on rights.

*In principle, do you agree that the province and criminal justice institutions in Ontario should explicitly commit to ensuring criminal AI systems do not discriminate, protect privacy rights, and can be explained?*

*In your view, which of the components listed above are necessary to ensure criminal AI systems protect rights? Does Canadian law suggest which components should be adopted?*

*What is the best way to evaluate the rights impact of various criminal AI systems? Should there be a sliding-scale of mitigation requirements depending on the risk of the system?*

### 4. Disclosure

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

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

*Should there be a mandatory AI register or public report? If so, what should be included:*

- *A detailed or summary impact assessment?*
- *Comprehensive or a summary description of training data?*
- *Output data to facilitate independent auditing, oversight and performance monitoring?*

*How to promote disclosure while protecting other legitimate objectives, such as sensitive investigating techniques?*

### 5. Impact Assessments

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

- *Should the province require a mandatory impact assessment for criminal AI systems in Ontario? Do you agree an impact assessment should address privacy, human rights and procedural fairness and provide assurances about how an AI system will comply with other legal obligations?*
- *What other information or risks should be included?*
- *How to ensure impact assessments are being used and reported consistently?*

## 6. Bail and Sentencing Risk Assessments

Bail and sentencing risk assessment AI and algorithms raise many challenges, including questions regarding bias and discrimination, disclosure and an accused's ability to challenge an algorithm's predictions.

***How can the legal system ensure that AI-generated risk scores maintain the standards of openness, transparency, and reliability needed to protect the rights of individuals and uphold the integrity of the judicial process?***

***Do AI risk assessments, producing outputs based on discriminatory data, have a place in sentencing Indigenous and Black offenders?***

***If an AI risk assessment cannot consider colonial or racist legacies or histories that may have played a role in formulating the data its processes, would the assessment circumvent Criminal Code s. 493.2?***

## 7. AI Litigation

The Issue Papers discuss how criminal AI systems raise new and complex procedural, evidential and litigation challenges, including:

- Admissibility and reliability of AI evidence and whether AI is “expert evidence.”
- Use of AI to generate incident reports, summarize or analyze body cam data, etc.
- AI-assisted submissions to court or disclosure summaries.
- Deep fake evidence.
- AI-generated witness statements, victim impact statements, *Gladue* reports, etc.
- Litigating assertions of “trade secrets” or “investigative privilege.”
- Warrants or *O'Connor* Applications for third-party evidence.

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

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

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



## 8. Public Engagement

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

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

## 9. Access to Justice

The Issue Papers included extensive discussions about the potential systemic impact of criminal AI systems on access to justice and racialized, Indigenous or low-income communities in Ontario.

*In addition to the measures discussed above, how can Ontario's criminal justice system ensure access to justice if criminal AI systems are widely adopted in Ontario?*

*What policies or supports are needed to ensure access to justice for criminal defendants who lack the resources to challenge criminal AI systems?*

## 10. Institutional Capacity

The Issue Papers discuss how criminal AI systems raise new challenges for Ontario's criminal justice institutions.

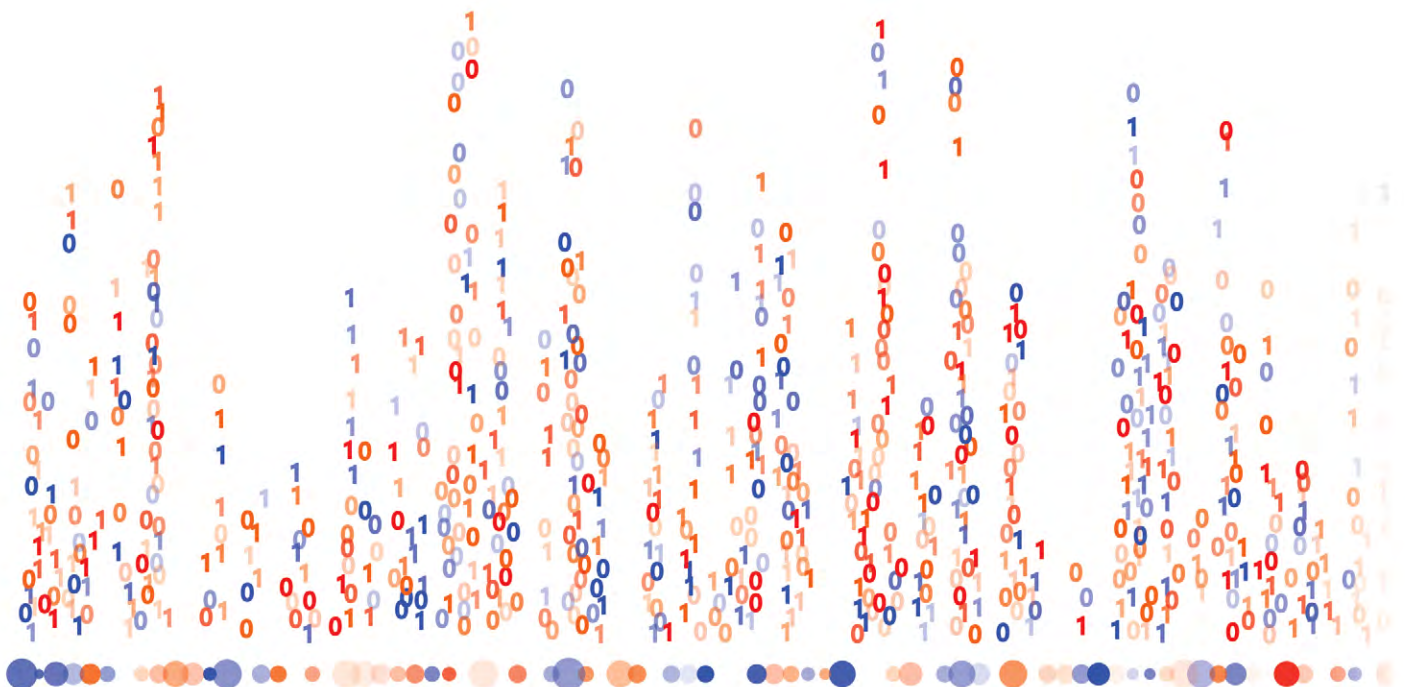
*Does the provincial justice system have capacity to respond to these challenges? If not, what tools or supports are needed to help institutions to proactively respond to these challenges?*

## 11. Systemic Oversight

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

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

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



# Endnotes

- 1 Predictive policing is discussed in the LCO’s Criminal AI Project Issue Paper 2, Use of AI by Law Enforcement [LCO Police AI Issue Paper] by LCO Counsel Ryan Fritsch. This paper is available online at <https://www.lco-cdo.org/en/our-current-projects/crimai/>. 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>; 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>.
- 2 Ferguson 2019 at 491.
- 3 To Surveil and Protect at 41-46.
- 4 See generally, LCO Police AI Issue Paper and NAS Predictive Policing at 3-4.
- 5 To Surveil and Protect at 47.
- 6 Law enforcement FRT is discussed in the LCO Police AI Issue Paper. 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>.
- 7 IPC FRT Report at 1.
- 8 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.
- 9 Europol, *AI and Policing: The Benefits and Challenges of Artificial Intelligence for Law Enforcement* [EUROPOL] (2024), online: <https://www.europol.europa.eu/publication-events/main-reports/ai-and-policing> at 21-29.
- 10 For example, see United States Government Accountability Office, *Report to Congressional Requesters, Facial Recognition Technology: Federal Law Enforcement Agencies Should Better Assess Privacy and Other Risks* (2021), online: <https://www.gao.gov/assets/gao-21-518.pdf>.
- 11 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* [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/>.
- 12 Toronto Police Services, *Update on the Implementation of the Board’s Policy on the Use of AI Technology* (January 11 2024), online: <https://tpsb.ca/jdownloads-categories?task=download.send&id=813:january-11-2024-public-agenda&catid=32>.

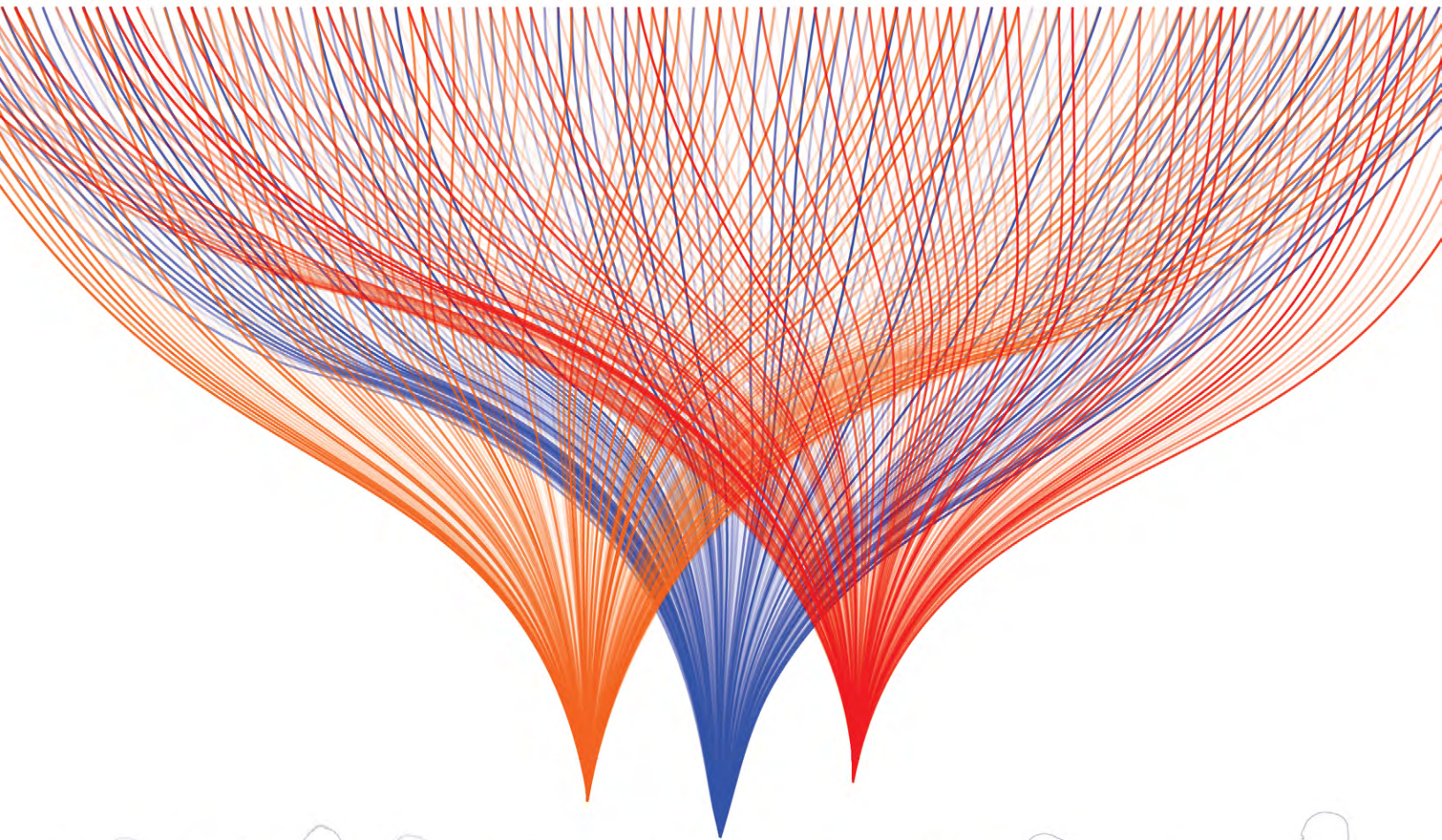
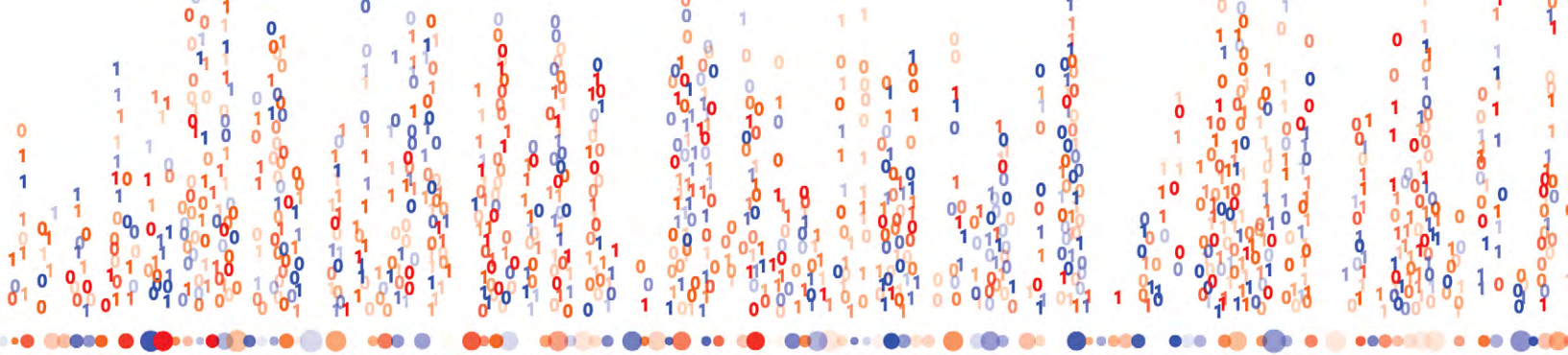
- 13 Bail and sentencing AI systems are discussed in the LCO Criminal AI Project Issue Paper 3, AI and the Assessment of Risk in Bail, Sentencing and Recidivism [LCO AI in Bail and Sentencing Issue Paper] by Armando D'Andrea, Criminal Panel Manager and former Criminal Duty Counsel, Legal Aid Ontario and Gideon Christian, Professor of Law, University of Calgary Faculty of Law. This paper is available online at <https://www.lco-cdo.org/en/our-current-projects/crimai/>. See also Law Commission of Ontario, The Rise and Fall of Algorithms in American Criminal Justice: Lessons for Canada [LCO American Lessons] (2020) [LCO Criminal AI Issue Paper], online: <https://www.lco-cdo.org/wp-content/uploads/2020/10/Criminal-AI-Paper-Final-Oct-28-2020.pdf>.
- 14 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>. See also LCO American Lessons.
- 15 Sarah Picard-Fritshe et al, Center on Court Innovation, Beyond the Algorithm: Pretrial Reform, Risk Assessment, and Racial Fairness (2019), online: [https://www.courtinnovation.org/sites/default/files/media/document/2019/Beyond\\_The\\_Algorithm.pdf](https://www.courtinnovation.org/sites/default/files/media/document/2019/Beyond_The_Algorithm.pdf) at 3.
- 16 These systems are described in several LCO Criminal AI project papers, including Paper 1, Introduction to the LCO Criminal AI Project [LCO Criminal AI Introduction] by LCO Executive Director Nye Thomas; Paper 2 LCO Police AI Issue Paper; and Paper 4, AI at Trial and Appeal, by Paula Thompson, Strategic Initiatives, Ministry of the Attorney General and Eric Neubauer, Defense Counsel, Neubauer Law, and Co-Chair, Criminal Lawyers Association Technology Committee. These papers are available online at <https://www.lco-cdo.org/en/our-current-projects/crimai/>.
- 17 For an extensive discussion of the AI data bias, see LCO American Lessons at 20-26. For a detailed discussion of AI and human rights generally, see Law Commission of Ontario, *Accountable AI*, (2022) [Accountable AI], online: <https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/regulating-ai-critical-issues-and-choices/> at 40-55. The LCO and Ontario Human Rights Commission have also recently developed the first AI human rights impact assessment (HRIA) based on Canadian law. The LCO/OHRC HRIA and an accompanying background paper is online at <https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/human-rights-ai-impact-assessment/>.
- 18 INCLO Challenging FRT at 25. The best-known FRT bias study is a 2019 report by the National Institute of Standards and Technology study which found that “[t]he majority of commercial facial-recognition systems exhibit bias” and “falsely identified African-American and Asian faces 10 to 100 times more than Caucasian faces.” National Institute of Standards and Technology (NIST), Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (2019), online: <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf> at 3. NIST also identified concerns regarding false negatives false positives, gender, and age.
- 19 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.” See also, Partnership on AI (PAI), Report on Algorithmic Risk Assessment Tools in the U.S. Criminal Justice System, (April 2019), online: <https://www.partnershiponai.org/report-on-machine-learning-in-risk-assessment-tools-in-the-u-s-criminal-justice-system/>.
- 20 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>; INTERPOL Policy Framework; and INCLO Challenging FRT.
- 21 See generally, INTERPOL Policy Framework and INCLO Challenging FRT as illustrative examples.
- 22 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>.

- 23 For example, see INTERPOL Policy Framework at 15-16. See also 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>. This report sets out detailed guidance addressing FRT implementation issues, operational considerations, and program review and evaluation at 4-33.
- 24 See the LCO’s American Lessons report for a good summary of these issues.
- 25 Joint Clearview AI Investigation.
- 26 David Freeman Engstrom & Daniel E. Ho, “Algorithmic Accountability in the Administrative State” in (2020) Yale Journal on Regulation 800, online: [papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3965041](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3965041) at 821.
- 27 See INCLC Challenging FRT, Ferguson 2019, and LCO American Lessons for representative examples of this analysis.
- 28 The variations between and within criminal AI systems confirm the need for tools and criteria to evaluate AI benefits and risks systematically. For example, an FRT system monitoring a public protest has more serious *Charter* and privacy risks than an FRT system monitoring a closed, secure facility. Predictive policing systems can also vary widely in scope and risk: Location-based systems have been used to manage police patrols, identify times and locations where specific crimes are likely to occur, and identify areas where community interventions could reduce crime. Person-based systems, on the other hand, have been used to predict individuals more likely to be involved with crime, to promote officer safety when responding to 911 calls, and to promote “focussed deterrence.”
- 29 NAS Predictive Policing at 1.
- 30 These reports are documented comprehensively in each of the LCO Criminal AI Project Issue Papers.
- 31 European Union, AI Act (Regulation (EU) 2024/1689 of the European Parliament and of the Council of Europe laying down harmonized rules on Artificial Intelligence [EU AI Act] (2024), online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689>. Chapter II, Article 5 of the EU AI Act sets out several “unacceptable risks” and prohibitions on specified AI systems. These systems are deemed “unacceptable” because they are a clear threat to European values and fundamental rights. Article 5 prohibits two AI systems that are directly relevant to criminal justice:
1. *Real-time remote biometric identification in publicly accessible spaces for law enforcement.*
  2. *Assessing the risk of an individual committing criminal offenses solely based on profiling or personality traits.*
- Both prohibitions are subject to important exceptions.
- 32 The EU AI Act, Chapter III, Annex III list of “high risk” systems include:
- 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.*

- 33 American initiatives are discussed at length in the LCO Criminal AI Introduction. See also generally, United States, Office of the President, Executive Order 14110 “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence” (November 1 2023), online: <https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence>; Office of Management and Budget, Executive Order M-24-10 “Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence” (March 2023); AINow Institute, “A Taxonomy of Legislative Approaches to Face Recognition in the United States” in *Regulating Biometrics: Global Approaches and Open Questions* (Sept 2020), online: <https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions>; New York Police Department, *Facial Recognition Technology Policy*, P.G. 212-129, (2020), online: <https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page>; and Policing Project, New York University School of Law, *Regulating Police Use of Facial Recognition Technology – Resources for Legislators* (accessed March 2025), online: <https://www.policingproject.org/regulating-police-use-of-face-recognition-technology>.
- 34 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>.
- 35 AIDA, s. 3.
- 36 See, for example, a joint open letter from 45 civil society organizations, experts and academics criticizing AIDA on numerous grounds, online: <https://bccla.org/policy-submission/joint-letter-of-concern-regarding-the-artificial-intelligence-and-data-act-aida/>.
- 37 Canada. Innovation, Science and Economic Development Canada, “Letter to the Chair of the Standing Committee on Industry and Technology on Bill C-27” (November 28, 2023), online: <https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12751351/12751351/MinisterOfInnovationScienceAndIndustry-2023-11-28-Combined-e.pdf>. The relevant classes of prohibited systems include Class 3 (“The use of an artificial intelligence system to process biometric data...”), Class 6 (“The use of an artificial intelligence system by a court or administrative body...”) and Class 7 (“The use of an artificial intelligence to assist a police officer...”).
- 38 See, for example, Privacy and Access Council of Canada, “Key stakeholders call for withdrawal of controversial AI legislation,” April 24, 2024, online: <https://pacc-ccap.ca/aida-open-letter/>.
- 39 Canada, Directive on Automated Decision-Making [Canada ADM Directive] (2019), online: <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592>; and Algorithmic Impact Assessment Tool [Canada AIA], online: <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html>.
- 40 Accountable AI.
- 41 See Accountable AI at 57-66.
- 42 Canada ADM Directive, s. 5.1. Note that the Directive applies only to federal departments subject to Treasury Board Secretariat.
- 43 This review is expected to be completed in 2025.
- 44 The creation of NTOP is discussed in 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>.
- 45 RCMP Communication with the LCO.
- 46 Royal Canadian Mounted Police, National Technology Onboarding Program, *Transparency Blueprint: Snapshot of Operational Technologies*, [RCMP Transparency Blueprint] (2024), online at <https://rcmp.ca/en/corporate-information/publications-and-manuals/national-technology-onboarding-program-transparency-blueprint>.
- 47 RCMP Transparency Blueprint at 9.
- 48 Enhancing Digital Security and Trust Act, S.O. 2024, c. 24, [EDSTA], online: <https://www.ontario.ca/laws/statute/24e24>.

- 49 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>.
- 50 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/>.
- 51 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.] 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.
- Second, s. 5(1) allows the province to prescribe AI “uses” or “circumstances” that are subject to the legislation.
- 52 Government of Ontario, Ministry of Public and Business Service Delivery and Procurement, Responsible Use of AI Directive, December 1, 2024 [Ontario AI Directive].
- 53 The Ontario AI Directive is discussed at length in the LCO Criminal AI Project Introduction.
- 54 Toronto Police Services Board, Use of Artificial Intelligence Technology [TPS AI Policy] (February 28, 2022; updated January 11, 2024), online: <https://tpsb.ca/policies-by-laws/board-policies/195-use-of-artificial-intelligence-technology>.
- 55 TPS AI Policy, “Guiding Principles.”
- 56 TPS AI Policy, “Guiding Principles.”
- 57 TPS AI Policy, “Policy of the Board.”
- 58 Toronto Police Services, Update on the Implementation of the Board’s Policy on the Use of AI Technology (January 11 2024), online: <https://tpsb.ca/jdownloads-categories?task=download.send&id=813;january-11-2024-public-agenda&catid=32>.
- 59 Durham Regional Police Services Board, Use of Artificial Intelligence Policy, October 2024, online at <https://durhampoliceboard.ca/policies-and-bylaws/>.
- 60 The Ontario Human Rights Commission and the Information and Privacy Commissioner of Ontario recently criticized the TPS for categorizing their use of certain AI technologies – including automated license plate readers and fingerprint identification – as “low risk technologies” with fewer assessment and oversight requirements. 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](https://www.ohrc.on.ca/en/news_centre/approval-high-risk-technologies-under-toronto-police-services-boards-policy-use-artificial).

- 61 These reports include: Office of the Privacy Commissioner of Canada, Police use of Facial Recognition Technology in Canada and the Way Forward (June 10 2021), online: [https://www.priv.gc.ca/en/opc-actions-and-decisions/ar\\_index/202021/sr RCMP/](https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr RCMP/); Privacy Commissioners Joint Clearview AI Investigation; Privacy Commissioners of Canada, Joint Statement, Privacy guidance on facial recognition for police agencies (May 2022), online: [https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd\\_fr\\_202205/](https://www.priv.gc.ca/en/privacy-topics/surveillance/police-and-public-safety/gd_fr_202205/); OPC Police FRT Guidance (2022); IPC Mugshot Guidance (2024); and 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>.
- 62 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>.
- 63 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](https://www.manitobacourts.mb.ca/site/assets/files/2045/practice_direction_-_use_of_artificial_intelligence_in_court_submissions.pdf); Québec, “Integrity of Court Submissions When Using Large Language Models” (October 2023) online: [https://coursuperieureduquebec.ca/fileadmin/cour-superieure/Communiqués\\_et\\_Directives/Montreal/Avis\\_a\\_la\\_Communité\\_juridique-Utilisation\\_intelligence\\_artificielle\\_EN.pdf](https://coursuperieureduquebec.ca/fileadmin/cour-superieure/Communiqués_et_Directives/Montreal/Avis_a_la_Communité_juridique-Utilisation_intelligence_artificielle_EN.pdf).
- 64 Canadian Judicial Council, Guidelines for the Use of Artificial Intelligence in Canadian Courts (Sept. 2024) [CJC Guidelines], online at <https://cjc-ccm.ca/en/news/canadian-judicial-council-issues-guidelines-use-artificial-intelligence-canadian-courts>.



LAW COMMISSION OF ONTARIO  
COMMISSION DU DROIT DE L'ONTARIO

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