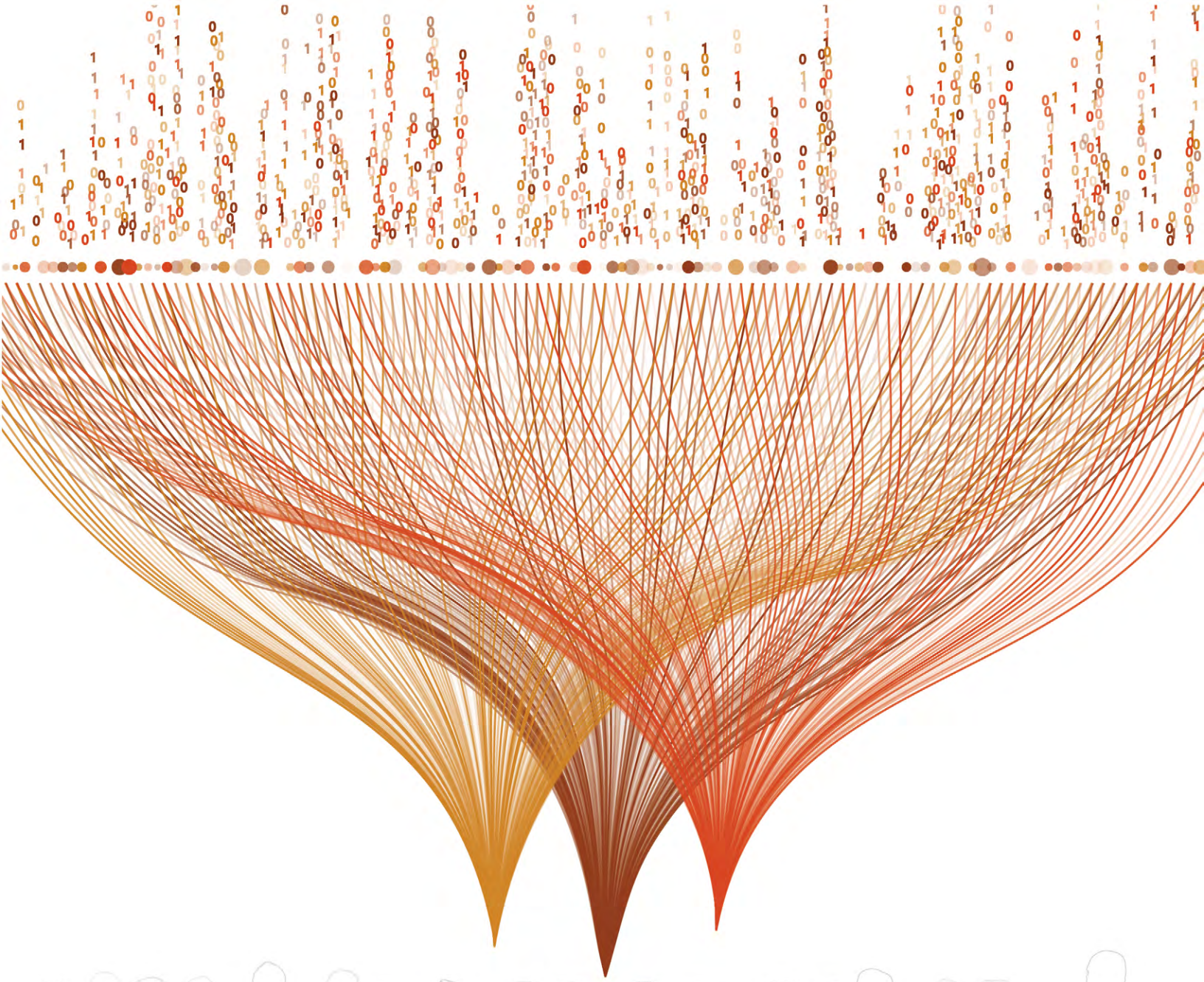


Law Commission of Ontario

AI IN CRIMINAL JUSTICE PROJECT | PAPER 3

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

April 2025

LCO
CDO

LAW COMMISSION OF ONTARIO
COMMISSION DU DROIT DE L'ONTARIO

About the Law Commission of Ontario

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

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

The LCO has considerable experience analyzing AI regulation in the Canadian justice system. Recent LCO reports and submissions addressing these issues include:

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

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

Authors

Armando D'Andrea, Staff Lawyer, Provincial Office, Legal Aid Ontario
Gideon Christian, Professor of Law, Faculty of Law, University of Calgary

Series Editors

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

The LCO AI In Criminal Justice Project Paper Series

Paper 1	Introduction and Summary: LCO AI in Criminal Justice Project 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.

Student Researchers

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

External Advisory Committee

Alpha Chan, Chief Information Security Officer, Toronto Police Services

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

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

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

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

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

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

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

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

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

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

Michael Swinburne, Senior Policy Advisor, Canadian Human Rights Commission

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

Disclaimer

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

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

Citation

Law Commission of Ontario, ***AI and the Assessment of Risk in Bail, Sentencing and Recidivism: Paper 3 in the LCO AI in Criminal Justice Project*** (Toronto: April 2025).

Contact

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

Tel: (416) 650-8406
E-mail: LawCommission@lco-cdo.org
Web: https://www.lco-cdo.org
LinkedIn: https://linkedin.com/company/lco-cdo
Bluesky: @lco-cdo.bsky.social
X: @LCO_CDO
YouTube: @lawcommissionofontario8724

Funders

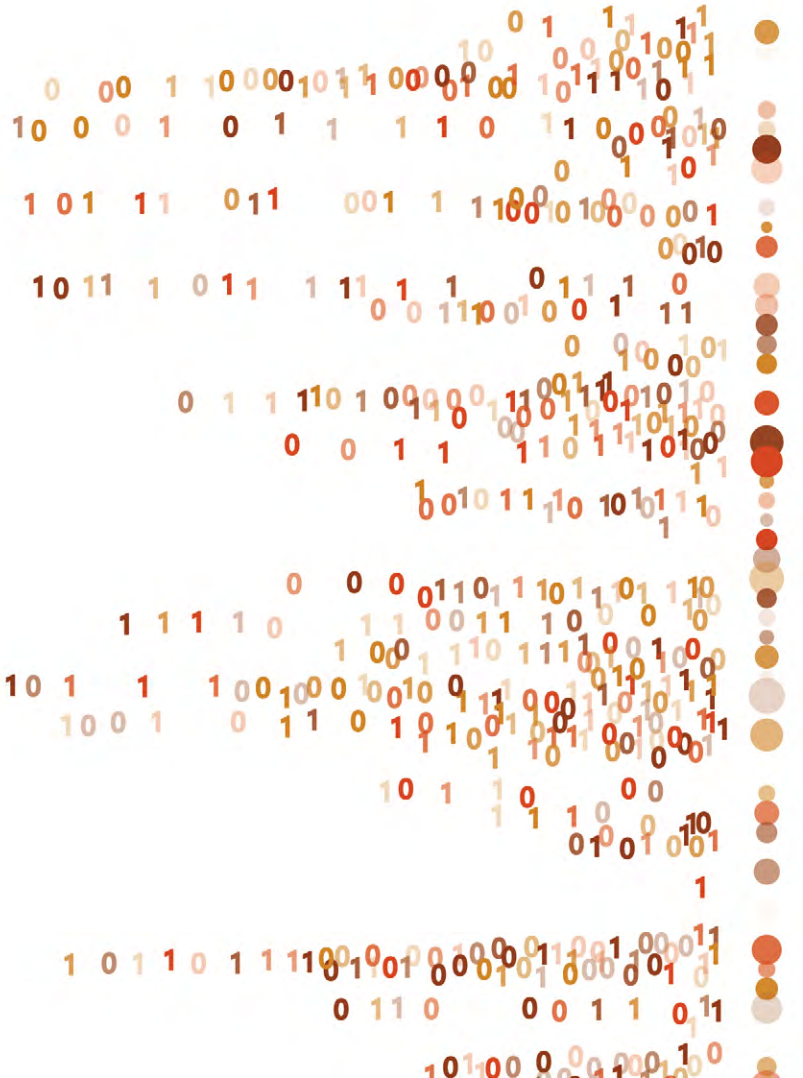
Financial support is provided by the Law Foundation of Ontario, the Law Society of Ontario, and Osgoode Hall Law School. The LCO is located at Osgoode Hall Law School in Toronto.

The Law Foundation of Ontario
Advancing access to justice

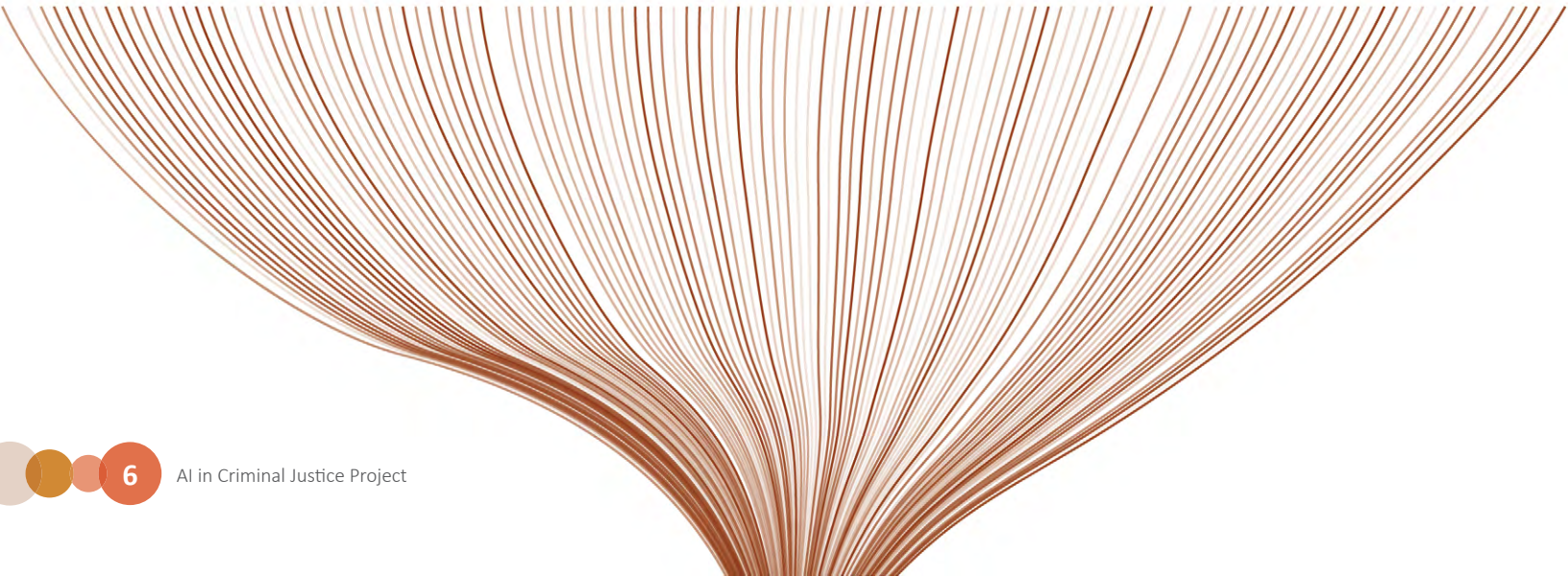
Law Society of Ontario | Barreau de l'Ontario

OSGOODE HALL LAW SCHOOL | YORK UNIVERSITÉ UNIVERSITY

Layout and Design by 12thirteen.



Contents



1. Introduction

1.1 The LCO AI in Criminal Justice Project

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

Many AI technologies have potential to improve public safety, improve police investigations, and improve the efficiency and fairness of criminal proceedings. Many AI technologies also appear to have potential to address, at least in part, long-standing concerns about racialized criminal justice and access to justice.

At the same time, the use of AI in criminal justice is controversial. Technologies such as predictive policing, facial recognition and biometric surveillance, and bail/sentencing algorithms have been criticized in many jurisdictions for their impact on racialized and low-income communities, constitutional rights, human rights, criminal procedure, criminal common law principles, privacy, and access to justice.

The LCO AI in Criminal Justice Project is a unique collaboration of leading practitioners and experts from across the Canadian criminal justice system. Project authors and advisors include representatives from governments, police services, Crowns, the criminal defence bar, courts administration, legal aid, human rights commissions, civil society organizations, and academics.

Working together, the LCO and our collaborators believe this project is an important contribution towards developing "Trustworthy Criminal AI" in the Canadian justice system. Our collective goal is help inform institutions, policymakers and stakeholders about the law reform issues, choices, opportunities, and challenges in this complex and fast-moving area.

This paper is the third of a series of five Issue Papers that comprise the project. Each Issue Paper is an expert collaboration considering the use of AI in a distinct phase of the criminal justice process, including:

Paper 1	LCO AI in Criminal Justice Project: 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 in Criminal Justice.

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

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

To their credit, some Canadian police services and other agencies have taken important initiatives to address AI risks. As will be seen, however, there are still wide and consequential gaps in the legislative or legal framework governing these systems. Indeed, Canadian lawmakers are far behind their international counterparts where the first "wave" of criminal justice AI governance has already been supplanted by more sophisticated laws and policies.

The LCO AI in Criminal Justice Project is organized around four key themes or topics.

First, the project considers several important practical and legal questions that will soon confront Canadian police, courts, policymakers, Crowns, defence counsel, and criminal accused, including:

- What AI tools are or may be used at each important stage of Canadian criminal justice?
- What legal issues are likely to arise at each stage?
- What is the state of Canadian law and procedures to address these issues, particularly in relation to the Canadian *Charter of Rights and Freedoms*, procedural fairness, evidence law, and criminal common law?
- What issues cut across specific proceedings or stages and suggest the need for a systemic response or framework?

Second, the LCO project asks who is likely to be affected by AI in the criminal justice system. What institutions, agencies, organizations, or individuals will be affected in some way? And what does the breadth or complexity of those actors suggest about criminal justice AI regulation and governance?

Third, the LCO project surveys potential solutions at the specific and systemic level. In so doing, the project highlights the speed, variety, sophistication, and breadth of AI regulation in recent years. This Introduction and the Issue Papers discuss potential policy, procedural, or law reform responses to the issues arising at each respective stage, including:

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

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

The LCO's series of Issue Papers are designed to facilitate discussion and consultation. We have learned that "trustworthy criminal AI" depends on complex legal, technical and operational considerations. We have also learned that broad collaborations and consultations are crucial. Accordingly, each Issue Paper includes questions for Canadian criminal AI policymakers and stakeholders. In this manner, the LCO hopes the papers will become a catalyst for a wider Canadian discussion about these issues.

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

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

Background and Definitions.

Readers are encouraged to first review LCO's *Introduction and Summary: LCO AI in Criminal Justice Project*. This paper establishes a definition for "artificial intelligence" used throughout this project. In addition, the paper provides an overview of various AI technologies in criminal justice and gives a primer on the basic legal and policy frameworks governing AI in Canada and elsewhere.

1.2 Executive Summary: AI-enabled risk assessments in the criminal justice system

The specific subject of this, the third in the series of Consultation Papers, is AI-enabled risk assessment tools in bail, sentencing, and predicting recidivism.

An array of AI-enabled tools now exist that aim to aid criminal courts in determining pretrial bail, sentencing, and post-sentencing risk and recidivism. The impact of these tools is considerable. For an accused or convicted person, such tools may determine in-custody or release status, parole status, the length of detention, the conditions of detention, and conditions on community living.

AI-enabled risk assessments are thus an important case study in the use of AI and algorithms in criminal justice. Bail, sentencing, and post-sentencing proceedings adjudicate and balance fundamental liberty and public safety issues while needing to ensure high standards of due process, accountability, and transparency. According to the Partnership on AI (PAI), an American research organization focussing on best practices for AI, criminal risk assessment tools "present a paradigmatic example of the potential social and ethical consequences of automated AI decision-making."[1]

Although AI-enabled risk assessment tools are not currently in use in the Canadian criminal justice system, their use is certain to be considered. AI-enabled risk assessment tools may also be adopted by institutions who directly or indirectly inform criminal justice proceedings, such as support and diversion services provided to children, families, or persons with addictions or mental disorders. It is only a matter of time before AI-enabled risk assessment tools face judicial scrutiny and make their way into the criminal justice system.

It is thus important to identify issues related to the use of this novel technology in the Canadian criminal justice system, as well as develop recommendations for addressing such issues. Consistent with other papers in this series, AI is analyzed through the law on which

Canadian criminal justice stands: the *Canadian Charter of Rights and Freedoms*, procedural fairness, and the principles and precedents of criminal common law.

The use of AI-enabled risk assessment scores – intended to provide "evidence-based data" and assist in streamlining or enhancing the bail or sentencing calculus – raises a number of concerns with procedural fairness, the *Charter of Rights and Freedoms*, and human rights in Ontario's criminal courts.

In sum, the desire to introduce AI-enabled risk assessments that improve efficiency and accuracy faces a difficult legal gauntlet. Established provisions in the *Criminal Code* of Canada (CCC), common law, and criminal procedure raise questions about their role, admissibility, and viability. Furthermore, the novelty and complexity involved in assessing AI-enabled risk assessment tools foreshadow the additional legal challenges and resources that will be required before the use of such tools can be permitted, and call into question the capacity of courts to provide continuous oversight for their use. These challenges suggest the need for a more proactive, systemic approach to assessing, authorizing, and continually overseeing the potential deployment of AI-enabled risk assessment tools in Ontario's criminal justice system.

What other risk assessment tools may be at play?

The focus of this paper concerns the use of AI-enabled risk assessments for determining bail, sentencing, and post-sentencing risk and recidivism. Criminal proceedings often rely on yet other forms of risk assessment, including assessments for diversion to mental health courts, drug treatment courts, and community programs. While this paper does not examine the potential impact of AI on these specific risk assessment tools, the discussion that follows surfaces many of the critical legal, ethical and procedural themes equally applicable to such risk assessment tools.

Section 2 of this paper introduces a discussion about the role, nature and legal characterization of AI-enabled risk assessment tools.

First and foremost, it remains an open question as to how AI-enabled risk assessment evidence will be characterized. Courts may interpret these instruments variously as "expert opinion" or "demonstrative aid" evidence. This, in turn, raises competing common law tests for the admissibility, reliability and weight given to such evidence, and its role in assessing risk, eligibility and conditions in bail, sentencing, and community diversion.

A second key challenge is the inability to pierce the "black box" nature of AI-enabled risk assessment tools. The inability to cross examine this evidence – particularly raising questions about reliability and relevance – will be key to determining the admissibility of this evidence.

A third preliminary concern is the nature of sentencing and bail as highly individualized processes. It remains to be seen whether AI-enabled tools will capably identify, weigh, and interpret personal circumstances, social context, and acknowledged vulnerabilities and mitigating measures. A further and perhaps more intractable concern is the potential admission of AI-enabled risk assessment evidence based on historical data that reflects biased practices and antecedents. This may conflict directly with the aims of statutory and jurisprudential developments that stress the contextualization and amelioration of that history.

Section 3 then takes a deeper dive into a series of practical legal challenges AI-enabled risk assessment tools will have to navigate. This includes:

- Bias in the training, development and use of AI-enabled risk assessment tools;
- Navigating disclosure, trade secrets and intellectual property rights;
- Assessing predictive accuracy;
- AI-enabled risk assessment tools as expert evidence;
- AI-enabled risk assessment tools as demonstrative aid evidence;

- AI-enabled risk assessment as an aggravating factor;
- Sentencing and post-sentencing risk assessment; and
- Challenging AI-enabled risk assessment in the bail process.

Overall, the discussion suggests that the use of AI-enabled risk assessment tools in bail, sentencing and community diversion may offend recent jurisprudence.

As explored below in sections 3.1 and 3.2, understanding the character and nature of AI-enabled risk assessment will determine the appropriate approach to assess admissibility.

If it is a form of opinion evidence, it will engage the well-entrenched jurisprudential framework for admitting expert opinion evidence in which issues will arise related to relevance and necessity. However, AI evidence gives rise to several foreseeable legal and practical challenges. This can include:

- The inability to directly cross-examine the opinion of an AI system.
- The unavailability of AI expertise and experts for cross-examination.
- The inscrutability of an AI system.
- Assertions of trade secrets and intellectual property.
- A lack of independent assessment and reporting on the performance, validity, reliability and predictability of AI systems and their outputs
- The availability of training data sets.
- Changes in the AI algorithm and software over time, including differences between iterations or versions.
- Determining how AI experts may be paid and who is responsible for paying them.

These issues ultimately put AI tools in conflict with admissibility rules as currently constituted. Section 3.4 proposes other possible characterizations of the algorithmic risk assessment, including as a demonstrative aid.

Additional complications with AI-enabled risk assessment tools arise at sentencing and in post-sentence risk assessment. Section 3.5 problematizes an essential tension in AI-enabled risk assessment: using a group of individuals with similar characteristics to make predictions and recommendations in context of individualized assessment and sentencing. A further issue arises if the algorithm's prediction draws primarily from historical data that may be racist or biased. Reliance on these scores – particularly in sentencing for Indigenous and Black defendants – likely conflicts with current sentencing frameworks that explicitly consider and attempt to ameliorate historically racist or biased practices in criminal justice that diminish the moral culpability of the accused.

Finally, section 3.6 of this paper examines complications arising in bail. There has been a re-invigorated appreciation for the importance of the bail decision after *Antic, Myers* and *Zora*.[2] The principles reflected in this jurisprudence may conflict with the application of AI risk assessments. For instance:

- The bail process continues to value efficient process, while the potential introduction and reliance on AI-enabled risk assessment will require greater scrutiny and rigor which may prolong and add complexity to the proceedings.
- AI recommendations may be seen as engaging in "discriminatory thinking" in conflict with safeguards defined in *Criminal Code* s. 493.2.
- The validity, reliability and explainability of AI may undermine high-risk designations, and fail to reflect, account for, or have the capability to rationalize individualized assessment.

Consultation Questions

Section 4.2 of the paper consolidates the set of consultation questions identified throughout this paper, outlines next steps for consultations, and describes how to get involved. For convenience, the consultation questions are outlined below.

AI-enabled risk assessment tools in criminal justice

1) Assessments and predictions about risks, public safety and other factors are not new. However, AI-enabled risk assessments bring new complications, such as a lack of verification, calibration, and certification; technological deference where humans are over-reliant and uncritical about AI-generated recommendations; and other factors. Given this, what weight should jurists assign to AI-enabled prediction? How is this similar to or different from other traditional risk assessment tools?

Bias in the training, development and use of AI risk tools

2) Given the significant influence of private commercial actors in the development of AI risk assessment tools, what regulations or policies are needed to ensure a transparent process involving criminal justice stakeholders, aiming to safeguard public interest and improve the reliability and fairness of these tools?

Navigating disclosure, trade secrets and intellectual property rights

3) How can the criminal justice system balance the need for transparency and the fair administration of justice with the proprietary rights of commercial corporations that design AI risk assessment tools, ensuring that all parties involved in a legal matter have access to and understanding of the methodologies behind these tools?

4) Given the Supreme Court of Canada's stance on access to proprietary information as necessary to preserve Charter rights, what legal frameworks or guidelines should be developed to guide commercial corporations entering the Canadian criminal justice market on the disclosure of proprietary information, especially in situations where such disclosure is crucial to ensuring a fair trial and upholding the rights of the accused?

Assessing predictive accuracy

5) Where the prosecution in a criminal proceeding seeks to introduce evidence from an AI risk tool, should a burden be imposed on the prosecution to lead evidence relating to the reliability and validity of the AI tool? Should similar burden be imposed on the defence where it seeks to use AI risk assessment evidence as a mitigating factor?

AI-enabled risk assessment tools as expert evidence

6) Considering the opacity of algorithmic risk assessment, particularly in the absence of any ability to cross examine, how can a judge properly scrutinize its processes, examine its integrity, and determine if its expertise can be properly "qualified?" Will the current inability of defence counsel to cross examine "black box" algorithmic risk assessment be critical to its admissibility?

7) Are AI-enabled risk assessments likely to result in frequent litigation and legal challenges that place an undue resource burden on the justice system? In the Court of Justice, where many pleas can be arranged and traversed into the plea court quickly and on the same day, are Crown attorneys, duty counsel and defence counsel going to have the time and resources to litigate the admissibility of algorithmic risk assessments?

8) What systemic policies, practices, and conventions are in play and how might they need to be addressed for any of the following:
   - What is the role of the Crown and what kinds of systemic issues should the Crown look at to ameliorate some of the problems?
   - What can the judiciary do?
   - What can Legal Aid Ontario do?

9) AI-generated risk scores are increasingly relied on as expert evidence in some criminal justice systems (such as the United States) while increasingly restricted in other jurisdictions (such as the European Union). What are the expectations of existing Canadian legal standards for risk assessments in relation to openness, transparency, and reliability, and how do these apply to AI-based risk assessments?

10) Given the varied acceptance of AI-generated risk scores as expert evidence across different courts, what policy measures should be implemented to standardize the scrutiny and admissibility of such evidence in criminal proceedings to safeguard against potential biases and ensure fair treatment of all individuals within the justice system? How can the legal system maintain the required standards of openness, transparency, and reliability to protect the rights of individuals and uphold the integrity of the judicial process?

AI-enabled sentencing and post-sentencing risk assessment

11) How can the Canadian criminal justice system maintain the principle of individualized sentencing while integrating AI-generated risk scores in the decision-making process, ensuring these tools do not override judicial discretion and contribute to potential over-incarceration or stereotyping of offenders?

12) Given the risk of AI recidivism risk assessments facilitating decision-making based on the behaviour of others and potentially contributing to racial discrimination, what measures can be implemented to critically evaluate and adjust the variables used by these tools to prevent the perpetuation of structural racism within the criminal justice system?

13) Can algorithmic risk assessments, producing outputs on the basis of a discriminatory history, have a place in sentencing Indigenous and Black offenders in light of current sentencing caselaw like *Ipeelee* and *Morris*?

Challenging AI-enabled risk assessment in the bail process

14) Defence counsel run bail hearings on serious charges with only a synopsis read in and no disclosure. Is the power of an algorithmic risk assessment stronger or different than a graphic synopsis on a serious charge? If it is, is it fair that accused be advised to wait for disclosure regarding inputs or on an algorithm's operation (and stay in custody longer while counsel attempts to decipher it), or proceed with the risk assessment number looming large in court?

15) Is there a concern about the "relevance" of the risk assessment score if it is based on information that would legally be "irrelevant" at the bail hearing? Does this put an impetus on counsel to request and wait for the inputs?

16) Recent developments in jurisprudence (such as Ipeelee and Morris) and legislation (CCC s. 493.2) require consideration of how historical bias and discrimination have played a role in the disproportionate disadvantage and criminalization of Indigenous and Black communities. If the algorithm cannot consider colonial or racist legacies or histories that may have played a role in formulating the data it processes, does admission of the score circumvent *Criminal Code* s. 493.2? Can counsel successfully argue that given the principles of s493.2, the unexplained risk score should be given less (or no) weight?

17) Do release matrix recommended conditions – such as house arrest or a curfew –amount to boilerplate conditions "inserted by rote" where there is no justification of the score or of the accused's placement in that category?

18) If reasons are to represent a promotion of visibility – including ensuring that racial bias plays no role in the bail decision – can there be any place for evidence that in and of itself does not give any reasons?

19) What legislative or regulatory measures should be introduced to set standards and ensure rigorous testing and validation of these tools for bias before their deployment in the criminal justice system, and how can ongoing oversight be maintained?

1.3 Consultations, contacts, and project support

Consultations

The LCO believes that successful law reform depends on broad and accessible consultations with individuals, communities, and organizations across Ontario. As a result, the LCO is seeking comments and advice on this issues paper. There are many ways to get involved. Ontarians can:

- Learn about the project and sign up for project updates on our project website.
- Contact us to ask about the project.
- Provide written submissions or comments on this issues paper.

Project Lead and Contact

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

The LCO can be contacted at:

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

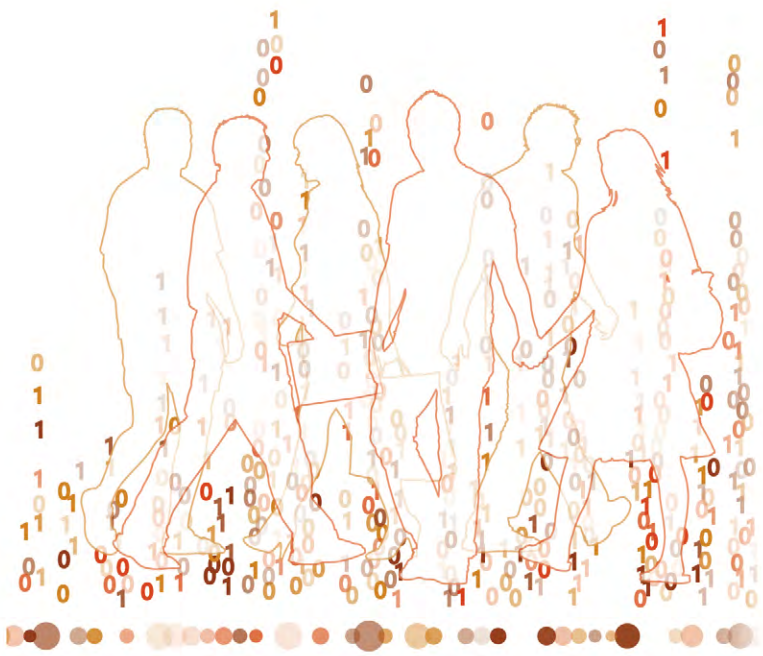
Tel: (416) 650-8406
E-mail: LawCommission@lco-cdo.org
Web: https://www.lco-cdo.org
LinkedIn: https://linkedin.com/company/lco-cdo
Bluesky: @lco-cdo.bsky.social
X: @LCO_CDO
YouTube: @lawcommissionofontario8724

Author and Project Editors

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

Project authors include:

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



Advisory Committee

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

- Alpha Chan, Chief Information Security Officer, 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

2. AI-enabled Risk Assessment in the Criminal Justice System

2.1 What are risk assessment tools?

Risk assessment is the process of determining the likelihood that an accused, convicted, or incarcerated person will reoffend (recidivism). The process aims to assist in determining the appropriate limitation on the subject's freedom.

Risk assessment tools and their underlying philosophies have long been part of the criminal justice system.[3] But today, technological innovation – especially in AI – is making new models of recidivism risk assessment tools available. The big data revolution has propelled data-driven decision-making processes in both the private and public sector. Evidence-based risk assessment in the criminal justice system reflects these developments.[4] Tools built on AI technology are now used in many criminal justice systems outside Canada and in all phases of a proceeding.

AI-driven risk assessment tools may now be used during:

- Pretrial: to determine whether an accused person should be granted bail or community diversion, pending trial or other disposition of the charges.
- Sentencing: to inform a judge and determine an appropriate sentence upon conviction.
- Post-sentencing: to inform correctional officers who identify the level of security classification of inmates, and parole officers who decide an incarcerated person's eligibility for parole.[5]

Common to all risk assessment tools is reliance on a mix of dynamic and static characteristics:

- Dynamic risk factors are traits or characteristics of an individual that may contribute to recidivism and may change over time.[6] Examples include lack of employment or education, lack of respect for constituted authority, membership in criminal organizations like gangs, substance abuse, and other antisocial behaviours that are likely to encourage a person to gravitate towards criminality. These factors are dynamic in that they could be altered by education, treatment, or voluntary individual activity.
- Static risk factors are embedded traits in an individual's life that may lead someone to gravitate towards reoffending, such as a past criminal record, age at the time of first arrest, and gender.[7] Unlike dynamic factors, static factors tend to be permanent and hence not easily amenable to alteration or intervention.

Effective risk assessment influences decision making in every phase of the criminal justice system. But this has always been undermined by several factors, several of which may be ameliorated or exacerbated by AI-enabled risk assessment tools. Two of these are highlighted at the outset.

First, courts are unlikely to have direct control over the risk assessment tools that they are called upon to oversee and interpret. A wide array of risk assessment tools may be developed, selected, and used by different justice sector institutions.

Furthermore, courts routinely rely on adjacent social or medical service providers, social and medical professionals, and others. These providers may directly or indirectly intersect with criminal justice proceedings through government and community support services provided to children, families, recently incarcerated persons, and persons with mental disorders. Such assessments may be admitted into a criminal proceeding and relied on by judges, prosecutors, and others. However, these court actors may have no formal training in such tools and are unlikely to have had any direct control or input on the development of such tools. Understanding the strengths, limitations, and appropriate interpretation and application of an array of third-party tools is thus a crucial competency and procedure that courts need.

Second, all risk assessment tools have the inherent problem of potentially generating biased outcomes. This applies to both traditional risk assessment tools in which humans make the assessment (which are known as first-, second-, and third-generation tools) and now AI-enabled tools in which algorithms make assessments (known as fourth-generation tools).

Human risk assessment by criminal justice and clinical professionals, part of the first-generation risk assessment approach, makes possible a personalized or individualized risk assessment that considers the individual's unique circumstances. However, this process is obviously susceptible to human biases, as criminal justice decisions affecting fundamental liberties of the subjects – from pretrial release to sentencing and beyond – are guided by human instincts and biases dressed up as professional, clinical or otherwise objective or "common sense" opinions. This has inevitably resulted in biased outcomes, with different treatment of individuals who may ostensibly have similar circumstances.[8]

At the other end of this spectrum are the fourth-generation risk assessments that rely less on human than algorithmic insights. These enable the automation of risk assessment by incorporating complex AI processes, such as machine learning algorithms. The simplistic perspective here is that if AI algorithms could rightly assess risks posed by individuals in the criminal justice system, such tools would eliminate human bias. The outcome would be similar treatment of similar cases and a fairer system.

On the other hand, criticisms and experience in the use of AI-enabled risk assessment tools suggest that there are many limitations that undermine this aspiration of AI systems, including the potential for spurious correlations the justice system should not rely on (such as proxies for recidivism like race or postal code), reliance on historically and endemically biased justice system data, and the operation of AI recommendations as a "black box" technology incapable of rationalizing or explaining the decisions or recommendations it makes.

These limitations are explored further in the following section.

2.2 How is AI different than other risk assessment tools?

In reference to the use of risk assessment tools in carceral institutions, the Supreme Court of Canada (SCC) has linked the Correctional Services of Canada (CSC) obligations under the *Correction and Conditional Release Act* (CCRA)[9] to results generated by risk assessment tools. Specifically, the CCRA s. 24(1) obligates the CSC to "take all reasonable steps to ensure that any information about an offender that it uses is as accurate, up to date and complete as possible."[10] This obligation extends to results generated from risk assessment tools while a subject is incarcerated by the carceral institution.

One issue introduced by AI-powered risk assessment tools is their use of population-based rather than individual assessments. Accurate sentencing should be based on assessment of facts specific to the individual offender and the offence. But modern recidivism risk assessment tools built on algorithms and big data provide predictions based on average recidivism of a general population of people who share characteristics similar to the accused.[11] Modern recidivism risk assessment technology would thus appear to deprive the subject of the right to an individualized sentence, one that is based on accurate information. Neglecting this obligation therefore raises a *Charter* issue relating to the constitutionality of assessments made by the technology.[12]

Legal and ethical issues also exist pertaining to the AI technology methodologies used in recidivism risk assessments. These methodologies are typically considered proprietary trade secrets and thus may not be readily available for scrutiny by the court, the accused, or the prosecution. This has the impact of restricting the ability of these parties to access or determine what factors have been considered as part of the assessment, as well as the degree of weight attached to those factors.[13] The proprietary nature of these AI tools therefore raises some important legal and ethical concerns related to fairness, accountability, and transparency. This will most obviously be the case where a convicted or incarcerated individual seeks access to proprietary information to challenge judicial or administrative decisions impacting their freedom or liberty, including criminal sentencing or security classifications.

Risk Assessment In the Age of AI: The Case Studies of Zilly and Loomis[14]

Historically speaking, we might never know who the first human being was to be imprisoned by AI. But we can point to early and cautionary cases – and to the irrevocably changed lives that resulted – to get a sense of the promises and perils at issue in AI-based risk assessment.

The 2013 US prosecution of Paul Zilly began routinely: a Wisconsin man was found guilty of stealing a lawn mower to sell it for parts.[15] Accounting for the history of the accused and his recent attempts to reform his behaviour, the prosecutor recommended a prison sentence of 12 months. Mr Zilly and his defence counsel were amenable to the proposal, and consent was given to a plea deal on those terms.

In many cases, a plea deal effectively resolves the proceeding. In Zilly's sentencing hearing, however, the presiding judge decided to take an additional step. Beyond the joint sentencing submission of the prosecution and the defence, the judge considered the opinion of COMPAS (the "Correctional Offender Management Profiling for Alternative Sanctions," created by Northpointe, Inc.). COMPAS is an opaque algorithmic profiling system analyzing over 100 personal details gathered from various sources, including from the accused himself. Based on these characteristics, COMPAS determined Zilly's recidivism risk score and predicted a high likelihood for future violent recidivism. The sentencing judge interpreted the score as being "about as bad as it could be."[16]

In what is surely an early example of AI-related automation bias at work, the judge accepted COMPAS's recommendation at face value and set aside the plea deal. Zilly now faced the imposition of a revised sentence of 24 months, which doubled the 12-month sentence agreed to by the prosecutor and the defence and added 36 months of community supervision to follow thereafter.[17]

On appeal, the court reviewed the rationale for Zilly's expanded sentence with apprehension. They found the testimony of the COMPAS programmer hesitant and hedged, elusive and incomplete in describing how the algorithmic risk assessment could be so confident in inferring future crimes from Zilly's history, personal characteristics, and present circumstances.[18]

The appeal court further considered how access to the algorithmic source code was blocked as a corporate trade secret and thus inscrutable to review by the court in a public airing. Unconvinced about the judicial process of relying on the COMPAS recommendation, as well as the soundness of COMPAS's "black box"[19] recommendation, the appeal court allowed Zilly's sentence appeal and reduced it from 24 to 18 months. Although this was still longer than the original plea deal of 12 months, it evidently reflected the consensus of the legal code: "Had I not had the COMPAS," the trial judge later acknowledged, "I believe it would likely be that I would have given one year, six months."[20]

Notwithstanding these shortcomings, some would characterize Zilly's case as merely a narrow miss in comparison with others less fortunate. In a 2016 case, *State v. Loomis*,[21] the prosecution and court similarly relied on a COMPAS score for sentencing, but the stakes were rather higher. As reported in the plain language of a newspaper headline, the court in Loomis sent a man to prison for six years "by a software program's secret algorithm."[22] Looking back on his own close encounter with the profiling proclivities of algorithmic justice, Zilly said, "Not that I'm innocent, but I just believe people do change."[23]

Taken at face value, the Zilly and Loomis cases suggest that AI-based risk-assessment systems may be poorly conceived and developed, and then deployed with inadequate procedural supports and safeguards. This can compound well-known systemic biases while further complicating transparency and due process.

Specifically, Zilly's case demonstrates:

- a poorly defined or circumscribed role for the "human-in-the-loop" (namely, the prosecutor, the defence, the accused, and the judge), leading to muddled interpretation of AI recommendations and arbitrary decision-making;[24]
- automation bias and blind technological deference;
- diminished standards for procedural fairness and due process in such routine matters as compelled disclosure of personal information (submitting to a profiling exercise), a clear explanation and rationale for reasons (rather than merely receiving a determination), or the right to examine and cross-examine the evidence or opinion of an expert (whether that expert is a person or a machine!);
- biased data and loaded profiling;
- rough inferences drawn from historical and personal data with limited verification, validation, or calibration;
- a lack of transparency and disclosure about the tools being used; and
- limited or no technological competence in the officers and advocates of the court.

2.3 Algorithmic Bias and AI risk assessment tools

In the era of big data, AI and algorithms, risks assessments are as good (or as bad) as the data used in training the system. The lingo of "garbage in, garbage out" is well known in the field of computer science: if faulty input is fed into a computer program, it similarly and inevitably regurgitates faulty output. In the AI risk assessment lexicon, this lingo can be modified to "bias in, bias out": feeding biased data into AI tools will inevitably result in the tools generating biased outputs.

Algorithmic risk assessment is not bias-free. There are generally three sources of bias which are introduced into AI-enabled tools.

First, an AI tool may be deliberately designed to produce desired outcomes. This can take many forms, including by setting objective rates for approval or disproval. To achieve such goals, AI software may be engineered or trained to achieve the desired ends, and which doesn't necessarily reflect requirements of law or apply the correct legal standard (setting aside the issue of whether it is appropriate for AI systems to act as *de facto* adjudicators at all).[25] Furthermore, there may be great variation in how humans interpret and apply risk scores. For instance, some US criminal court jurisdictions interpret a high-risk score as requiring the accused to remain in custody. Other jurisdictions may interpret the same score as indicating the person is suited for release but with necessary supports like housing, income support, and access to social worker assistance.[26]

Second, unintentionally biased data may be used to train computer algorithms to make predictions. A good example is when historical data are used to train a machine learning algorithm. The issue is that such data could well be tainted by various factors which, though legal at the time the data were collected, have ceased to be legal (or even become illegal) as a result of legal or policy changes aimed at addressing the overrepresentation of certain groups in the criminal justice system.[27]

Third, an AI tool may be trained on data that are responsive to or linked to unique factors in a particular environment but then deployed for use in a different environment for which that data is inappropriate.[28] Both this case and the second case above would generally result in implicit bias.

A study by American investigative publication *ProPublica* exemplifies the tendency of algorithmic risk assessment tools to perpetuate existing racial bias and stereotypes in society.[29] (See also the sidebar above, "Risk assessment in the age of AI: the case studies of Zilly and Loomis" for more of the backstory and human impact).

The study focused on recidivism risk predictions by COMPAS, one of the most widely used AI-based risk assessment tools in the U.S. criminal justice system. In addition to raising doubts about the accuracy of predictions made by this tool, the study raised even more serious concerns about the racial bias evident in COMPAS risk predictions.[30]

The study revealed that COMPAS not only falsely assessed Black defendants as future criminals, but the AI tool did so at "twice the rate as white defendants."[31] In fact, white defendants were more often misclassified as "low risk" than Black defendants.[32] Thus, the study from *ProPublica* seems to establish that the use of COMPAS in risk assessment more often results in white defendants getting an unfair pass, while Black defendants, in contrast, more often get an unfair penalty.[33] Yet COMPAS software still remains a dominant risk assessment tool in the U.S. criminal justice system.

The tendency of AI risk assessment tools to produce results biased against people of colour has been referred to as "algorithmic racism," defined as "systemic, race-based bias arising from the use of AI-powered tools in the analysis of data in decision making resulting in unfair outcomes to individuals from a particular segment of the society distinguished by race."[34] Algorithmic racism may indeed result from the use of historical data collected from an era of biased criminal justice that is then used to develop or train AI technology for risk assessment, as suggested above.

Canada has had its own share of biased criminal justice, which has seen minority communities over-represented in the carceral system and law enforcement practices that unfairly target these communities. This includes a history of discriminatory profiling through the practice of "carding" or "street checks" by some major police departments in Canada. The practice was highly criticized for unfairly targeting young Black and Indigenous people.[35] Thus, it is important to identify the extent to which algorithmic risk assessment tools built on AI technology may reinforce implicit and explicit bias against minority groups, especially Black and Indigenous offenders who constitute a disproportionate population in the Canadian criminal justice system.

2.4 Consultation questions

1) Assessments and predictions about risks, public safety and other factors are not new. However, AI-enabled risk assessments bring new complications, such as a lack of verification, calibration, and certification; technological deference where humans are over-reliant and uncritical about AI-generated recommendations; and other factors. Given this, what weight should jurists assign to AI-enabled prediction? How is this similar to or different from other traditional risk assessment tools?

3. Key Concerns, Issues and Questions

3.1 Bias in the training, development and use of AI risk tools

3.1.1 Current critiques of AI and risk assessment bias

It is logical that an AI risk assessment cannot be better than the data used to train or develop the tools used in the assessment. Nevertheless, it is solely the private commercial actors in the business of AI tools development who decide what data are used to train an AI risk assessment tool. This training process may unfold with little to no input from criminal justice actors who are charged with the responsibility of protecting public interest and criminal justice subjects. Without question, the decisions of these private businesses will significantly inform how the AI tools function, including the outputs they produce.[36]

This lack of input by key players in the criminal justice system is a critical issue. As was noted by Brauneis and Goodman, these private entities effectively assume public office without accountability, while potentially withholding critical information from government and public agents who *are* accountable to the public.[37]

Importantly, individuals from minority communities are disproportionately represented in data collected from discriminatory carceral and law enforcement practices, thus falsely implying that those communities are more prone to crime. Problems then arise, as an AI tool trained on such data will inevitably regurgitate the bias and stereotypes implicit in this data. Such bias becomes even more blurred in AI risk predictions because of many people's false belief that technology is race neutral and colour blind.[38]

Algorithmic bias also arises where an AI tool developed and trained on data from one predominant group is deployed for use on another group that is not adequately represented in the training data. Facial recognition software is one technology that has demonstrated this problem.[39] Although AI risk assessment tools have yet to be deployed in the Canadian criminal justice system, the SCC case of *Ewert v. Canada*[40] clearly illustrates this problem.[41] In *Ewert*, the SCC noted that the cross-cultural application of risk assessment tools would result in "cultural bias."[42]

The cultural bias issue identified in *Ewert* relates to the more general lack of knowledge in the criminal justice system that AI risk assessment tools are not, in fact, a "one size fits all" tool. Several types of recidivism risk assessments exist in the criminal justice system: pretrial recidivism, general recidivism, violent recidivism, sexual recidivism, and so forth. Developers create tools that may be unique to one of these diverse risk assessment types, which adds yet another layer to this complex landscape.

The Zilly case demonstrates this risk. At trial, COMPAS's creator Tim Brennan testified that he never designed the tool for use in court or in sentencing decisions.[43] It is therefore important that judges who seek to use an AI risk assessment presented to their court ensure the assessment was generated from an appropriate AI tool – which means one that was designed to assess risks unique to that phase of the criminal justice system and, importantly, independently validated as safe, reliable, and suited to purpose.

In sum, deploying AI tools for use in an environment different from those for which they were originally and purposefully designed will result in biased and inaccurate predictions of actual risks posed by subjects in the criminal justice system. If the tool generates a flawed low risk score, this will put public safety at risk since this could result in the release of high-risk accused/criminals into the community. On the contrary, if the tool generates a flawed high-risk score, it will result in over-incarceration and thus deprivation of the *Charter*-protected personal liberty of subjects in the criminal justice system.

3.1.2 Consultation questions

2) Given the significant influence of private commercial actors in the development of AI risk assessment tools, what policies can be implemented to ensure a transparent process involving criminal justice stakeholders, aiming to safeguard public interest and improve the reliability and fairness of these tools?

3.2 Navigating disclosure, trade secrets, and intellectual proprietary rights

3.2.1 Assertions of intellectual property rights undermine disclosure

Another significant issue associated with using AI risk assessment tools in the criminal justice system concerns their proprietary nature, as the operational methodology of these AI tools is often a closely guarded trade secret. This is especially the case when the tools are designed by commercial for-profit corporations, which have numerous commercial reasons to restrict access to the operational methodologies of their tools.

However, this lack of access raises serious issues relating to transparency, an aspect vital to the fair administration of criminal justice. Without this transparency, the accused, the prosecutor, and even the courts are deprived of access to this pivotal information, as the factors that contribute to the assessment scores are obscured, along with how much weight is attached to each of them.

In Canada, our criminal justice system relies heavily on the work of defence counsel to scrutinize the prosecution's case as a means to safeguard the offender's Charter rights. These rights arise at the trial, sentencing, and post-sentencing phases of the system.[44] Since the imposition of a criminal sentence involving incarceration could result in the deprivation of the offender's right to personal liberty, such deprivation must be in accordance with the law and must follow a process that is procedurally fair. As such, serious *Charter* issues could be implicated when an offender who is challenging a sentence seeks access to the proprietary information inherent in the AI risk tools that were among the factors shaping the judge's sentencing decision. Such a legal challenge foregrounds the conflict between the offender's *Charter* right and the proprietary right of a corporation to maintain its trade secrets.

An alarming example arises in the US case of *Loomis* case.[45] In that case, the Wisconsin Supreme Court ruled that the court's use of algorithmic risk assessment generated by the COMPAS tool in imposing a six-year sentence on the accused did not violate the accused's due process right, even though he was denied access to the proprietary methodology used to arrive at the assessment that led to the sentence.

Given the black box nature of the tool, the judge, the prosecution and the accused all lacked any knowledge of how the algorithmic tool arrived at the numerical estimate. The defence counsel also had no ability to access and examine (or cross-examine) the methodological information in these proprietary tools—representing a further danger.[46] The fact that the judge would, in absence of this knowledge, rely on the assessment in imposing a sentence on the accused underscores the extent to which the criminal justice system risks relinquishing vital judicial functions to data scientists and software engineers hiding behind black box algorithms.

A second concerning example is the US case of *People v. Chubbs.*[47] In this case, an accused who was convicted and sentenced to death was denied access to proprietary information relating to the operation of a forensic software used to convict him because the developer asserted trade secret privilege over the software. The judge at the trial court had ordered the disclosure of the proprietary information subject to a protective order on the ground that failure to disclose the information would result in the accused being denied his "right to confront and cross-examine witnesses."[48] However, the developer successfully appealed the order on the ground that the proprietary information was protected under a statutory trade secret privilege.

Chubbs is now cited by prosecutors and criminal justice technology developers to justify withholding proprietary information from defendants in criminal proceedings.[49] To address this issue, proposed legislation entitled the *Justice in Forensic Algorithms Act* of 2021, was tabled in the US Congress.[50] Section 2(b)(1) of the proposed legislation clearly provides that "[t]here shall be no trade secret evidentiary privilege to withhold relevant evidence in criminal proceedings in the United States courts."[51]

3.2.2 Addressing conflicting rights: the need for a framework

The Canadian legal context differs somewhat from the American one. It is helpful to review the leading law, contrast it with the American approach, and consider how a lack of vigilance, or the uncritical reception of otherwise unregulated technology, can quickly work to upend fundamental civil liberties and other rights.

At least one case exists in which the SCC upheld the right of offenders to access proprietary computerized risk assessment tools: *May v. Ferndale*.[52] The appellants in *Ferndale*, who were inmates serving life sentences in minimum-security correctional institutions, were involuntarily transferred to a medium-security facility following a reclassification of their security rating by the CSC. The CSC had used a computerized risk tool – the Security Reclassification Scale (SRS) – in its review of their security classification.

Ultimately, the SCC ruled that the common law duty of procedural fairness required that the inmates to be given access to the proprietary SRS scoring matrix used to make the decision.[53]

However, the SCC made an important distinction. It ruled that the criminal disclosure standard in R. v. *Stinchcombe* (which is higher than the common law standard) was not applicable as it applied only when the accused innocence was at stake.[54] In *Ferndale*, the appellants had already been convicted and sentenced. This ruling implies that the *Stinchcombe* disclosure rule may not apply during the sentencing stage, when a convicted offender seeks access to algorithmic information used in computing or assessing the impugned sentence, as was the case in *Loomis.*[55]

Ferndale is also helpful as the court further held that a statutory duty of disclosure also applies. The duty in this case arises in the *Corrections and Conditional Release Act*, which generally obligates any person or body taking a decision affecting an inmate, within a reasonable time before the decision is to be made, to give the offender "all the information to be considered in the taking of the decision or a summary of that information."[56]

Ferndale contrasts with the approach taken in the US case of *Loomis* case, where the court held that a denial of the offender's access to inner workings of the tool could be justified by the offender's knowledge of the information used in the risk assessment, as well as the opportunity afforded him to deny or explain away any inaccurate information before they are processed by the algorithmic tool. Conversely, the SCC took the position in the *Ferndale* case that offenders' knowledge of the information contributing to the assessment and their opportunities to modify that information at the information-gathering stage (via interviews, questionnaires, and so forth) were insufficient; they were entitled to know not only the factors taken into consideration by the computerized tool, but also the values assigned by the tool to those factors and how the tool generated its final score.[57] Significantly, the SCC did not take issue with the CSC's use of the computerized tool in risk assessments of inmates in its correctional facilities; rather, it was that inmates were being deprived of access to vital information about the assessment tool that was problematic.

Nothing in *Ferndale* particularly suggests that the CSC refused to disclose the SRS formulas and methodology required to generate the classification specifically because it sought to protect any proprietary trade secrets. Still, it is important to note that the SRS scoring formulas and methodology *are* core proprietary information. Thus, the SCC's decision in this case leaves no doubt that where access to algorithmic information is necessary to preserve the offenders' *Charter* rights, even if it is proprietary in nature, the *Charter* right would and should rightly transcend any commercial interest in the proprietary information.

Furthermore, since the SCC applied the relatively low common law standard to their decision in *Ferndale*, situations that warrant the application of the much higher *Stinchcombe* standard of disclosure[58] would inevitably weigh even more in favour of disclosure and not protection of the proprietary information.

Shortly after the decision in *Ferndale,* a case relating to the confidentiality of risk assessment tools came before the Saskatchewan Provincial Court in *R. v. B.H.D.*[59] While the information relating to the risk assessment was disclosed to the defendant in that case, the Crown, acting on the interest of the risk assessment tool developer, sought an order sealing public access to all information relating to the tool in the court record. The court judge declined to make the sealing order but rather agreed to put a note in the court file requiring notice be served on the Crown where an *ex parte* application is made for access to the record.[60]

The few Canadian cases that exist in this area suggest that the Canadian courts – unlike those in the U.S. – will be more inclined to allow access to proprietary information in AI risk assessment tools when the *Charter* rights of an individual subject to the criminal justice system conflict with the proprietary rights of a commercial corporation. Thus, it is important for commercial corporations getting into the business of AI risk assessment tools in the Canadian criminal justice market to be fully aware of this position. Their entry into the Canadian market implies consent to Canada's higher risk of disclosure of proprietary information in criminal proceedings.

Additionally, government agencies seeking to use proprietary AI risk assessment tools should proactively include provisions in the licensing agreement with the developers to deal with such disclosures where they are made or ordered by the court in criminal proceedings. This will prevent a situation where such government entities get into the dilemma of having to comply with a court ordered disclosure despite a non-disclosure contractual term in their licensing agreement with a private developer of a risk assessment tool.

3.2.3 Consultation questions

3) How can the criminal justice system balance the need for transparency and the fair administration of justice with the proprietary rights of commercial corporations that design AI risk assessment tools, ensuring that all parties involved in a legal matter have access to and understanding of the methodologies behind these tools?

4) Given the Supreme Court of Canada's stance that access to proprietary information is necessary to preserve *Charter* rights, what legal frameworks or guidelines should be developed to guide commercial corporations entering the Canadian criminal justice market regarding the disclosure of proprietary information, especially in situations where such disclosure may be crucial to ensuring a fair trial and upholding the rights of the accused?

3.3 Assessing predictive accuracy

The accuracy of the predictions made by AI risk assessment tools presents another important issue that merits consideration with respect to their use in the criminal justice system; unquestionably, poor accuracy inevitably raises questions about the validity of using these tools at all. This also points to the broader issue of reliability as a matter of the law of evidence. Hence, the court in *B.H.D.* noted the following:

> Unless there is a clear admission, any fact regarding a risk assessment, if it is to be relied upon by a Court in sentencing a […] person, must not be used as a matter of law unless it has met the threshold of relevance or reliability.[61]

In this case, the actuarial tool used had assessed the offender as "high risk," with a 70% likelihood of reoffending in the next two years. However, a re-assessment of the same offender by a human expert challenged this actuarial prediction, as the human expert's assessment yielded a 52% likelihood of reoffending in the next two years – 18% lower than the actuarial tool.[62] This gap raised critical questions about the reliability of the tool's predictions; in this case, this resulted in the court ditching the tool's assessment. This scenario suggests that judges would be wise to be cautious in admitting AI evidence, which may only be as accurate as an evidentiary coin toss.[63] Thus, whenever the state seeks to use AI-generated risk scores in any part of a criminal proceeding, it should be responsible for the evidentiary burden of establishing the accuracy and reliability of the chosen tools to generate evidence.[64]

The reliability of risk assessment tools has been a focus of research and academic discussions in many literatures. Much of the research cites inaccuracy in the tools' predictions, particularly evident along racial and gender lines.[65] Validation data for COMPAS and LSI-R risk assessment tools have shown that both tools provide recidivism scores with inconsistent validity when tested on different ethnic/racial populations. For example, African Americans were more likely to be overclassified – that is to say, predicted to be rearrested when they actually were not – than Caucasians or Hispanics across all predictive measures.[66] This was further corroborated by a *ProPublica* study and a subsequent study by Dressel.[67]

The validity of a risk assessment tool is an important aspect of its reliability. To assist in addressing validation problems related to the use of software in the criminal justice system, including AI software, Abebe *et al.* propose a robust adversarial testing mechanism. They identified three current validation mechanisms and their limitations:[68]

- *Source code review*: This review is conducted *by the defence counsel* to help determine the validity of the evidentiary software and to identify programming errors. However, this has limited value since merely reviewing the source code without testing the software may not reveal vital information, such as the accuracy or error rate in the prediction made by the software.[69]
- *Validation studies or peer reviews of the tools*: These are conducted *by relevant scientific committees or scholars* to help assess the accuracy of the tools. This mechanism has limitations, however. For example, if the independence of the committees or scholars is questionable or unclear, this can undermine the authenticity of their findings about the tools – such as when they have some financial or other disqualifying affiliations with the developers of the tools.[70] To be reputable, validation studies must therefore be conducted by committees or scholars that are truly independent, with no vested interest in particular study outcome.
- *Direct testing of the software tool:* This testing involves the defence counsel, through their expert, gaining access to the executable source code, selecting the input relevant to the case of its client, and running the software to assess the outcome generated. Abebe et al. noted the current lack of guidance available to the defence counsel to conduct such tests.[71] It is also important to note that because of the technical nature of these software programs, defence access to the professionals needed to test the software may be costly and out of reach, especially for indigent clients.

In the U.S., the principles in the proposed *Justice in Forensic Algorithms Act,*[72] which was tabled before the U.S. Congress in 2021, could be fittingly applied to AI risk assessment software. The proposed legislation provides for establishing Computational Forensic Algorithm Testing Standards and a Computational Forensic Algorithm Testing Program. The standards would be used to validate algorithmic software used in the criminal justice system: "standards shall include an assessment for the potential for disparate impact, on the basis of race, ethnicity, socioeconomic status, gender, and other demographic features," and would address, among other concerns, the need for testing the software, including a system to report the accuracy and error rates of the software.[73] The proposed legislation further enables several key pieces to be disclosed to the defendant: the results of the software's algorithmic analysis, an executable copy of this analysis showing both the source code and the results, and relevant files and data used by the software.[74]

As discussed in the LCO's paper ***Introduction and Summary: The LCO AI in Criminal Justice Project***, Canada's proposed AI legislation, the *Artificial Intelligence and Data Act*, would require "high risk" uses of AI to comply with a set of disclosure requirements.[75] However, as of second reading in Parliament, the legislation does not specifically:

- identify "criminal risk assessment" as a "high-risk" situation;
- concretely define how such AI may be assessed or certified for validity or reliability;
- detail transparency and disclosure requirements; or
- establish a set of assessment and disclosure requirements specific to the grave risk to human rights and civil liberties inherent in a criminal prosecution.

The lack of such a governance framework suggests that such tools will not only be met with scepticism in a criminal proceeding, but may not be able to be used efficiently or reliably without regular challenge. Other papers in the LCO series compare this state of affairs to the efficient and routine use of other well regulated technologies, such as breathalyzers, which are subject to testing, certification and user training regimes that make their use transparent, efficient, and more reliable.[76]

3.3.1 Consultation questions

5) Where the prosecution in a criminal proceeding seeks to introduce evidence from an AI-risk tool, should a burden be imposed on the prosecution to lead evidence relating to the reliability and validity of the AI-tool? Should similar burden be imposed on the defence where it seeks to use AI-risk assessment evidence as a mitigating factor?

3.4 AI-enabled risk assessment tools as expert evidence

3.4.1 How do courts characterize risk assessments as expert evidence?

While algorithmic risk scores by AI tools can prove useful in risk assessment in the criminal justice system, the process that generates the risk scores must be open, transparent, and subject to evidentiary scrutiny. Relevance and reliability are the bedrock of admissibility in the law of evidence, and the closer the evidence is to what might be considered an expert opinion, the more stringent the requirement for reliability. Justice Sopinka rightly noted in *R. v. Mohan*:

> [I]t appears from the foregoing that expert evidence which advances a novel scientific theory or technique is subjected to special scrutiny to determine whether it meets a basic threshold of reliability and whether it is essential in the sense that the trier of fact will be unable to come to a satisfactory conclusion without the assistance of the expert. The closer the evidence approaches an opinion on an ultimate issue, the stricter the application of this principle.[77]

The Saskatchewan Provincial Court in *B.H.D* categorized risk assessment data as "expert evidence."[78] It found that risk scores, as evidence before the court, should be placed on the same pedestal as opinions by experts in a criminal proceeding. If a human expert were to tender evidence relating to the risk posed by an offender in the criminal justice system, such evidence would be subject to all the safeguards and scrutiny for the admissibility of expert evidence.

Justice Turpel-Lafond in *B.H.D*[79] referenced the Supreme Court of Canada decision in *R. v. Mohan,*[80] noting the following:

> *[R]isk assessment data is information which would fall into the category of "expert evidence," whether adduced by the Crown or Defence. If a party seeks to provide the Court with a validated prediction as to a level of risk to re-offend then this evidence would need to meet the expert evidence rules which are well established in the criminal law area.*[81]

According to the decision, there is no reason why same evidence coming from an AI tool should be subject to lesser safeguards or scrutiny. Elevating the requirement for the admissibility of evidence from AI-generated risk scores in the criminal justice system is fundamental to protecting the right of vulnerable members of society, especially when they risk being deprived of their personal liberty rights by an all-powerful state and its agents.

At the same time, while the Saskatchewan Provincial Court took the position that risk assessment scores fell under the category of expert evidence, other courts are yet to follow. This includes several legal distinctions with AI and expert evidence that merit more detailed consideration. The process and potential issues for having AI-generated risk assessments admitted as expert evidence are discussed below.

3.4.2 Does AI produce "opinions?"

Expert evidence is comprised of opinions. An opinion in evidence law is an "inference from observed fact."[82] This involves:

> "[…] inductive reasoning, which derives conclusions based on the uniformity of prior human experience. The conclusion is not inherent in the offered evidence […] but flows from an interpretation of that evidence derived from experience [.... I]f the premises, or the primary facts, are accepted, the inductive conclusion follows with some degree of probability but not of necessity."[83]

A basic analysis of an algorithm's process and production of a risk assessment may meet this definition of "opinion." A risk assessment algorithm is given as much information as possible about the defendants but is not directed as to what factors humans think "correlate best with failure in the pretrial phase." Instead, the algorithm "work[s] its magic," and, with the data it's been provided, "figure[s] out on its own" what makes a given defendant high or low risk to not attend court.[84]

Ultimately, the algorithm extracts "patterns in a massive amount of data," and in doing so engages in "inferential reasoning" in each layer.[85] The algorithm's outputs are "generated by correlating information and recognizing patterns from past events or data with new data to forecast the likelihood of an event or instance occurring in the future – meaning AI models offer probabilities and carry inherent uncertainty."[86] Fundamentally, the algorithm's outputs are predictions.[87]

These "predictions" are "not proofs." When AI processes and "thinks" about how historical data informs new events there will always be a level of uncertainty or error rate, as with humans.[88]

These descriptions give rise to a possible analogy between the algorithm's output prediction and the human use of inductive reasoning to express an opinion. It may be argued that the human "interpretation" of evidence derived from prior experience is akin to the algorithm's correlation of information and recognizing patterns in the data it's fed – the algorithm's own "interpretation" of "prior experience." The human "interpretation" of evidence, derived from experience, forms a conclusion which follows with a degree of probability and not necessity. Similarly, the algorithm uses its interpretation of information – derived from its correlation of data and pattern recognition – to forecast a probable outcome which is not a certainty. Therefore, it may be argued that the algorithm's output or prediction is the product of inductive reasoning – it is also an inference drawn from facts. Thus the algorithm's output potentially meets the forensic definition of opinion.

Why is characterizing the algorithm's output as "opinion" important?

It is the trier of fact who is entitled to draw inferences from facts. Witnesses are generally not permitted to testify as to inferences or opinions that they draw from facts.[89] Thus, if the algorithm's risk assessment score is indeed some form of an opinion, it may be presumptively inadmissible on this basis.

However, in some cases judges or juries may not have "special knowledge or experience" required to understand some information.[90] In these cases judges and jurors may not be "equipped to draw true inferences from facts stated by witnesses." Therefore, in such cases a witness is "allowed to state his opinion about such matters, provided he is expert in them."[91] Where the "judicial admissibility control process" is satisfied, the expert's "ready-made factual inference […] drawn from a body of facts" may be left with the trier of fact.[92]

As indicated above, there has been judicial recognition that risk assessment evidence is expert evidence that should be subject to the same admissibility rules as expert opinion evidence.[93]

Therefore, if the risk assessment from the algorithm is classified as a form of expert opinion evidence, then where the Crown seeks to tender it at sentencing the Crown must also satisfy the common law requirements for its admissibility.[94] The Crown must thus persuade a court that algorithmic risk evidence meets all of the admissibility requirements for expert opinion evidence set out in *White Burgess Langille Inman v. Abbott and Haliburton Co.*[95] This proceeds in two steps: analysis of factors for assessing admissibility, and then determining if the benefits of admitting the evidence outweigh the risks associated with it.

At the first step of the analysis, the proponent of the evidence must establish the threshold requirements of admissibility. These are the four *Mohan* factors:[96]

- Relevance;
- Necessity;
- Absence of an exclusionary rule;
- A properly qualified expert.

At the second step, the judge balances the potential risks and benefits of admitting the evidence in order to decide whether the potential benefits justify the risks. This balancing has been described as the trial judge deciding "whether expert evidence that meets the preconditions to admissibility is sufficiently beneficial to the trial process to warrant its admission despite the potential harm to the trial process that may flow from the admission of the expert evidence."[97]

Defining algorithmic risk assessment evidence as expert opinion evidence may be critically important on a procedural level. A key concern with algorithmic risk assessment evidence has been the frustration that many defence counsel have endured in attempting to litigate its admission. Because of issues relating to disclosure, time, energy, or expertise they cannot effectively challenge this evidence. Further, the "system is designed at every step to keep litigants from getting to the information needed to raise the issues appropriately."[98]

But characterizing algorithmic risk assessment score as expert opinion evidence means that if the Crown seeks to admit it, then it is the Crown who must satisfy the *Mohan* and *White Burgess* criteria. This removes the onus on the defence to prove the problems with the algorithmic risk assessment score; it instead falls on the state to exert resources to establish the forensic reliability of this evidence.

The sections that follow explore how the use of AI risk assessments, characterized as expert opinion evidence, fit into the *Mohan* and *White Burgess* framework.

Case Study: How are AI risk assessments characterized and contested in a bail hearing?

A key consideration in these cases concerns the practicalities in contesting AI-related evidence in context of existing norms in bail or sentencing practices. To review several case study scenarios illustrating these practical challenges, please see LCO AI in Criminal Justice Project ***Annex B, Project Case Studies***.

3.4.3 Does AI expert evidence meet the thresholds of logical relevance and necessity, or engage an exclusionary rule?

Assessing Relevance

Evidence is logically relevant and material if, as a matter of logic and human experience, it tends to make a fact in issue more or less likely. Expert evidence that does not meet this threshold is inadmissible.[99]

There have been concerns raised over algorithmic risk assessments' accuracy. For example, someone who "has molested a small child every day for a year" could be identified as "low risk because he probably has a job," while an alcoholic "will look high risk because he's homeless."[100] Discrepancies such as these may cloud the evidence's tendency to demonstrate an offender's dangerousness. This may in turn put its logical relevance in doubt.

Further, an understanding of what precisely the algorithmic risk assessment score predicts may raise another question about its logical relevance. Risk assessment tools purport to predict future crime, but in fact generally predict future arrest.[101] This is because the dataset usually fed into the algorithm does not necessarily indicate with certainty whether a person has actually committed crimes in the past. Most crimes are not reported, some are reported falsely, and sometimes crime reports do not properly identify criminal perpetrators.[102] A "record" of past crimes is "really a record of crime reports and law enforcement actions, and the relationship of that record to actual crimes committed is opaque."[103]

Therefore, a closer analysis of the risk assessment's accuracy and what it is actually measuring – a likelihood of re-arrest – may raise doubt as to the score's tendency to actually demonstrate the likelihood of the accused re-offending. These may be issues to consider in determining whether the evidence meets the threshold for logical relevance under this prong of the *White Burgess* criteria.

Assessing Necessity

Expert opinion evidence is necessary where the expert deals with a subject that ordinary people are unlikely to form a correct judgement about without assistance. The party tendering the expert evidence must show that it is necessary. If a judge can form their own conclusion on the facts without help, then the opinion evidence from the expert is not necessary.[104] Evidence is not admissible simply because it may be helpful.[105]

Crucially, several studies suggest that AI risk assessments do not generate more accurate predictions than humans. A January 2018 study found "no evidence that algorithms were more accurate in predicting recidivism than human beings."[106] Earlier studies characterized risk scores assigned to over 7,000 people arrested in Broward County, Florida in 2013 and 2014 as

"remarkably unreliable […] forecasting" that was only slightly more accurate than a coinflip.[107]

Given these observations, an issue arises as to what extent the algorithm's risk score assists a sentencing judge to form a correct judgement about the offender before the court. As "helpfulness" is insufficient to meet this threshold, a question may arise whether this evidence is actually "necessary."

The absence of an exclusionary rule

Expert opinion evidence cannot be admitted if it breaches another rule of admissibility.[108] This paper only raises suggested characterizations of algorithmic risk assessment evidence. The definition of this evidence remains an open question. Further study and litigation over this evidence may raise other exclusionary concerns that may preclude admission as expert opinion evidence or otherwise.

3.4.4 Can AI be properly qualified as an expert?

Under the "properly qualified expert" prong of threshold admissibility, *White Burgess* articulates another consideration that the tending party must meet: the expert must be fair, objective and non-partisan, and aware of their duty to assist the court. Experts should also possess both the knowledge and expertise needed, and have the independence and impartiality needed. If the witness is unable or unwilling to fulfill the duty, they do not qualify to perform the role of an expert, and the evidence should be excluded.[109]

The knowledge and expertise element

Expertise requires "special knowledge and experience going beyond that of the trier of fact" in the matter at hand. The special training or experience needed to acquire, comprehend, or use such information need not be acquired through formal training or education. It must, however, reflect "systematic learning" that goes beyond mere anecdotal observation, transient personal experience, or modest study.[110] Whether a proposed expert has demonstrated a "systematic" assessment of the data is also relevant to properly qualifying a witness as an expert.[111]

It may be argued that the algorithm can do what a normal trier of fact cannot do. An algorithm may well take into account upwards of 100 predictors or factors which may have varying associations with re-offence or failing to attend court. [112] It is understood that the algorithm can learn "from millions of observations [… and] make predictions and learn simultaneously."[113] The machine learning algorithm can "reveal correlations and patterns that the judge was not expecting or was not able to see on her own."[114] On this basis, at least initially, the algorithm may demonstrate it has a special knowledge or experience beyond that of the trier of fact.

However, whether the algorithm – as the "expert" – can demonstrate "systematic learning" and a "systematic assessment of the data" is not clear. Ideally the defence should be able to review the training data, which would provide an opportunity to identify potential biases built into the system, and the source code itself which provides details of how the system works.[115] However, given that many of these algorithms are proprietary in nature and developed by private companies, disclosure of these items has been resisted and third-party reviews of the systems – even by other expert witnesses – have been prohibited by the vendor.[116]

In any event, the disclosure of this information may be of limited assistance in determining whether the algorithm is demonstrating "systematic learning" and a "systematic assessment of the data." Recall the earlier description of the algorithm "working its magic."[117] Some "unsupervised algorithms operate like a black box; they produce a score from a combination of hundreds of factors without the ability to tell how the score was generated."[118] These algorithms "develop their own decisional rules which are usually not intelligible to humans," in a manner that is "non-linear."[119] Some algorithms are "constantly evolving as new data is fed into the system. Consequently, even the computer programmers who built the algorithms are frequently in the dark regarding the specific procedures through which the algorithm achieves a given result."[120] The inability to appreciate the algorithm's "black box" process – how it learns and then makes reasoning decisions based on that learning and ultimately provides a score – is concerning in the sentencing context.[121]

Further, a court's ability to assess proof of "systematic learning" or "systematic assessment of the data" may also be frustrated as the algorithm cannot be subjected to cross-examination. As will be discussed further below, the algorithm cannot be questioned by the Crown, defence counsel, or the Court to explain itself. It is unclear how the Crown calling a human witness to explain the algorithm's "thought process" or methodology would advance this inquiry, when the computer programmers who built the algorithm themselves are "in the dark" about how the algorithm makes its decisions.

The point of the expert opinion evidence framework is to ensure that "the trier of fact maintains the ability to critically assess the evidence," and to "ensure that expert evidence enhances, rather than distorts, the fact-finding process."[122] The trier of fact may have difficulty in assessing or scrutinizing the algorithm's process to determine evidence of "systematic assessment of the data" or "systematic learning" due to the algorithm's opacity. This may raise another issue with respect to its admissibility.

The independence and impartiality component

The expert's opinion must be impartial in that it reflects an objective assessment of the questions at hand. It must be independent in the sense that it is uninfluenced by which side retained them. It must be unbiased in the sense that it does not unfairly favour one party's position over another. Overall, "the acid test" is whether the expert opinion would remain the same, regardless of which side retained them.[123] This will be assumed unless the opposing party shows "a realistic concern that the expert's evidence should not be received because the expert is unable and/or unwilling to comply with the duty."[124]

At this stage there are concerns that risk assessment tools are a "technology of governmentality" that forms part of a "culture of control"; individuals who are identified as "risky" are controlled through incapacitation.[125] To that end, risk algorithms have been described as "value-laden," since "in designing the operational perimeters [of the algorithm…] it is not uncommon for developers to have desired outcomes in mind that privilege some values and interests over others."[126] Therefore, the possibility has been raised that privately developed technology sold for government use may cater primarily to those customer interests instead of broader public ones.[127]

Given the infancy of this technology in Canadian criminal law, the AI risk assessment's compliance with the independence and impartiality threshold may be better addressed after further litigation or technological development. Perhaps eventually third-party proprietary concerns will be overridden or discarded, and technological advancements can assist with better uncovering the algorithm's processes, unveiling any potential built-in biases or partiality.[128]

3.4.5 AI and the threshold of reliability for novel and contested science

White Burgess defines a further consideration applicable at the threshold stage: where an opinion is based on novel or contested science, or for science used for a novel purpose, the reliability of that underlying science will be questioned.[129] This applies to any "expert" technique or theory, whether or not it is grounded in science in the conventional sense; if the technique or theory is "novel," these rules will apply.[130] Evidence that does not meet these threshold requirements should be excluded.[131]

As indicated above, some studies have called into question the reliability of AI risk assessment tools. The ability to evaluate the reliability of AI risk assessment tools according to this standard may also be limited by the opacity or lack of explainability of some algorithms' "black box" processes, as discussed above.

Further, a central consideration on this threshold is not whether a technique is new within its own field or discipline, but rather whether it is "novel" to courts. As noted in *R. v. Trochym* (citation omitted), "there is a difference between reliability for the purposes of a profession and sufficient reliability for use in a court of law. What is being tested by the novel science doctrine is forensic reliability."[132]

Therefore, evidence of the successful use of an algorithm in, for example, credit card approval or car insurance approval may not assist at this stage of the framework. The Crown must demonstrate the algorithm's "forensic reliability," its "sufficient reliability for use in a court of law." Although an algorithmic risk assessment was used In *Loomis* and the Wisconsin Supreme Court declined to interfere with the original sentencing decision, the court still noted that the tool was a "poor fit" at sentencing.[133] This is hardly an enthusiastic endorsement approving the algorithm for forensic use in the criminal sentencing process.

3.4.6 The discretionary gatekeeping stage: weighing risks and benefits of admitting evidence

Even where the basic threshold is met, the judge must still engage in a "gatekeeping stage." The above requirements remain part of a "sliding scale" which continue to play a role in weighing the overall competing considerations in admission. Ultimately the judge must be satisfied that "the potential helpfulness of the evidence is not outweighed by the risk of the dangers materializing that are associated with expert evidence."[134]

Assessing the "helpfulness" of admitting AI evidence

The "helpfulness" of this evaluation requires a consideration of the probative potential of the evidence and the significance of the issue to which the evidence is directed. When looking at potential probative value, the reliability of the evidence must be considered, which requires a consideration again of the methodology used.[135]

As has been raised earlier, concerns remain about the reliability of algorithmic risk assessments, along with concerns about understanding their precise methodology.[136] These concerns may serve to diminish the risk assessment score's potential probative value.

Further, risk assessments may be found to have less probative value during sentencing because a sentencing hearing is not meant to be an exclusive inquiry as to an accused's future risk. Instead, a sentencing hearing seeks to impose a "just sanction"[137] by taking into account what has already happened. The "fundamental principle" of sentencing is that "[a] sentence must be proportionate to the gravity of the offence and the degree of responsibility of the offender."[138]

Evidence of re-offence risk may be relevant to other sentencing principles, such as rehabilitation[139] or a need to separate offenders from society.[140] It may be relevant to probation conditions and length. However, the significance of the risk of future re-offence cannot displace or circumvent the "fundamental principle" governing sentencing, which primarily looks at the offence that has occurred and the offender's individual history in assessing their degree of responsibility.

If addressing this "fundamental principle" is the central issue at a sentencing hearing, then algorithmic risk assessment evidence may take on a slightly diminished significance. In conjunction with potential issues regarding its reliability, the benefit of admitting this evidence may be mitigated at the gatekeeping stage.

Assessing the "risk of dangers" of admitting the AI evidence

Possible prejudicial effects of expert evidence could include excessive time consumption, diverting attention from the real issues in the case, or the inability of a party to deal with expert evidence tendered by the other party who enjoys a resource advantage. Further, if the evidence is inflammatory or invites stereotypical reasoning, this also increases the costs of its admission.[141]

It may be years before the question of AI risk assessment admissibility comes before an appellate court that issues a conclusive and binding judgement on how this evidence is to be received. Absent that appellate direction, admission of this evidence may repeatedly be litigated in lower courts where the Crown tenders this evidence regularly at sentencing or on bail.

This raises several possible prejudicial effects. The practice may result in a significant consumption of time required to litigate the admission of this evidence in what may be an otherwise routine sentencing or bail hearing, particularly where adjournments will be required to secure available disclosure.

Further, if defence counsel or duty counsel are going to be tasked with defending against the admission of this evidence, even in those routine matters, a question arises about the apportionment of resources to do so. Even though the onus remains on the Crown for admission, defence counsel may require time to learn about the technical operation of the algorithm, confer with their own experts, or possibly digest and rely on academic or technical articles to try and raise questions about its forensic reliability. Legal aid plans may not be in a position to fund this potentially significant preparation time for many such applications. A prejudicial effect of admitting AI risk assessment evidence tendered by the Crown may arise where this funding is unavailable or inadequate for the defence to properly prepare to deal with it.

There may be a further prejudicial effect in the evidence's possible potential to invite stereotypical reasoning. This will be discussed further at a later point in the article.

The most important danger at the gatekeeping stage is the risk that the trier of fact will be unable to make an effective and critical assessment of the evidence. This danger may be realized where a trier of fact "adopt[s] the expert evidence without adequate scrutiny" in light of the complexity of the material on which the opinion is based, the "impenetrable jargon in which the opinion is wrapped," and the inability to cross-examine.[142]

The inability of the defence to cross the algorithm as an "expert witness" and the court's inability to properly scrutinize this evidence

Ultimately, "algorithmic risk assessments are akin to 'an anonymous expert [that the defendant] cannot cross-examine.'"[143] Unlike the flesh-and-blood expert witness who can be verbally examined, challenged, and asked to explain themselves, the algorithm "cannot be called into court" for cross-examination.[144]

This inability to cross-examine the "expert" who is providing opinion evidence may represent a significant danger under this prong of the framework. The concern is critical where the algorithm's outputs emanate from a "black box" methodology that developers themselves cannot explain or interpret. The inability to cross examine in this instance may make it virtually impossible for a judge to properly and critically scrutinize this evidence.

Historically, actuarial risk assessments have often been prepared by probation officers, resulting "in an expression in the PSR [Pre-Sentence Report] of the author's opinion as to future risks."[145] The officer could then be subpoenaed for cross-examination of their competence where the defence did not accept the risk score.[146]

However, this option – to question the author of the opinion evidence – does not currently seem available when tendering an algorithm's risk assessment. The imperviousness of the algorithm to being questioned and having its opinion more thoroughly scrutinized, as has been done with similar evidence previously, may represent a significant admission danger under this branch.

3.4.7 Will "automation bias" make it more likely to accept AI as an expert?

If the point of the expert opinion evidence admissibility framework is to ensure that the trier of fact maintains the ability to critically assess the evidence, then the presence of "automation bias" as described by some commentators may raise a further danger.

Some apprehension has been expressed about this "phenomenon," where "information presented by a machine is viewed as inherently trustworthy and above skepticism."[147] This can result in humans "over-rely[ing] on the accuracy or correctness of automated systems."[148] The use of the algorithm thus becomes "a heuristic replacement for vigilant information seeking and processing [… turning] a computerized suggestion into a final, authoritative decision."[149]

In their gatekeeping capacity, a judge must be vigilant. Understanding how algorithms work can be difficult, and this "is particularly relevant in the case of criminal justice, since most legal professionals have no training in computer science."[150] However, it has been suggested that judges are no less susceptible to simply accepting this evidence because it came from a machine.[151]

Thus, a "high-risk score can become a convenient, critical and quick measure of a defendants' suitability for release"[152] despite the judge's lacking a thorough understanding of its actual probative value or reliability – specifically, how the score was conceived and what it may actually mean. Acceptance of such evidence on the basis of "automation bias," without any effective and critical assessment or scrutiny of it, may pose a "most important" admission danger to consider at the gatekeeping stage of the expert opinion admission inquiry.[153]

3.4.8 If not opinion evidence, can algorithmic risk assessment evidence be characterized as a "demonstrative aid?"

Further research and litigation may alter the characterization of algorithmic risk assessment as a form of opinion evidence. Different descriptions in the literature raise other possible interpretations of the character of this evidence. The algorithmic risk assessment score "appears to provide simple, easy to understand and usable summaries of complex statistical predictions."[154] Algorithmic risk assessment has also been described as "summarizing" all "relevant information in a more efficient way than can the human brain."[155] From this perspective, it may be better characterized as a demonstrative aid.

In cases where a "large body of documents have been filed, a party may wish to have them summarized so that their salient and germane points are teased out."[156] Demonstrative aids have been used in this regard, as they can "effectively synthesize […] cumbersome and confusing evidence." A "schedule or summary" may be admitted to assist the trier of fact in understanding evidence already filed.[157] However, where a summary is filed, the trier of fact must still make a determination whether to accept the facts on which the summary rests.[158]

The admissibility of the risk assessment score as a demonstrative aid or summary of data ultimately depends on the exercise of judicial discretion which balances probative value against the potential for prejudice.[159] A key consideration in this analysis, echoing concerns related to the admission of algorithmic risk assessments as opinion evidence, is, again, whether "the maker of the document is available for cross examination."[160]

As indicated above, machine learning algorithms may take into account hundreds of predictors and make "millions" of observations.[161] Given this volume, it may not be feasible to expect the Crown to file all the algorithm inputs at the sentencing, or for a judge to make a finding of whether or not to accept them. And if it is the algorithm that is considered to be "making" the demonstrative aid, we may find ourselves in a similar position as indicated above: trying to assess this evidence in the absence of an ability to cross examine its author.

3.4.9 The admission of the algorithmic risk assessment at sentencing as an aggravating factor

The evidentiary characterization of algorithmic risk assessment and the application of the appropriate rules of admissibility are only the first steps in the sentencing calculus. The ultimate consideration of this evidence must still comply with the *Criminal Code*'s statutory regime for sentencing.

When algorithmic risk assessment evidence indicates a higher future risk of re-offence for offenders sharing the same characteristics as an accused, the accused – as part of that group – is deemed to therefore share a similar higher risk of re-offence.[162] This is potentially significant, as Canadian jurisprudence has long recognized that an accused's higher future risk of re-offence is an aggravating fact at sentencing.[163]

Where the Crown seeks to rely on an algorithmic risk assessment score – which may be part of a presentence report, as it was in *Loomis*- as an aggravating fact on sentencing, the Crown must prove it beyond a reasonable doubt as per section 724(3)(e).

Therefore, if the Crown wishes to tender this evidence and rely on it as aggravating on sentence, the burden to meet is a high one. After a determination of what type of evidence the algorithmic risk assessment is – expert opinion evidence, a demonstrative aid, or something else – the Crown must demonstrate this evidence meets the appropriate admissibility requirements. However proper compliance with the Code's sentencing regime will then also require the Crown to prove the algorithmic risk assessment score beyond reasonable doubt. This must be done in light of the aforementioned concerns about its reliability and often opaque methodology.

3.4.10 Consultation questions

6) Considering the opacity of algorithmic risk assessment, particularly in the absence of any ability to cross examine, how can a judge properly scrutinize its processes, examine its integrity, and determine if its expertise can be properly "qualified?" Will the current inability of defence counsel to cross examine "black box" algorithmic risk assessment be critical to its admissibility?

7) Are AI-enabled risk assessments likely to result in frequent litigation and legal challenges that place an undue resource burden on the justice system? In the Court of Justice, where many pleas can be arranged and traversed into the plea court quickly and on the same day, are Crown attorneys, duty counsel and defence counsel going to have the time and resources to litigate the admissibility of algorithmic risk?

8) What systemic policies, practices, and conventions are in play and how might they need to be addressed for any of the following:

- What is the role of the Crown and what kinds of systemic issues should the Crown look at to ameliorate some of the problems?
- What can the judiciary do?
- What can Legal Aid Ontario do?

9) How can the legal system ensure that AI-generated risk scores, which are increasingly being considered as expert evidence in criminal justice decisions, maintain the required standards of openness, transparency, and reliability to protect the rights of individuals and uphold the integrity of the judicial process?

10) Given the varied acceptance of AI-generated risk scores as expert evidence across different courts, what policy measures should be implemented to standardize the scrutiny and admissibility of such evidence in criminal proceedings to safeguard against potential biases and ensure fair treatment of all individuals within the justice system? How can the legal system maintain the required standards of openness, transparency, and reliability to protect the rights of individuals and uphold the integrity of the judicial process?

3.5 AI-enabled sentencing and post-sentencing risk assessment

The use of algorithmic risk assessment tools at sentencing must comply with statutory parameters in section 718 of the *Criminal Code*.[164] Its use must also comply with the fundamental principle in section 718.1, which requires that a criminal sentence "be proportionate to the gravity of the offence and the degree of responsibility of the offender."[165] Each individual offender and each individual offence must therefore be considered in detail in determining a sentence.

3.5.1 Generalized versus individualized sentencing

It is a cardinal principle of the Canadian criminal justice system that sentencing should be individualized. According to Justice Nakatsuru of the Ontario Superior Court in *R. v. Jackson:*

> Sentencing is and has always been a very *individual* process. A judge takes into account the case-specific facts of the offence and the offender to determine a just and fit sentence.[166]
>
> The more a sentencing judge truly knows about the offender, the more exact and proportionate the sentence can be.[167]

The use of group-based analytics via algorithmic risk assessments, when applied in sentencing decisions for individual offenders, may offend this key principle. AI-generated risk scores are based on general factors; while these may be similar to the offender's background, they are not specific to the individual offender.

This may provide a basis to challenge the use of algorithmic risk assessments at sentencing. In the *Loomis* case the offender challenged his criminal sentence based on its use of scores from an algorithmic risk assessment tool.[168]The offender argued that the COMPAS system used general information about a broader group to predict his risk score, which was, in turn, considered by the judge in imposing a criminal sentence. The offender also argued that the use of COMPAS infringed on his right to due process.

The court in *Loomis* reiterated the importance of individualized sentencing in the criminal justice system. It acknowledged that algorithmic risk scores are based on the data of groups similar to the offender and are thus not individualized. However, the court distinguished between cases where a risk score from an algorithmic tool is *the determining factor* considered by the judge in sentencing, and other situations where the risk score is but *one* of many other factors considered by the court. While the court agreed that a due process challenge may succeed in the former case – where the risk score is the key factor – the court rejected the argument that *any* consideration of the risk score in the sentencing decision-making process violates the offender's due process right.

Therefore, algorithmic risk scores could *assist* in achieving an individualized sentence where they are considered by the court as only one of many factors to that end. However, sentencing judges cannot abdicate their judicial responsibility to data scientists and software engineers. They must *use their own judgment* and judicial discretion to assign the appropriate weight to the risk score. This may result in discounting altogether or attaching very low weight to an algorithmic risk assessment that appears to be incongruent with the unique individual circumstances of the accused. This could apply, for example, to a first-time offender convicted of a minor offence who is assessed by an algorithmic risk tool as high risk. Risk scores should not be used as a tool to justify over-incarceration – in essence, punishing an offender for a crime they have not yet committed. Similarly, sentencing judges can strive to be more amenable to the use of an algorithmic risk score when it mitigates rather than aggravates the sentence imposed on the offender.

Nevertheless, in *Loomis* the court did recognize the risk to individualized sentencing that algorithmic risk tools could pose. Unfortunately, the court addressed this only with a recommendation that a warning be included in any pre-sentencing investigation report containing a COMPAS risk score. This warning should be directed to the sentencing judge and highlight that COMPAS risk assessment scores are based on group data and hence capable of identifying *groups* of high-risk offenders but not a particular high-risk *individual.*[169] The fact that the *Loomis* court found this warning to be necessary further illustrates the weight algorithmic risk scores carry – the potential for automation bias – especially in the minds of sentencing judges presented with this information.

Additionally, categorizing an individual as a high-risk offender because they have a high-risk score may be stereotypical profiling. Individuals with high-risk scores share *similar characteristics* with the general population of high-risk offenders, but this is not the same as being one.[170] Risk scores are not always understood as correlations and may be mistakenly interpreted as ascribing the characteristics of a risk group to the individual.[171]

The central issue is that AI recidivism risk assessments facilitate decision making about an individual's freedom based on *the behaviour of others*.[172] This may impugn proportionality as a fundamental principle of sentencing.[173] A sentence must be proportionate to the gravity of the offence as well as the degree of responsibility of the offender, but *not that of other offenders* with similar risk factors. Basing sentencing decisions on the history or data of "like groups" problematizes how this principle is reflected in AI recidivism risk assessment.

3.5.2 Bias at sentencing: historically biased training data and sentencing of indigenous and black offenders

Some of the generalized factors used by AI risk assessment tools to assess recidivism risk levels may also indirectly contribute to racial discrimination, even when the assessment models do not actually consider race as a variable.[174] Variables which could induce race-based outcomes in AI risk assessment include location/address, associates, employment, police encounters, etc.[175] Though blatant racism is no longer prominent in the American criminal justice system compared to the pre-civil rights era,[176] and the same is likely true in Canada, these systems are still entangled in elements of structural racism they have inherited from the past. Eckhouse *et al.* have noted that "[in] a society structured by racism and segregation, many variables commonly included in [recidivism risk assessment] models […] will be correlated with race."[177]

A fundamental concern in dealing with algorithmic risk assessment is the effect it may have on sentencing Indigenous or racialized offenders. Algorithmic risk assessment scores make predictions by being fed data from the past. Because the data or inputs used by the algorithm – arrests, convictions, incarceration sentences, education, employment, etc. – "are themselves the results of racially disparate practices, the results or scores of pretrial risk assessments are inevitably biased."[178]

In the context of Black defendants, the long history of social and economic oppression of Black people has produced higher rates of arrest, prosecution, conviction, and incarceration than their white counterparts. "The result is that criminal history now correlates with race. Any form of risk assessment that relies on criminal history will have a disparate impact on Black communities and on [B]lack men in particular."[179]

The higher arrest rates are the product of racist institutional and systemic practices. They reflect bias. As these biased arrest rates are fed into the algorithm, which looks to the past to predict the future, then the concern becomes clear – "because the rate of arrest was higher among the black defendants, they, on average, had higher arrest-risk profiles."[180] Hence "bias in, bias out":[181] The algorithm considers those higher arrest rates of the past, and then calculates a higher arrest risk, a product of that biased data, for the offender before the court.

As we see with the potential concerns with "automation bias," judicial deference to the algorithm's output may result in any number of prejudicial outcomes to a racialized defendant. This raises the risk of perhaps further custody or perhaps more stringent probation conditions. Either outcome can keep that racialized defendant in the criminal justice system for a longer period of time, or subject to more oversight, restriction, or control. This in turn may result in a domino effect of enhanced police monitoring, risks of further charges for not complying with conditions, or longer sentences in the event of future convictions – not for any rational reason, but because of a risk score that was itself inherently biased and based on prior racist practices. This is how an algorithm's prediction based on past racist practices simply "project[s] history forward."[182] The algorithm thus can "perpetuate or amplify social inequality, all while maintaining the veneer of high-tech objectivity."[183]

The application of algorithmic risk assessment in this respect may therefore be entirely violative of sentencing principles binding sentencing judges to take judicial notice of racism and discrimination when crafting an individualized sentence for Black or Indigenous offenders, as discussed below.

Does algorithmic risk assessment potentially conflict with jurisprudence on sentencing black offenders?

The Ontario Court of Appeal in *Morris*[184] indicated an understanding that anti-Black racism is "reflected in many social institutions, most notably the criminal justice system."[185] An expert report on criminal justice and the "Experience of Black Canadians in Toronto" was filed at the original sentencing, which "drew a connection between the long history in Canada of overtly racist attitudes and social practices and present day institutional and systemic discrimination against Black people." The Court of Appeal found that the trial judge could have taken judicial notice of many of these facts.[186]

The Court further held that evidence of anti-Black racism and its impact on the specific offender could be an "important consideration when determining the appropriate sentence."[187] Racism may have impacted the offender in a way that bears on their moral culpability for the crime, and this can serve to mitigate the ultimate sentence.[188]

Algorithmic risk assessment is based on numerous inputs – including those indicative of marginalization, poverty, lack of opportunities, and subjugation to aggressive police presence – that may reflect systemic racism and discrimination.[189] These discriminatory historical factors input into an algorithm may result in a higher re-arrest risk score for racialized offenders in the sentencing court, with, as indicated above, resultant restrictions on liberty and more severe sentences.

Yet now there is appellate caselaw directing judges to contextualize those same factors as reflecting discriminatory practices. In this light their impact on the moral culpability of a Black offender before the court is to be considered. In balancing the interests of the proportionality principle, a judge can find those factors to be mitigative in the ultimate imposition of a sentence.

Thus, there is a potential conflict between what the algorithmic risk assessments are doing and what today's sentencing courts are directed to do. Algorithmic risk assessment relies on historical data that is the product of racism and discrimination, and in doing so may output a score indicating a high risk of re-offence. This may be an aggravating factor that makes a sentence longer or more stringent. Yet after *Morris* the sentencing court must take judicial notice of that same historical racism and discrimination, consider its specific effects on the moral culpability of the offender before the court, and find that those same factors may serve to mitigate the sentence. This potential conflict may raise questions about the appropriate use of algorithmic risk assessments, as currently constituted, in sentencing Black offenders after *Morris*.

Does algorithmic risk assessment potentially conflict with jurisprudence on sentencing indigenous offenders?

There is little doubt that Indigenous people are "victims of a discriminatory justice system."[190] Socioeconomic factors such as employment status, level of education, family situation, etc. appear on the surface as neutral criteria. Yet they can conceal bias in the sentencing process. Convicted persons with employment and stability in their lives, or at least prospects of the same, are less likely to be sent to jail for offences that are borderline imprisonment offences. The unemployed, transients, and the poorly educated are all more likely to be incarcerated. When the social, political, and economic aspects of society place Aboriginal people disproportionately within the ranks of the latter, society sentences more of them to jail. This is systemic discrimination,[191] and there can be little doubt that it is rooted in colonialism and racism.[192] In this way the justice system has failed the Indigenous community.[193]

S.718.2(e) of the *Criminal Code* sought to address Indigenous carceral overrepresentation,[194] indicating that "all available sanctions, other than imprisonment, that are reasonable in the circumstances […] should be considered for all offenders, with particular attention to the circumstances of Aboriginal offenders."[195] In what is now trite law, those "circumstances" include: a) the unique systemic or background factors which may have played a part in bringing the particular Aboriginal offender before the courts, and b) the types of sentencing procedures and sanctions which may be appropriate for the offender because of their particular Aboriginal heritage or connection.[196]

In determining a sentence for Indigenous offenders judges must now consider those discriminatory systemic and background factors including "the history of colonialism, displacement, and residential schools and how that history continues to translate into lower educational attainment, lower incomes, higher unemployment, higher rates of substance abuse and suicide, and of course higher levels of incarceration for Aboriginal peoples."[197] In keeping with the ameliorative aims of s718.2(e), the requirement to consider these circumstances for Indigenous offenders may lead to a similar assessment as in *Morris*: circumstances of "social and economic deprivation with a lack of opportunities and limited options for positive development," may reflect "constrained circumstances" which in turn may diminish moral culpability[198] and mitigate the sentence.

This "different method of analysis" in sentencing supports s718.2(e) as a remedial provision, "designed to ameliorate the serious problem of overrepresentation of Aboriginal people in Canadian prisons, and to encourage sentencing judges to have recourse to a restorative approach to sentencing."[199] Hence the mandated judicial approach to Indigenous sentencing pursuant to s718.2(e) and cases like *Ipeelee* is to have a sensitivity to this discriminatory, colonial and racist history that has resulted in more incarceration. To ameliorate this disproportion, judges must instead consider how these circumstances affect moral culpability and consider sanctions other than custody where appropriate.

However, using algorithmic risk assessments at sentencing for Indigenous offenders raises similar concerns as with Black offenders. The Alberta Court of Appeal in *R v. Natomagan*[200] explained the issues with inputting factors, such as those indicated above, that reflect discrimination into risk assessment tools for Indigenous offenders:

> "In short, some of the inputs into actuarial tools are discriminatory. Those inputs go directly into the statistical mix without further consideration, as though into an algorithm, and come out again as a measure of correlation [….] The actuarial tools that purport to provide measurable, objective, and scientific results have, to some degree, the effect of laundering discrimination."[201]

The algorithmic risk assessment score is based on historical discriminatory data, reflecting the oppression of Indigenous people and their disproportionate incarceration. As this predictive method looks to the past, the past inequalities are projected forward. Thus an Indigenous offender may now be saddled with a high re-arrest score – and face further custody or more restrictions on liberty - because the algorithm has based its prediction on biased data from the past.

Consequently, as with Black offenders, there is a potential conflict in what the algorithm risks doing with historical data and what the sentencing court is directed to do with it. The algorithm relies on past inputs reflecting colonial oppression and overt racism to produce a potentially high re-offence score, which risks further incarceration for an Indigenous offender. But s.718.2(e) and caselaw like *Ipeelee* direct the sentencing judge to consider that colonial history in an entirely different vein – to weigh its specific effect on the moral culpability of the offender before the court, and find how those same factors may serve to mitigate the sentence and any incarceration. This conflict – between what the algorithm does and what the court is required to do – may again raise a question about the place for algorithmic risk assessments in sentencing Indigenous offenders.

Case Study: How could AI-generated photographic evidence interfere with sentencing?

A key consideration in these cases concerns the practicalities in contesting AI-related evidence in context of existing norms in bail or sentencing practices. To review several case study scenarios illustrating these practical challenges, please see LCO AI in Criminal Justice Project paper ***Annex B, Project Case Studies***. In particular, one scenario shows some of the complications that arise with the characterization of AI-generated photographic images at sentencing.

3.5.3 Consultation questions

11) How can the Canadian criminal justice system maintain the principle of individualized sentencing while integrating AI-generated risk scores in the decision-making process, ensuring these tools do not override judicial discretion and contribute to potential over-incarceration or stereotyping of offenders?

12) Given the risk of AI recidivism risk assessments facilitating decision-making based on the behavior of others and potentially contributing to racial discrimination, what measures can be implemented to critically evaluate and adjust the variables used by these tools to prevent the perpetuation of structural racism within the criminal justice system?

13) Can algorithmic risk assessments, producing outputs on the basis of a discriminatory history, have a place in sentencing Indigenous and Black offenders in light of current sentencing caselaw like *Ipeelee* and *Morris*?

3.6 Challenging AI-enabled risk assessment in the bail process

3.6.1 The assessment of evidence in bail

Given the expeditious nature of bail hearings, it is unlikely that the characterization of algorithmic evidence and what admissibility rules apply can be litigated to any great degree in a busy bail court. Bail must be determined quickly, as even a short period of custody on a presumptively innocent accused can have a detrimental impact on their life. This dynamic "places great significance on the value of efficiency. A number of features of the bail hearing are driven by this normative component."[202]

It is recognized that this efficiency in bail court comes at a "cost."[203] With the emphasis on expedience, informality is required. This translates into a relaxation of evidence rules.

Nevertheless, there is a reinvigorated appreciation that the "bail hearing is arguably that single most important step in criminal proceedings."[204] It can have an impact on the accused's ability to make full answer and defence and on the outcome of the trial. The Supreme Court's more recent decisions on bail seem to support this view, with a powerful directive in 2017 that "[i]t is time to ensure that the bail provisions are applied consistently and fairly. The stakes are too high for anything less." [205] The Court also noted that a presumptively innocent accused must not find it necessary to plead guilty to be released.[206]

Two years later the Supreme Court again drew a connection between denial of bail in certain cases and concerns with induced guilty pleas, which are "profoundly" detrimental to the integrity of the criminal justice system.[207]

The connection between bail denied and forced guilty pleas reflects this renewed appreciation of the importance of the bail decision. This may raise a question of whether efficiency at bail hearings needs to be balanced against more rigorous scrutiny of the value and admission of algorithmic risk assessment evidence.

Case Study: How could AI-generated photographic evidence interfere with bail?

A key consideration in these cases concerns the practicalities in contesting AI-related evidence in context of existing norms in bail or sentencing practices. To review several case study scenarios illustrating these practical challenges, please see LCO AI in Criminal Justice Project paper ***Annex B, Project Case Studies***. In particular, one scenario shows some of the complications that arise with the characterization of AI-generated photographic images in a bail proceeding.

3.6.2 Is disclosure of the algorithm's operation feasible at the bail stage?

As discussed earlier, many commentators have raised concerns about problems with the disclosure process of how the algorithmic risk assessment tools operate, in large measure because many of these tools are proprietary and rely on trade secrets.[208] However, there are some cases where parties relying on algorithmic tools have made certain disclosures with respect to their inputs.[209] This information could potentially reveal flaws in the data and raise reliability concerns with the risk assessment score.

There may be some challenges with the disclosure of this information in a busy bail court, if practically possible at all. First, assuming counsel can circumvent proprietary or third-party disclosure issues to obtain it, information about the algorithm's operation may well be extremely technical. Counsel would require time to fully digest and understand it, to the extent that this can even be done for "black box" algorithms. Also, as discussed above, some algorithms make "millions" of observations.[210] Some forecasts use well over 100 predictors.[211] The more inputs used, the more inputs would need to be disclosed to counsel.

Ultimately, it may be that disclosure of this information could result in increased complexity and time consumption at the bail hearing. Thus, where the Crown proceeds to tender this powerful evidence at the bail hearing, the accused may find themselves facing an impossible choice. They may instruct their counsel to wait for disclosure of this technical and complex information, necessitating adjournments to obtain and digest it – again, to the limited extent possible, given the risk assessment's "black box" opacity and thereby risk staying in custody longer. Alternatively, they may instruct their counsel to proceed forthwith in the absence of disclosure, and run the risk of the algorithm's output, bolstered by automation bias, weighing heavily in the bail decision with less information to attack its reliability.

3.6.3 Challenging the relevance of the algorithmic risk assessment at the bail hearing

The "relevance" of evidence at a bail hearing is determined by the "substance" of the proceedings. To adjudicate on bail the justice requires information about the allegations, the accused, and their personal circumstances. The criteria listed in section 515(10) of the *Criminal Code* are then applied to this information to determine the issue of bail. The question of relevance "may be tested by considering the proffered evidence in light of these substantive areas."[212]

As the algorithm predicts re-arrest, is it still relevant to the question of whether there is a secondary ground concern – that if released, an accused will commit further offences?

In many bail cases a main question for the Justice of the Peace to answer is whether detention is necessary for the protection or safety of the public, "*having regard to all the circumstances including any substantial likelihood that the accused will, if released from custody, commit a criminal offence* or interfere with the administration of justice."[213] Parliament chose specific wording for this directive: a jurist must find a "substantial likelihood" that an accused "will […] commit a criminal offence." This requires a high degree of probability that an accused will engage in criminality in order to prevent release from custody.

However, a closer analysis of what the algorithmic risk assessment actually predicts may raise a concern about the value of this evidence in bail court. As indicated above, the dataset fed into the algorithm does not necessarily indicate whether crimes have been committed in the past. A record of past crimes is "really a record of crime reports and law enforcement actions, and the relationship of that record to actual crimes committed is opaque."[214] Therefore, while most tools "purport to predict future crime," that is "not actually what they predict. They generally predict future arrest."[215]

An arrest is not necessarily the same as the commission of an offence. There may be an argument that the prediction of future arrests – particularly when based on inputs that may reflect biased or racist past practices – has limited value in an analysis that seeks to determine whether there is a substantial likelihood that an accused will commit further criminal offences. This may place the relevance of the algorithmic assessment in some doubt.

Does the algorithm's prediction window – in some cases, two years – affect its relevance at the bail hearing?

It should be clear at the bail hearing that some "algorithmic risk assessment tools predict the likelihood of re-arrest and fail[ure] to appear over a fixed time period, typically two years."[216]

As practitioners in the Ontario Court of Justice know, many matters that start out in bail court resolve well before two years. This is important as "if a defendant's period of pre-trial release is half as long as a tool's horizon, then the defendant will be *less likely* to be rearrested than the tool predicts. Unless this aspect of the risk score is disclosed and understood, the risk score and tool may be misleading."[217]

This may raise the question again about the probative value of a risk assessment score measured over a two-year period when the timeline of a charge may be quite shorter than that. This raises a concern about how this evidence would advance the inquiry under section 515(10), in turn placing its relevance in question.

Is the algorithmic risk assessment score relevant if its score is based on inputs that have been judicially recognized as "irrelevant?"

Police "occurrence reports" are sometimes tendered at bail hearings. Police typically create these reports when there is an interaction between police and the accused, but no charges are laid. They cast the accused in a bad light and may contain prejudicial hearsay.[218]

Submitting these reports at bail hearings has raised concerns. While rules of evidence are relaxed in bail hearings, they are not abdicated.[219] Bail hearings should not become "file dumps" of everything in a police computer that has an accused's name on it. Interactions or "tips" listed in "occurrence reports" are often without sources. They do not result in charges and there is usually no explanation why. It is impossible to test this evidence to determine if it is credible and trustworthy. As such, a reference to police being involved with an accused, "without more, [is] irrelevant."[220]

However, these types of uncharged interactions could make their way into an algorithm's inputs. Inputs that record "[y]oung black males [...] stopped by police dozens of times, even when they've done nothing wrong" can be fed into the algorithm and be correlated to risk.[221] If computer records of "carding," absent an indication of wrongdoing or charges, could be fed into an algorithmic risk assessment and correlated to risk, it may not be a stretch to consider that "occurrence reports" could be used in the same fashion.

Thus, there may be a concern that an algorithmic risk assessment, in taking that "irrelevant" information and then correlating it to risk, is doing the very thing that the Superior Court in *Downey* has admonished.[222] This concern demonstrates why it may be important for counsel to request and wait for disclosure of at least the algorithm's inputs at the bail stage. If the algorithm does indeed produce a risk assessment prediction based at least in part on information that may be deemed irrelevant for the bail hearing, then the risk assessment output may itself have its "relevance" attenuated.

3.6.4 Bias at Bail: how will courts treat AI training data in light of *Criminal Code* obligations to the historical circumstances of Indigenous and vulnerable groups?

How do concerns about the past data processed by the algorithm conflict with s493.2(a) and (b)?

As indicated above, inputs into algorithmic risk assessments – arrests, convictions, incarceration sentences, education, employment – may themselves reflect racially biased practices. Again, this raises the concern that the resulting scores based on that data are themselves biased.[223] A biased score based on racially biased inputs could have potentially catastrophic consequence for an Indigenous or racialized accused. They may be saddled with a high-risk assessment score and be unreasonably or inappropriately detained or subjected to extremely tight bail conditions because of a discriminatory history of others.

Sections 493.2(a) and (b) of the *Criminal Code* mandate particular attention to the circumstances of Aboriginal accused and accused belonging to other vulnerable populations that are overrepresented in the criminal justice system, respectively. At the Standing Committee on Justice and Human Rights, Department of Justice counsel testified that the purpose behind Parliament's enactment of section 493.2 was "to get those who make decisions about release to 'try to remove any kind of discriminatory thinking about people who don't fit their mould of the 'good citizen.'"[224] However, algorithmic risk assessments may conflict with the aims of section 493.2.

What does s. 493.2(a) aim to achieve?

Section 493.2(a) of the *Criminal Code* states: "In making a decision under this Part, a peace officer, justice or judge shall give particular attention to the circumstances of […] Aboriginal accused."[225]

The plight of Indigenous accused in bail court is well known: Indigenous accused are too frequently subjected to bias and "an unfortunate institutional approach that is more inclined to refuse bail."[226] Factors considered at bail include antecedents, employment, housing stability, education, and links with the community. The social and economic disadvantages endured by Indigenous accused respecting these factors often leave them unable to meet a court's section 515(10) concerns. This has resulted in their detention.[227]

Section 493.2 aims to change this by prompting bail jurists to consider how systemic factors may have played a role in an Indigenous accused's antecedents. To the extent the Indigenous accused's criminal antecedents can be attributed to systemic factors stemming from colonialism and subsequent poverty and substance abuse, jurists applying this section "should view prior convictions as systemically motivated rather than as intentional disregard for the law, particularly in relation to conviction for failing to attend court or failing to comply with conditions."[228] This approach, through the use of a "*Gladue* lens," also mandates a contextualization of antecedents that appreciates how "impairments can originate from the dislocation and hardship caused by colonialism and residential schools."[229]

Therefore, under section 493.2(a), the bail jurist dealing with an Indigenous accused must consider the context of their criminal record, substance abuse, poverty, lack of education and employment, and disconnection from the community. The bail jurist must have an awareness of the colonial legacies and racist practices that may have played a role in the generation of these circumstances, rather than assuming that these circumstances reflect a risk of, or a propensity to, criminality. In this way section 493.2(a) assists with the elimination of "discriminatory thinking" in the bail adjudication.

What does s. 493.2(b) aim to achieve?

S493.2(b) states: "In making a decision under this Part, a peace officer, justice or judge shall give particular attention to the circumstances of […] accused who belong to a vulnerable population that is overrepresented in the criminal justice system and that is disadvantaged in obtaining release under this Part."[230] The section's purpose has been reiterated as aiming to "ameliorate the pre-trial overincarceration of the overrepresented, vulnerable groups referred to […. T]he most obvious means is to release more of [these] accused."[231]

A similar contextual approach as in section 493.2(a) has been implemented for Black accused in bail court under section 493.2(b). There is judicial recognition of anti-Black racism and the problem of Black overrepresentation in the justice system, and this recognition should apply at the pretrial stage also.[232] This calls for "[a] critical approach to overrepresentation" that can affect the evaluation of the three grounds of bail and guide the process of crafting conditions.[233]

Similar to section 493.2(a), the "critical approach" under s493.2(b) requires a more contextualized assessment of the "overrepresented and vulnerable" accused's antecedents. For example, some Black accused, for systemic reasons, may have had more limited opportunities for education and employment. Others may have been subject to a more aggressive police presence. Appreciating this context, and sensitivity to the irrefutable presence of systemic biases, may help provide a more "realistic perspective" on a Black accused's antecedents and failures to comply with bail or probation conditions.[234] Recognizing that some of these antecedents may be systemically influenced may have "the direct effect of reducing the tendency of these convictions to cast doubt on the Applicant's trustworthiness on bail."[235]

Again, this section requires a contextualized appreciation of systemically racist or biased practices that may be responsible for the circumstances of the Black accused before the court, to prevent the automatic assumption that these antecedents reflect a propensity for criminality.[236] In this way, section 493.2(b) also assists with the elimination of "discriminatory thinking" in bail adjudication.

What role does algorithmic risk assessment have in bail court in light of s.493.2(a) and (b)?

Police-generated evidence, which may be rooted in institutional racism and in turn relied on at bail, is "a contributing factor to the mass incarceration of Indigenous, Black and marginalized people in pretrial detention in Canada."[237] To give effect to what section 493.2 aims for, evidence at the bail hearing must be viewed through a social context lens, and "attention must be paid to how racism and other forms of discrimination may impact the police assessment of the accused."[238] This section requires bail jurists and counsel to be aware of racist policing, systemic bias in the justice system as reflected in respective criminal records, and the legacy of colonialism and slavery on Indigenous and Black people.[239]

Section 493.2 seeks to interrupt the cycle of "bias in, bias out" in bail court. The evidentiary record at the Indigenous or Black accused's bail hearing must be contextualized. The aggravating features at bail hearings for these accused – the criminal antecedents, and impediments to bail like homelessness, joblessness, and addiction – can be explained, placed within historical and social context, and mitigated. Thus, the jurist can be persuaded that an Indigenous or racialized accused's "dangerousness," as based on these factors, may be a product of a biased justice system or racist systemic practices and thus unwarranted, militating for a release.

It is unclear to what extent an algorithm can be trained to be aware of colonial and racist legacies that have resulted in biased and disparate treatment of these communities. It is also unclear to what extent an algorithm can contextualize those factors for the purpose of producing a risk assessment prediction at the bail stage. To the extent that it cannot, the concern is that the algorithm may rely on that same type of biased and racially influenced historical data – arrests, convictions, sentences, unemployment, substance abuse, homelessness, etc. – without any of the systemic contextualization mandated by section 493.2. This risks the production of a prejudicial risk assessment score for the Indigenous or Black accused that may result in a detention order created without the statutory safeguards in the *Criminal Code*.

This may raise a concern that algorithmic risk assessment, left to its own devices, is engaging in precisely the type of "discriminatory thinking" section 493.2 seeks to eliminate. If so, admitting and using such risk assessment scores in bail adjudication may circumvent Parliament's intention in enacting section 493.2.

3.6.5 Does the "release matrix" for an AI risk assessment align with the law of bail on release conditions?

The "principle of restraint" statutorily directs justices in bail court to give primary consideration to the release of the accused on "the least onerous conditions that are appropriate in the circumstances" while taking into account the section 515(10) grounds.[240] The Supreme Court has reiterated that this principle requires bail conditions be "minimal in number, necessary, reasonable, least onerous in the circumstances, and sufficiently linked to the accused's risks regarding the statutory grounds for detention in s. 515(10)."[241]

Bail adjudication requires an "individualized approach."[242] This means that bail conditions are to be "tailored" to the individual risks an accused poses, and not imposed "by rote."[243] When setting a bail condition it must attenuate a specific risk that would otherwise prevent an accused's release, and not be imposed gratuitously or punitively.[244] The key point is that setting bail is an "individualized process" and there is no place for standard or boilerplate conditions.[245]

In light of these principles, some problematic aspects to using algorithmic risk assessments to assist with bail adjudication may arise. Algorithmic risk assessment does not make an express recommendation as to detention, release, or what conditions to impose. Instead, the score "slots" an accused into the appropriate box in a separate "decision making framework" or "matrix." This matrix sets out directives on how to deal with an accused based on their score.[246] For example, the Public Safety Assessment (PSA) tool has been accompanied by a release conditions matrix which matches conditions with an accused's risk assessment score based on local statutes, court rules, and policy preferences regarding bail release and conditions.[247]

There may be concerns that this process does not comply with the lawful imposition of bail conditions. Algorithmic risk assessment evidence may reflect risks raised by a group of individuals sharing the same characteristics as the accused rather than the accused themselves. To impose conditions on an individual accused because of a risk posed by a group may be an affront to the requirement that setting bail is an individualized process.

Further, as discussed, algorithmic processes are often unexplained and opaque. Usually, a human tells the computer which inputs to use, which outcomes to predict, and which learning method to use, and "the computer does the rest."[248] "(See particularly the discussion of Loomis and Zilly above at section 2.2). The accused may be subjected to a regime where conditions are imposed – potentially restrictive ones such as a curfew or house arrest- on the basis of an unexplained algorithm's risk assessment.

Again, bail conditions must be "tailored to the individual risks posed by the accused. There should not be a list of conditions inserted by rote."[249] Identifying the individual risks an accused poses may be impossible if the risk assessment score, making a prediction of "dangerousness," does not disclose specifically which inputs correlate to this re-offence risk. Without that understanding, to place an accused into a corresponding matrix category and impose prescribed conditions could be argued to result in the "insertion" of boilerplate conditions "by rote." This may threaten the application of restraint, reasonableness, and individualization in setting conditions in bail court.

3.6.6. How will the algorithm's risk assessment affect the court's duty to give reasons at the bail hearing?

At the hearing's end the justice is expected to provide reasons for the decision on bail.[250] In light of the increased appreciation of the importance of bail for the accused and society, this step may be taking on a new importance, requiring that reasons be more rigorous and thorough. An opaque, uninterpretable algorithmic risk assessment may impact this crucial step.

Cogent and reasoned analysis of the evidence is required to support the findings. This is necessary for a potential review, but is also important to the parties and the administration of justice.[251] Critical facts should be addressed.[252] Reasons on bail require a visible and reasoned explanation of the path between evidence and ultimate conclusion, and not simply an announcement of the result.[253] This means that explanations as to why a witness's testimony is preferred are required, [254] and conclusory statements with no analysis on how conflicts on material points are resolved are insufficient as reasons.[255]

Where a jurist finds that an accused is dangerous without any explanation or reference to the evidence as to why, this may fall short of sufficient reasons at bail. Yet an algorithm's risk assessment score may be opaque and unintelligible, with no explanation of what role certain inputs played in its analysis. In principle this may also amount to a conclusory statement. This raises a concern that a jurist, in simply adopting the algorithm's risk assessment score with no scrutiny or understanding of its underpinnings, is essentially re-articulating a conclusory statement. Further, it may be that accepting that opaque risk assessment score in effect constitutes the preference of a witness's evidence without any explanation why. The use of algorithmic risk assessment evidence may thus raise practical concerns and impacts on a court's duty to give reasons at bail.

3.6.7 Consultation questions

14) Defence counsel run bail hearings on serious charges with only a synopsis read in and no disclosure. Is the power of an algorithmic risk assessment stronger or different than a graphic synopsis on a serious charge? If it is, is it fair that accused be advised to wait for disclosure regarding inputs or on an algorithm's operation (and stay in custody longer while counsel attempts to decipher it), or proceed with the risk assessment number looming large in court?

15) Is there a concern about the "relevance" of the risk assessment score if it is based on information that would legally be "irrelevant" at the bail hearing? Does this put an impetus on counsel to request and wait for the inputs?

16) Recent developments in jurisprudence (such as *Ipeelee* and *Morris*) and legislation (CCC s. 493.2) require consideration of how historical bias and discrimination have played a role in the disproportionate disadvantage and criminalization of Indigenous and Black communities. If the algorithm cannot consider colonial or racist legacies or histories that may have played a role in formulating the data it processes, does admission of the score circumvent *Criminal Code* s. 493.2? Can counsel successfully argue that given the principles of s493.2, the unexplained risk score should be given less (or no) weight?

17) Do release matrix recommended conditions – such as house arrest or a curfew –amount to boilerplate conditions "inserted by rote" where there is no justification of the score or of the accused's placement in that category?

18) If reasons are to represent a promotion of visibility – including ensuring that racial bias plays no role in the bail decision – can there be any place for evidence that in and of itself does not give any reasons?

19) What legislative or regulatory measures should be introduced to set standards and ensure rigorous testing and validation of these tools for bias before their deployment in the criminal justice system, and how can ongoing oversight be maintained?

3.7 To use or not to use?

Having identified and discussed above the many issues associated with the use of AI risk assessment tools in the criminal justice system, the question then is whether we should be deploying these tools in the Canadian criminal justice system. The answer here is both yes and no.

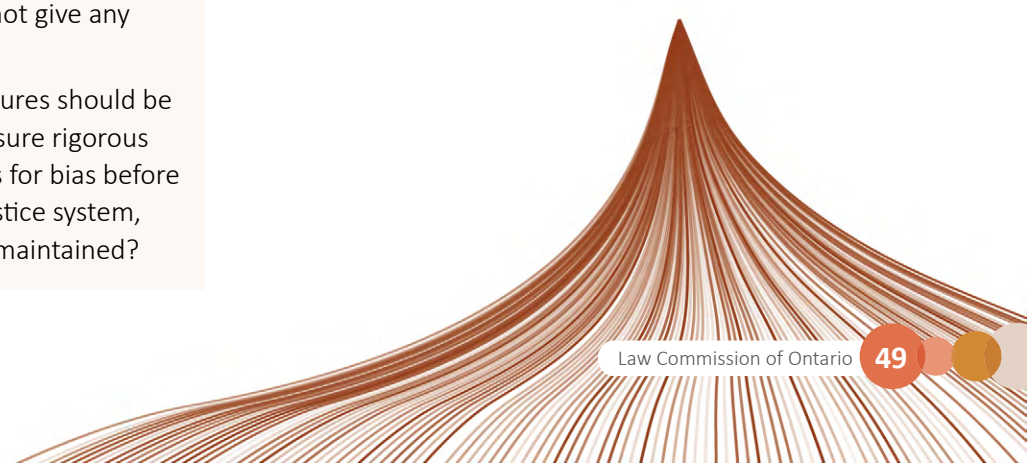
First, it is important to note that the future is unpredictable, and this truth applies equally to the future conduct of criminal justice subjects. We cannot predict with a certainty what individual subjects in the criminal justice system are capable or incapable of doing in the future.

Second, we still are lacking considerable knowledge and insight into the black box aspects of AI risk assessment tools.

Third, detailed studies and literature are available that continue to warn about the risks of different kinds of bias evident in AI risk assessment tools, such as those pertaining to race, gender, socioeconomic status, and so on.

Fourth, the philosophical question persists as to the morality of punishing an individual – or increasing their punishment – on the basis of a crime they *might* commit, but which they have not committed.

On the other hand, AI tools speed up the process of risk assessment in the criminal justice system. They could potentially ameliorate conscious and unconscious biases associated with human risk assessment if properly designed and assessed as doing so. Further, we now live in a world that is increasingly digital. The criminal justice system cannot escape the technological innovation sweeping through every aspect of human society.

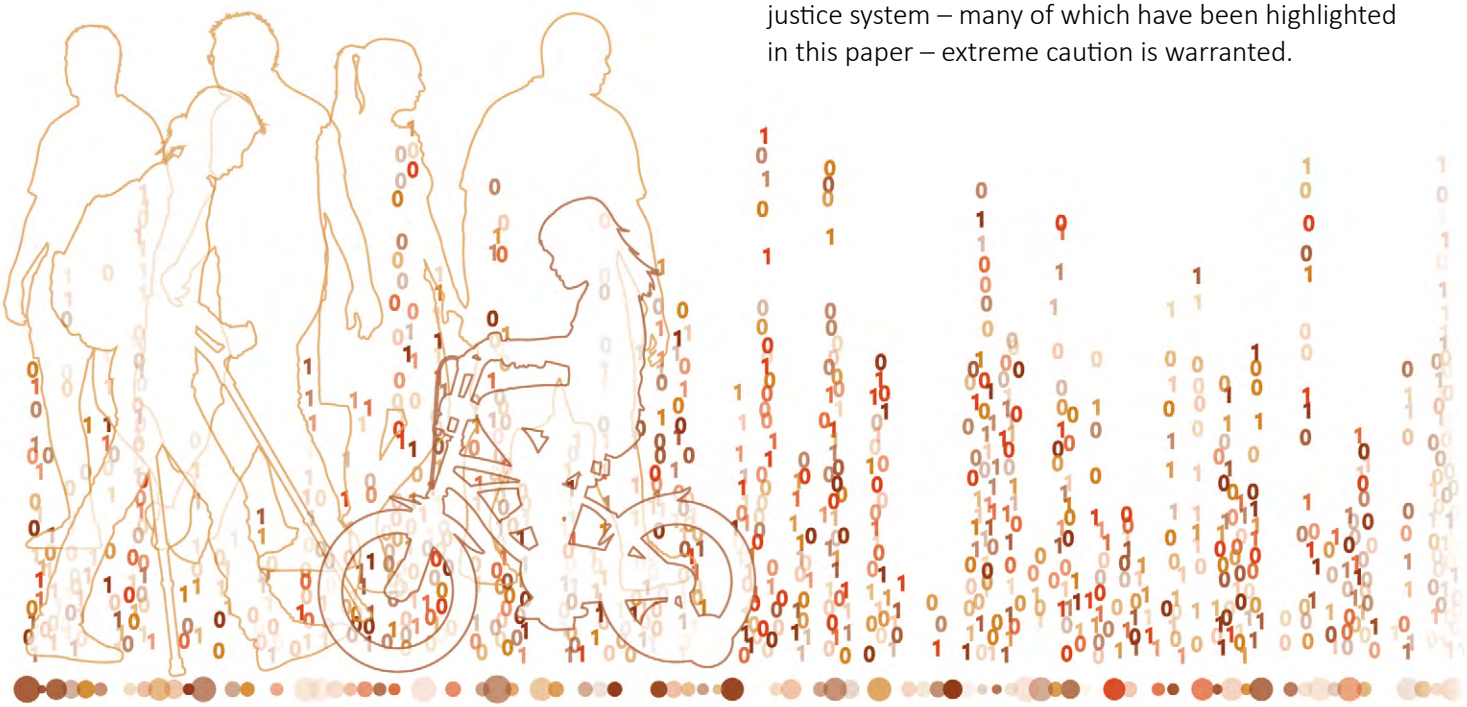


Nevertheless, we must also assert that currently there are many issues arising from the use of AI risk assessment tools in the criminal justice system. These concerns are evident in the U.S., where the use of these tools is very pronounced; indeed, the more we scrutinize them, the more issues we continue to unravel.[256] The Canadian criminal justice system is built on the fundamental principle of providing protection to the rights of subjects within the system and not removing or watering down their constitutional protection. The presumption of innocence and the need for proof of a subject's criminal conduct beyond a reasonable doubt remain fundamental to the system.

Furthermore, our criminal justice system is one in which minority members of society are disproportionately represented. This over-representation is being addressed by efforts to promote alternatives to incarceration. The use of AI tools should come with serious caution, since they carry the risk of further discriminating against members of society who are already overrepresented in the carceral system.

Considering the current state of knowledge about AI risk assessment tools, a sensible recommendation for the Canadian criminal justice system is that the tools be used only to the extent that the risk scores they provide are a potential mitigating, not aggravating, factor. When a tool's risk score serves only to aggravate the sentence on the individual, then other factors or evidence outside the tool's result should be invoked to support their use. AI risk scores should never be the sole basis or factor for increasing the punishment imposed on an offender.

Evidence from the numerous cases discussed throughout this paper shows how high-risk scores can bias judges, whether this unfolds consciously or unconsciously. In light of this basic aspect of human nature, another potential recommendation is that a high-risk score generated by an AI tool should not be made available to the judge at the sentencing phase of a criminal proceeding without other external evidence that supports a similar risk assessment. Even a warning label attached to the assessment, as was suggested by the appellate court in *Loomis,* does little to free the judge's mind of bias towards potentially heavier sentences. Until we have sufficient access to the methodologies employed by these AI tools, and enough evidence to address the various concerns arising from their deployment in the Canadian criminal justice system – many of which have been highlighted in this paper – extreme caution is warranted.



4. Next Steps and Summary of Consultation Questions

4.1 Consultation Process

The LCO's consultation process starts with the release of this Issues Paper.

The LCO wants to hear from a broad range of stakeholders including lawyers and legal organizations, NGOs, industry representatives, academics, government and justice system leaders, and individual Ontarians interested in the operation of the criminal justice system.

The LCO will be organizing several consultation processes over the next several months. The LCO is strongly committed to partnering with interested organizations and stakeholders to develop consultation initiatives. Individuals or organizations interested in working with the LCO are encouraged to contact our Project Lead.

The LCO also encourages written submissions, which can be sent to the LCO's general email address at LawCommission@lco-cdo.org.

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

The LCO is committed to sharing ideas and building constructive dialogue. Accordingly, the LCO expects to post written submissions on our project webpage, subject to limited exceptions. Individuals or organizations wishing to provide a written submission may want to contact the LCO for further information prior to their submission.

Project Lead and Contacts

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

The LCO can also be contacted at:

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

LawCommission@lco-cdo.org

4.2 Consolidated consultation questions

AI-enabled risk assessment tools in criminal justice

1) Assessments and predictions about risks, public safety and other factors are not new. However, AI-enabled risk assessments bring new complications, such as a lack of verification, calibration, and certification; technological deference where humans are over-reliant and uncritical about AI-generated recommendations; and other factors. Given this, what weight should jurists assign to AI-enabled prediction? How is this similar to or different from other traditional risk assessment tools?

Bias in the training, development and use of AI risk tools

2) Given the significant influence of private commercial actors in the development of AI risk assessment tools, what regulations or policies are needed to ensure a transparent process involving criminal justice stakeholders, aiming to safeguard public interest and improve the reliability and fairness of these tools?

Navigating disclosure, trade secrets and intellectual property rights

3) How can the criminal justice system balance the need for transparency and the fair administration of justice with the proprietary rights of commercial corporations that design AI risk assessment tools, ensuring that all parties involved in a legal matter have access to and understanding of the methodologies behind these tools?

4) Given the Supreme Court of Canada's stance on access to proprietary information as necessary to preserve Charter rights, what legal frameworks or guidelines should be developed to guide commercial corporations entering the Canadian criminal justice market on the disclosure of proprietary information, especially in situations where such disclosure is crucial to ensuring a fair trial and upholding the rights of the accused?

Assessing predictive accuracy

5) Where the prosecution in a criminal proceeding seeks to introduce evidence from an AI risk tool, should a burden be imposed on the prosecution to lead evidence relating to the reliability and validity of the AI tool? Should similar burden be imposed on the defence where it seeks to use AI risk assessment evidence as a mitigating factor?

AI-enabled risk assessment tools as expert evidence

6) Considering the opacity of algorithmic risk assessment, particularly in the absence of any ability to cross examine, how can a judge properly scrutinize its processes, examine its integrity, and determine if its expertise can be properly "qualified?" Will the current inability of defence counsel to cross examine "black box" algorithmic risk assessment be critical to its admissibility?

7) Are AI-enabled risk assessments likely to result in frequent litigation and legal challenges that place an undue resource burden on the justice system? In the Court of Justice, where many pleas can be arranged and traversed into the plea court quickly and on the same day, are Crown attorneys, duty counsel and defence counsel going to have the time and resources to litigate the admissibility of algorithmic risk assessments?

8) What systemic policies, practices, and conventions are in play and how might they need to be addressed for any of the following:

   - What is the role of the Crown and what kinds of systemic issues should the Crown look at to ameliorate some of the problems?
   - What can the judiciary do?
   - What can Legal Aid Ontario do?

9) AI-generated risk scores are increasingly relied on as expert evidence in some criminal justice systems (such as the United States) while increasingly restricted in other jurisdictions (such as the European Union). What are the expectations of existing Canadian legal standards for risk assessments in relation to openness, transparency, and reliability, and how do these apply to AI-based risk assessments?

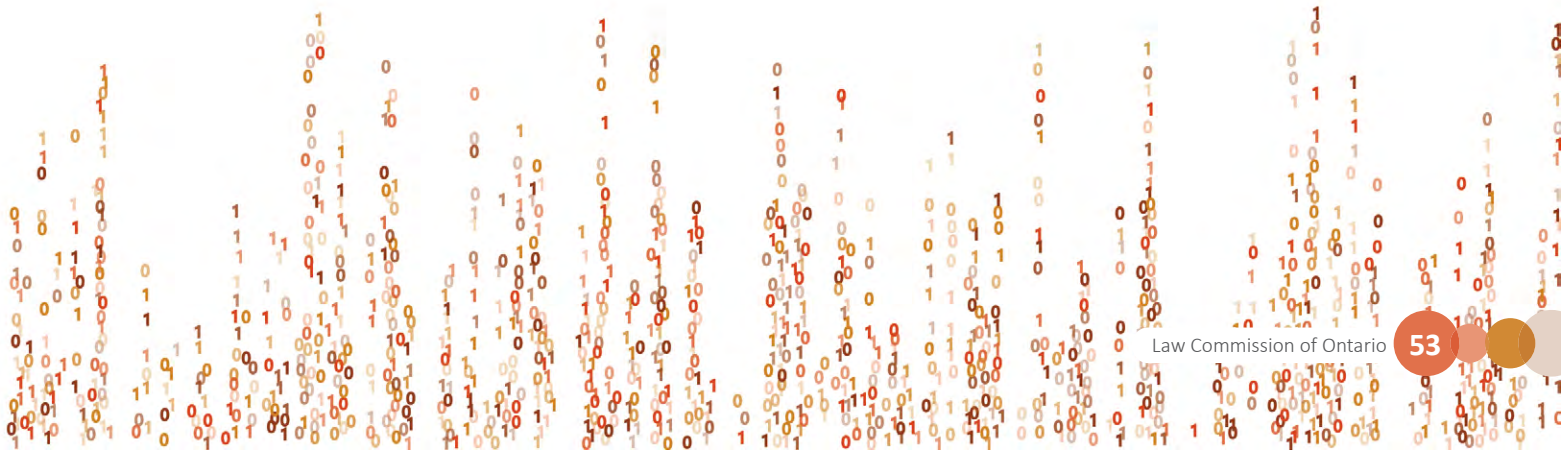
10) Given the varied acceptance of AI-generated risk scores as expert evidence across different courts, what policy measures should be implemented to standardize the scrutiny and admissibility of such evidence in criminal proceedings to safeguard against potential biases and ensure fair treatment of all individuals within the justice system? How can the legal system maintain the required standards of openness, transparency, and reliability to protect the rights of individuals and uphold the integrity of the judicial process?

AI-enabled sentencing and post-sentencing risk assessment

11) How can the Canadian criminal justice system maintain the principle of individualized sentencing while integrating AI-generated risk scores in the decision-making process, ensuring these tools do not override judicial discretion and contribute to potential over-incarceration or stereotyping of offenders?

12) Given the risk of AI recidivism risk assessments facilitating decision-making based on the behaviour of others and potentially contributing to racial discrimination, what measures can be implemented to critically evaluate and adjust the variables used by these tools to prevent the perpetuation of structural racism within the criminal justice system?

13) Can algorithmic risk assessments, producing outputs on the basis of a discriminatory history, have a place in sentencing Indigenous and Black offenders in light of current sentencing caselaw like *Ipeelee* and *Morris*?



Challenging AI-enabled risk assessment in the bail process

14) Defence counsel run bail hearings on serious charges with only a synopsis read in and no disclosure. Is the power of an algorithmic risk assessment stronger or different than a graphic synopsis on a serious charge? If it is, is it fair that accused be advised to wait for disclosure regarding inputs or on an algorithm's operation (and stay in custody longer while counsel attempts to decipher it), or proceed with the risk assessment number looming large in court?

15) Is there a concern about the "relevance" of the risk assessment score if it is based on information that would legally be "irrelevant" at the bail hearing? Does this put an impetus on counsel to request and wait for the inputs?

16) Recent developments in jurisprudence (such as Ipeelee and Morris) and legislation (CCC s. 493.2) require consideration of how historical bias and discrimination have played a role in the disproportionate disadvantage and criminalization of Indigenous and Black communities. If the algorithm cannot consider colonial or racist legacies or histories that may have played a role in formulating the data it processes, does admission of the score circumvent *Criminal Code* s. 493.2? Can counsel successfully argue that given the principles of s493.2, the unexplained risk score should be given less (or no) weight?

17) Do release matrix recommended conditions – such as house arrest or a curfew –amount to boilerplate conditions "inserted by rote" where there is no justification of the score or of the accused's placement in that category?

18) If reasons are to represent a promotion of visibility – including ensuring that racial bias plays no role in the bail decision – can there be any place for evidence that in and of itself does not give any reasons?

19) What legislative or regulatory measures should be introduced to set standards and ensure rigorous testing and validation of these tools for bias before their deployment in the criminal justice system, and how can ongoing oversight be maintained?

5. Endnotes

1 Partnership on AI, *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/ at 7. See generally, partnershiponai.org.

2 See the following cases discussed below: *R. v. Antic* (2017 SCC 27); *R. v. Myers* (2019 SCC 18); and *R. v. Zora* (2020 SCC 14).

3 Danielle Kehl, Priscilla Guo & Samuel Kessler, "Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing" (2017), *Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard Law School*, online: http://nrs.harvard.edu/urn-3:HUL.InstRepos:33746041 at 3.

4 See Sonja B Starr, "Evidence-Based Sentencing and the Scientific Rationalization of Discrimination" (2014) 66:4 Stan L Rev. 803 at 809.

5 See Electronic Privacy Information Center, "AI in the Criminal Justice System," online: https://epic.org/issues/ai/ai-in-the-criminal-justice-system/.

6 Danielle Kehl, Priscilla Guo & Samuel Kessler, "Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing" (2017), *Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard Law School*, online: http://nrs.harvard.edu/urn-3:HUL.InstRepos:33746041 at 9.

7 Research studies on gender and recidivism have found that men have a significantly higher risk of reoffending than women. See for example, Solveig Spjeldnes & Sara Goodkind, "Gender Differences and Offender Reentry: A Review of the Literature" (2009) 48:4 J Offender Rehabilitation 3114, DOI: https://doi.org/10.1080/10509670902850812.

8 In 2014, the then U.S. Attorney General, Eric Holder, warned of the danger in risk scores injecting bias into the court. He noted that while these tools might have been designed with the best intentions, they inadvertently undermine efforts to ensure justice by exacerbating biases that already exist in the criminal justice system. See Eric Holder, "Attorney General Eric Holder Speaks at the National Association of Criminal Defense Lawyers 57th Annual Meeting and 9th State Criminal Justice Network Conference" (11 July 2011), online: https://www.justice.gov/opa/speech/attorney-general-eric-holder-speaks-national-association-criminal-defense-lawyers-57th.

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

10 *Corrections and Conditional Release Act* (SC 1992, c 20), online: https://laws-lois.justice.gc.ca/eng/acts/C-44.6/ at s 24(1).

11 Big data is a term used to refer to extremely large datasets that may require complex electronic data processing methods to analyse for trends and patterns.

12 *Canadian Charter of Rights and Freedoms,* Part I of the *Constitution Act*, 1982, being Schedule B to the *Canada Act 1982* (UK) (1982, c 11).

13 *State v. Loomis* (881 NW2d 749 (Wis 2016)).

14 This sidebar reproduces and lightly edits extracts from Ryan Fritsch, "Chapter 2: Background: The Uneasy Meeting of Code and Law" in Jesse Beatson, Gerald Chan, Jill R. Presser (eds.), *Litigating Artificial Intelligence* (Toronto: Emond Publishing, 2020), online: https://emond.ca/ai21.

15 See Julia Angwin et al, "Machine Bias," ProPublica (23 May 2016), online https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

16 Julia Angwin et al, "Machine Bias," *ProPublica* (23 May 2016), online: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

17 Julia Angwin et al, "Machine Bias," *ProPublica* (23 May 2016), online: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

18 Julia Angwin et al, "Machine Bias," *ProPublica* (23 May 2016), online: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

19 Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge: Harvard University Press, 2016).

20 Julia Angwin et al, "Machine Bias," *ProPublica* (23 May 2016), online: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

21 881 NW2d 749 (Wis 2016), cert denied, Loomis v. Wisconsin 137 S Ct 2290 (2017).

22 Adam Liptak, "Sent to Prison by a Software Program's Secret Algorithms," New York Times (1 May 2017), online: https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html.

23 Julia Angwin et al, "Machine Bias," *ProPublica* (23 May 2016), online: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

24 An early meditation on the complex relationship between adjudicators and AI is found in Jesse Beatson, "AI-Supported Adjudicators: Should Artificial Intelligence Have a Role in Tribunal Adjudication?" (2018) 31:3 Can J Admin L & Prac 307.

25 A readily available example is found in the risk assessment software used by the United States Immigration and Customs Enforcement (ICE) department under the first Trump administration (2016-2020). Changes to the algorithmic review process rapidly tripled the number of immigrants being held in detention. See: Vice.com, "ICE Modified Its 'Risk Assessment' Software So It Automatically Recommends Detention" (June 26 2018), online: https://www.vice.com/en/article/ice-modified-its-risk-assessment-software-so-it-automatically-recommends-detention/.

26 See Law Commission of Ontario, The Rise and Fall of AI and Algorithms In American Criminal Justice: Lessons for Canada (Toronto: October 2020), at section 8, online: https://www.lco-cdo.org/wp-content/uploads/2020/10/Criminal-AI-Paper-Final-Oct-28-2020.pdf.

27 See John Logan Koepke & David G Robinson, "Danger Ahead: Risk Assessment and the Future of Bail Reform" (2018) 393:4 Wash L Rev. 1725 at 1725.

28 See *Ewert v. Canada* (2018 SCC 30).

29 Julia Angwin et al, "Machine Bias," *ProPublica* (23 May 2016), online: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

30 The study cited the examples of two criminal justice subjects—Vernon Prater, a white male, and Brisha Borden, a Black female. Brisha was charged with burglary and petty theft of a bike and scooter valued at $80. Brisha's prior criminal record was for misdemeanours committed while she was a juvenile. Vernon was described as "the more seasoned criminal." After serving five years in prison for armed robbery, Vernon was arrested for shoplifting. But surprisingly, when Vernon and Brisha were assessed for recidivism, Vernon's risk score was 3, indicating "low risk," while Brisha's risk score was 8, indicating "high risk." Julia Angwin et al, "Machine Bias," *ProPublica* (23 May 2016), online: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

31 Julia Angwin et al, "Machine Bias," *ProPublica* (23 May 2016), online: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

32 Julia Angwin et al, "Machine Bias," *ProPublica* (23 May 2016), online: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

33 See comments by Julia Angwin during "Forensic Algorithm: The Future of Technology in the US Legal System, Washington, D.C." (webinar) (12 May 2022), online: https://www.brookings.edu/wp-content/uploads/2021/10/051222-Forensic-Algorithms-Transcript.pdf.

34 Gideon Christian, "Artificial Intelligence, Algorithmic Racism and the Canadian Criminal Justice System," *Slaw* (26 October 2020), online: https://www.slaw.ca/2020/10/26/artificial-intelligence-algorithmic-racism-and-the-canadian-criminal-justice-system/.

35 See Jonny Wakefield, "Black People, Aboriginal Women Over-represented in 'Carding' Police Stops," *Edmonton Journal* (27 June 2017) online: https://edmontonjournal.com/news/local-news/black-people-aboriginal-women-over-represented-in-carding-police-stops.

36 Andrea Nishi, "Privatizing Sentencing: A Delegation Framework for Recidivism Risk Assessment" (2019) 119:6 Colum L Rev. 1671 at 1681.

37 Robert Brauneis & Ellen P Goodman, "Algorithmic Transparency for the Smart City" (2018) 20 Yale JL & Tech 103 at 109.

38 Gideon Christian, "Artificial Intelligence, Algorithmic Racism and the Canadian Criminal Justice System," Slaw (26 October 2020), online: https://www.slaw.ca/2020/10/26/artificial-intelligence-algorithmic-racism-and-the-canadian-criminal-justice-system/.

39 Facial recognition software developed by commercial corporations has been shown to achieve 99% accuracy in recognizing white male faces, but it has a 35% error rate in recognizing darker-skinned women. This accuracy gap has been attributed to the fact that the technology is trained predominantly on data of white male faces. Hence, deploying the technology to darker-skinned faces results in a lower accuracy rate. In fact, the darker the skin, the more flawed the results generated by the software. See Steve Lohr, "Facial Recognition Is Accurate, if You're a White Guy," *The New York Times* (9 February 2018), online: https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

40 See *Ewert v. Canada* (2018 SCC 30). In *Ewert,* an Indigenous man serving consecutive life sentences successfully challenged the use by the Correctional Services Canada (CSC) of psychological and actuarial tools in his risk assessment. The result of the risk assessment formed part of the factors that were considered in recommending a higher security classification for this Indigenous offender. However, the tools used by the CSC were developed and tested on predominantly non-Indigenous populations.

41 In Canada, AI-based facial recognition technology has been used in the criminal justice system and even in the immigration system. Its initial use by some Canadian police departments was clandestine and became controversial when made public. See Alex Boutilier, "RCMP Broke Privacy Laws in Using Controversial Clearview AI Facial Recognition Tools, Watchdog Says," *Toronto Star* (10 June 2021), online: https://www.thestar.com/politics/federal/rcmp-broke-privacy-laws-in-using-controversial-clearview-ai-facial-recognition-tools-watchdog-says/article_817e9c66-808a-5c17-9c2c-6861f87cd7a0.html. See also *Barre v. Canada (Citizenship and Immigration)* (2022 FC 1078).

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

43 Julia Angwin et al, "Machine Bias," *ProPublica* (23 May 2016), online: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

44 See *May v. Ferndale Institution* (2005 SCC 82) at para 76.

45 *State v. Loomis* (881 NW2d 749 (Wis 2016)).

46 Rediet Abebe et al, "Adversarial Scrutiny of Evidentiary Statistical Software" (paper delivered at FAccT '22, Seoul, 20 June 2022) in *FAccT '22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (New York: ACM, 2022) 1733 at 1733, DOI: https://doi.org/10.1145/3531146.3533228.

47 *People v. Superior Court (Chubbs)* (No B258569, 2015 WL 139069 (Cal Ct App Jan 9, 2015)).

48 *People v. Superior Court (Chubbs)* (No B258569, 2015 WL 139069 (Cal Ct App Jan 9, 2015)) at 4.

49 Rebecca Wexler, "Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System" (2018) 70 Stan L Rev. 1343, DOI: http://dx.doi.org/10.2139/ssrn.2920883 at 1360.

50 *Justice in Forensic Algorithms Act of 2021*, HR2438, 117th Cong (2021), online: https://www.congress.gov/bill/117th-congress/house-bill/2438.

51 *Justice in Forensic Algorithms Act of 2021*, HR2438, 117th Cong (2021), online: https://www.congress.gov/bill/117th-congress/house-bill/2438 at s 2(b)(1).

52 *May v. Ferndale Institution* (2005 SCC 82).

53 *May v. Ferndale Institution* (2005 SCC 82) at para 92.

54 *R. v. Stinchcombe* (1991 CanLII 45 (SCC), [1991] 3 SCR 326).

55 *May v. Ferndale Institution* (2005 SCC 82) at paras 89–91. See also *R. v. Stinchcombe* (1991 CanLII 45 (SCC), [1991] 3 SCR 326).

56 *Corrections and Conditional Release Act* (SC 1992, c 20), online: https://laws-lois.justice.gc.ca/eng/acts/C-44.6/ at s 27(1).

57 *May v. Ferndale Institution* (2005 SCC 82) at para 117.

58 The *Stinchcombe* standard applies in criminal cases. The standard is generally understood as higher in the criminal than administrative context. See *R. v. Stinchcombe* (1991 CanLII 45 (SCC), [1991] 3 SCR 326).

59 *R. v. BHD* (2006 SKPC 32).

60 *R. v. BHD* (2006 SKPC 32) at para 76.

61 *R. v. BHD* (2006 SKPC 32) at para 61.

62 *R. v. BHD* (2006 SKPC 32) at paras 51–52.

63 See Paul W Grimm, Maura R Grossman & Gordon V Cormack, "Artificial Intelligence as Evidence" (2021) 19:1 Northwestern J Tech & IP 9 at 94.

64 See Paul W Grimm, Maura R Grossman & Gordon V Cormack, "Artificial Intelligence as Evidence" (2021) 19:1 Northwestern J Tech & IP 9 at 94.

65 See Julia Angwin et al, "Machine Bias," *ProPublica* (23 May 2016), online: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; Alexandra Chouldechova, "Fair Prediction With Disparate Impact: A Study of Bias in Recidivism Prediction Instruments," *arXiv*. (24 October 2016), DOI: https://doi.org/10.48550/arXiv.1610.07524; Kelly Hannah-Moffatt, "Actuarial Sentencing: An 'Unsettled' Proposition," (2013) 30:2 Justice Quarterly 270, DOI: https://doi.org/10.1080/07418825.2012.682603 at 279–82; John Monahan & Jennifer L Skeem, "Risk Assessment in Criminal Sentencing" (2016) 12:1 Annual Rev. Clinical Psychology 498; Jon Kleinberg, Sendhil Mullainathan & Manish Raghavan, "Inherent Trade-offs in the Fair Determination of Risk Scores," *arXiv*. (17 November 2016), DOI: https://doi.org/10.48550/arXiv.1609.05807.

66 Tracy Fass et al, "The LSI-R and the COMPAS: Validation Data on Two Risk-Needs Tools" (2008) 35:9 Crim Justice & Behavior 1095, DOI: https://doi.org/10.1177/0093854808320497 at 1097.

67 Jeff Larson et al, "How We Analyzed the COMPAS Recidivism Algorithm," *ProPublica* (23 May 2016), online: https://www.propublica.org/article/how-we-analyzed-the-compas-recidivism-algorithm>. Dressel, Julia J, *Accuracy and Racial Biases of Recidivism Prediction Instruments* (Undergraduate thesis, Dartmouth College, 2017), online: https://digitalcommons.dartmouth.edu/senior_theses/121.

68 Rediet Abebe et al, "Adversarial Scrutiny of Evidentiary Statistical Software" (paper delivered at FAccT '22, Seoul, 20 June 2022) in *FAccT '22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (New York: ACM, 2022) 1733 at 1733, DOI: https://doi.org/10.1145/3531146.3533228 at 1736–37..

69 Rediet Abebe et al, "Adversarial Scrutiny of Evidentiary Statistical Software" (paper delivered at FAccT '22, Seoul, 20 June 2022) in *FAccT '22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (New York: ACM, 2022) 1733 at 1733, DOI: https://doi.org/10.1145/3531146.3533228 at 1736.

70 An example here is the validation studies conducted for TrueAlle DNA software, developed by Cybergenetics. Abebe et al noted that of the eight validation studies on the software, seven of the studies were co-authored by Mark Perlin, the CEO of the very company that developed the software. Two employees of Cybergenetics were acknowledged for their guidance and contributions to the remaining study, which did not include Mark Perlin. See Rediet Abebe et al, "Adversarial Scrutiny of Evidentiary Statistical Software" (paper delivered at FAccT '22, Seoul, 20 June 2022) in *FAccT '22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (New York: ACM, 2022) 1733 at 1733, DOI: https://doi.org/10.1145/3531146.3533228 at 1736.

71 Rediet Abebe et al, "Adversarial Scrutiny of Evidentiary Statistical Software" (paper delivered at FAccT '22, Seoul, 20 June 2022) in *FAccT '22: Proceedings of the 2022 ACM Conference on Fairness, Accountability, and Transparency* (New York: ACM, 2022) 1733 at 1733, DOI: https://doi.org/10.1145/3531146.3533228 at 1737.

72 *Justice in Forensic Algorithms Act of 2021*, HR2438, 117th Cong (2021), online: https://www.congress.gov/bill/117th-congress/house-bill/2438.

73 *Justice in Forensic Algorithms Act of 2021*, HR2438, 117th Cong (2021), online: https://www.congress.gov/bill/117th-congress/house-bill/2438 at ss 2(a)(1–2).

74 *Justice in Forensic Algorithms Act of 2021*, HR2438, 117th Cong (2021), online: https://www.congress.gov/bill/117th-congress/house-bill/2438 at s 2(f).

75 LCO, ***Introduction and Summary: LCO AI in Criminal Justice Project*** (Toronto: April 2025), online: https://www.lco-cdo.org/CrimAI.

76 LCO, ***AI at Trial and On Appeal: Paper 4 in the LCO AI in Criminal Justice Project*** (Toronto: April 2025), online: https://www.lco-cdo.org/CrimAI.

77 *R. v. Mohan* (1994 CanLII 80 (SCC), [1994] 2 SCR 9) at para 32.

78 *R. v. BHD* (2006 SKPC 32).

79 *R. v. BHD* (2006 SKPC 32).

80 *R. v. Mohan* (1994 CanLII 80 (SCC), [1994] 2 SCR 9).

81 *R. v. BHD* (2006 SKPC 32) at para 59.

82 *R. v. Collins* (2001 CanLII 24124 (ONCA)) at para 17.

83 *R. v. Alexander* (2006 CanLII 26480 (ON SC)) at para 22.

84 Doaa Abu Elyounes, "Bail or Jail? Judicial versus Algorithmic Decision Making in the Pretrial System" (2020) 24:2 Science & Technology L Rev. 376, DOI: https://doi.org/10.7916/stlr.v21i2.6838 at 395.

85 Han-Wei Liu, Ching-Fu Lin & Yu-Jie Chen, "Beyond *State v. Loomis*: Artificial Intelligence, Government Algorithmization and Accountability" (2019) 27:2 Intl JL & Information Tech 122 at 136.

86 Kay Firth-Butterfield & Karen Silverman, "Artificial Intelligence – Foundational Issues and Glossary" in *Artificial Intelligence and the Courts: Materials For Judges* (Washington, DC: American Association for the Advancement of Science, 2022), DOI: https://doi.org/10.1126/aaas.adf0782 at 6.

87 Kay Firth-Butterfield & Karen Silverman, "Artificial Intelligence – Foundational Issues and Glossary" in *Artificial Intelligence and the Courts: Materials For Judges* (Washington, DC: American Association for the Advancement of Science, 2022), DOI: https://doi.org/10.1126/aaas.adf0782 at 7.

88 Kay Firth-Butterfield & Karen Silverman, "Artificial Intelligence – Foundational Issues and Glossary" in *Artificial Intelligence and the Courts: Materials For Judges* (Washington, DC: American Association for the Advancement of Science, 2022), DOI: https://doi.org/10.1126/aaas.adf0782 at 8.

89 *White Burgess Langille Inman v. Abbott and Haliburton Co* (2015 SCC 23) at para 14.

90 David M Paciocco, Palma Paciocco & Lee Stuesser, *The Law Of Evidence*, 8th ed (Toronto: Irwin Law, 2020) at 234–235.

91 *White Burgess Langille Inman v. Abbott and Haliburton Co* (2015 SCC 23) at para 15.

92 *R. v. Phillips* (2017 ONCA 752) paras 124–126.

93 *R. v. BHD* (2006 SKPC 32) at para 59.

94 *R. v. Amara* (2010 ONSC 251). See also *R. v. Abbey* (2009 ONCA 624) at para 71.

95 *White Burgess Langille Inman v. Abbott and Haliburton Co* (2015 SCC 23).

96 *White Burgess Langille Inman v. Abbott and Haliburton Co* (2015 SCC 23) at para 23.

97 *White Burgess Langille Inman v. Abbott and Haliburton Co* (2015 SCC 23) at para 24, quoting *R. v. Abbey* (2009 ONCA 624) at para 76. See also *R. v. Hoggard* (2021 ONSC 5365) at para 68.

98 AI Now, "Litigating Algorithms: Challenging Government Use Of Algorithmic Decision Systems" (2018), online: https://ainowinstitute.org/publication/litigating-algorithms-3 at 14.

99 *R. v. Abbey* (2009 ONCA 624) at paras 82–84.

100 Julia Angwin et al, "Machine Bias," *ProPublica* (23 May 2016), online: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

101 Sandra G Mayson, "Bias in, Bias Out" (2019) 128:8 Yale LJ 2218 at 2251–2252.

102 Sandra G Mayson, "Bias in, Bias Out" (2019) 128:8 Yale LJ 2218 at 2251–2252.

103 Sandra G Mayson, "Bias in, Bias Out" (2019) 128:8 Yale LJ 2218 at 2251–2252.

104 David M Paciocco, Palma Paciocco & Lee Stuesser, *The Law Of Evidence*, 8th ed (Toronto: Irwin Law, 2020) at 256.

105 David M Paciocco, Palma Paciocco & Lee Stuesser, *The Law Of Evidence*, 8th ed (Toronto: Irwin Law, 2020) at 257.

106 Megan T Stevenson, "Assessing Risk Assessment In Action" (2018) 103 Minnesota L Rev. 303 at 325.

107 Julia Angwin et al, "Machine Bias," *ProPublica* (23 May 2016), online: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

108 David M Paciocco, Palma Paciocco & Lee Stuesser, *The Law Of Evidence*, 8th ed (Toronto: Irwin Law, 2020) at 257–58.

109 *White Burgess Langille Inman v. Abbott and Haliburton Co* (2015 SCC 23) at paras 46, 53.

110 David M Paciocco, Palma Paciocco & Lee Stuesser, *The Law Of Evidence*, 8th ed (Toronto: Irwin Law, 2020) at 259.

111 *R. v. Thomas* (2006 CanLII 1012 (ONSC)) at para 11.

112 Richard Berk & Jordan Hyatt, "Machine Learning Forecasts of Risk to Inform Sentencing Decisions" (2015) 27:4 Fed Sentencing Reporter 222 at 223.

113 Doaa Abu Elyounes, "Bail or Jail? Judicial versus Algorithmic Decision Making in the Pretrial System" (2020) 24:2 Science & Tech L Rev. 376, DOI: https://doi.org/10.7916/stlr.v21i2.6838 at 392.

114 Doaa Abu Elyounes, "Bail or Jail? Judicial versus Algorithmic Decision Making in the Pretrial System" (2020) 24:2 Science & Tech L Rev. 376, DOI: https://doi.org/10.7916/stlr.v21i2.6838 at 393.

115 Stephanie J Lacambra, Jeanna Matthews & Kit Walsh, "Opening the Black Box: Defendants' Rights to Confront Forensic Software," *The Champion* (May 2018), online: https://www.eff.org/document/opening-black-box-defendants-rights-confront-forensic-software at 34. See also Law Commission of Ontario, *The Rise and Fall of AI and Algorithms in American Criminal Justice: Lessons for Canada* (Toronto: LCO, 2020) at 32.

116 Stephanie J Lacambra, Jeanna Matthews & Kit Walsh, "Opening the Black Box: Defendants' Rights to Confront Forensic Software," *The Champion* (May 2018), online: https://www.eff.org/document/opening-black-box-defendants-rights-confront-forensic-software at 29.

117 Doaa Abu Elyounes, "Bail or Jail? Judicial versus Algorithmic Decision Making in the Pretrial System" (2020) 24:2 Science & Tech L Rev. 376, DOI: https://doi.org/10.7916/stlr.v21i2.6838 at 395–396.

118 Doaa Abu Elyounes, "Bail or Jail? Judicial versus Algorithmic Decision Making in the Pretrial System" (2020) 24:2 Science & Tech L Rev. 376, DOI: https://doi.org/10.7916/stlr.v21i2.6838 at 396.

119 Han-Wei Liu, Ching-Fu Lin & Yu-Jie Chen, "Beyond *State v. Loomis*: Artificial Intelligence, Government Algorithmization and Accountability" (2019) 27:2 Intl JL & Information Tech 122 at 136.

120 Angèle Christin, "Predictive Algorithms and Criminal Sentencing" in Daniel Bessner & Nicolas Guilhot, eds, *The Decisionist Imagination: Sovereignty, Social Science and Democracy in the 20th Century* (New York: Berghahn, 2018) 272 at 283.

121 Angèle Christin, "Predictive Algorithms and Criminal Sentencing" in Daniel Bessner & Nicolas Guilhot, eds, *The Decisionist Imagination: Sovereignty, Social Science and Democracy in the 20th Century* (New York: Berghahn, 2018) 272 at 283.

122 *R. v. Bingley* (2017 SCC 12) para 13.

123 *White Burgess Langille Inman v. Abbott and Haliburton Co* (2015 SCC 23) at para 32.

124 *White Burgess Langille Inman v. Abbott and Haliburton Co* (2015 SCC 23) at para 48.

125 Angèle Christin, "Predictive Algorithms and Criminal Sentencing" in Daniel Bessner & Nicolas Guilhot, eds, *The Decisionist Imagination: Sovereignty, Social Science and Democracy in the 20th Century* (New York: Berghahn, 2018) 272 at 286.

126 Han-Wei Liu, Ching-Fu Lin & Yu-Jie Chen, "Beyond *State v. Loomis*: Artificial Intelligence, Government Algorithmization and Accountability" (2019) 27:2 Intl JL & Information Tech 122 at 137–138, quoting Brent Daniel Mittelstadt et al, "The Ethics of Algorithms: Mapping the Debate" (2016) Big Data & Society, DOI: https://doi.org/10.1177/2053951716679679.

127 Han-Wei Liu, Ching-Fu Lin & Yu-Jie Chen, "Beyond *State v. Loomis*: Artificial Intelligence, Government Algorithmization and Accountability" (2019) 27:2 Intl JL & Information Tech 122 at 138.

128 Deployed with the goal of reducing discrimination, AI-powered tools may in fact help to reveal bias in existing technological and non-technological risk assessment systems. See Law Commission of Ontario, *The Rise and Fall of AI and Algorithms in American Criminal Justice: Lessons for Canada* (Toronto: LCO, 2020) at 21. See generally Jon Kleinberg et al, "Discrimination in the Age of Algorithms" (2019), 2018:10 J Leg Analysis 114, DOI: https://doi.org/10.1093/jla/laz001.

129 *White Burgess Langille Inman v. Abbott and Haliburton Co* (2015 SCC 23) at para 23.

130 David M Paciocco, Palma Paciocco & Lee Stuesser, *The Law Of Evidence*, 8th ed (Toronto: Irwin Law, 2020) at 266.

131 *White Burgess Langille Inman v. Abbott and Haliburton Co* (2015 SCC 23) at para 23.

132 David M Paciocco, Palma Paciocco & Lee Stuesser, *The Law Of Evidence*, 8th ed (Toronto: Irwin Law, 2020) at 267–268.

133 *State v. Loomis* (881 NW2d 749 (Wis 2016)) at para 97.

134 *White Burgess Langille Inman v. Abbott and Haliburton Co* (2015 SCC 23) at para 54.

135 *R. v. Abbey* (2009 ONCA 624) at para 87.

136 See above Julia Angwin et al, "Machine Bias," *ProPublica* (23 May 2016), online: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing; Sandra G Mayson, "Bias in, Bias Out" (2019) 128:8 Yale LJ 2218 at 2251–2252; Megan T Stevenson, "Assessing Risk Assessment In Action" (2018) 103 Minnesota L Rev. 303 at 325–26; Sonja B Starr, "Evidence-Based Sentencing and the Scientific Rationalization of Discrimination" (2014) 66:4 Stan L Rev. 803 at 806; Law Commission of Ontario, *The Rise and Fall of AI and Algorithms in American Criminal Justice: Lessons for Canada* (Toronto: LCO, 2020) at 23; Han-Wei Liu, Ching-Fu Lin & Yu-Jie Chen, "Beyond *State v. Loomis*: Artificial Intelligence, Government Algorithmization and Accountability" (2019) 27:2 Intl JL & Information Tech 122 at 138; Angèle Christin, "Predictive Algorithms and Criminal Sentencing" in Daniel Bessner & Nicolas Guilhot, eds, *The Decisionist Imagination: Sovereignty, Social Science and Democracy in the 20th Century* (New York: Berghahn, 2018) 272 at 283.

137 *Criminal Code* (RSC 1985, c C-46), online: https://laws-lois.justice.gc.ca/eng/acts/c-46/ at s 718.

138 *Criminal Code* (RSC 1985, c C-46), online: https://laws-lois.justice.gc.ca/eng/acts/c-46/ at s 718.1.

139 *Criminal Code* (RSC 1985, c C-46), online: https://laws-lois.justice.gc.ca/eng/acts/c-46/ at s 718(d).

140 *Criminal Code* (RSC 1985, c C-46), online: https://laws-lois.justice.gc.ca/eng/acts/c-46/ at s 718(c).

141 David M Paciocco, Palma Paciocco & Lee Stuesser, *The Law Of Evidence*, 8th ed (Toronto: Irwin Law, 2020) at 275.

142 David M Paciocco, Palma Paciocco & Lee Stuesser, *The Law Of Evidence*, 8th ed (Toronto: Irwin Law, 2020) at 275, quoting *R. v. Abbey* (2009 ONCA 624) at para 90.

143 Leah Wisser, "Pandora's Algorithmic Black Box: The Challenges of Using Algorithmic Risk Assessments in Sentencing" (2019) 56:4 Am Crim L Rev. 1811 at 1824, quoting Frank Pasquale, "Secret Algorithms Threaten the Rule of Law," *MIT Technology Review* (1 June 2017), online: https://www.technologyreview.com/2017/06/01/151447/secret-algorithms-threaten-the-rule-of-law/.

144 Han-Wei Liu, Ching-Fu Lin & Yu-Jie Chen, "Beyond *State v. Loomis*: Artificial Intelligence, Government Algorithmization and Accountability" (2019) 27:2 Intl JL & Information Tech 122 at 133.

145 S Casey Hill, David M Tanovich & Louis P Strezos, *McWilliams' Canadian Criminal Evidence*, 5th ed (Toronto: Thomson Reuters, 2013) at 36:15.

146 S Casey Hill, David M Tanovich & Louis P Strezos, *McWilliams' Canadian Criminal Evidence*, 5th ed (Toronto: Thomson Reuters, 2013) at 36:15.

147 Partnership on AI, *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/ at 23.

148 Partnership on AI, *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/ at 23.

149 Danielle Citron, "(Un)fairness of Risk Scores in Criminal Sentencing," *Forbes* (13 July 2026), online: https://www.forbes.com/sites/daniellecitron/2016/07/13/unfairness-of-risk-scores-in-criminal-sentencing/?sh=5e5e2a94ad21.

150 Angèle Christin, "Predictive Algorithms and Criminal Sentencing" in Daniel Bessner & Nicolas Guilhot, eds, *The Decisionist Imagination: Sovereignty, Social Science and Democracy in the 20th Century* (New York: Berghahn, 2018) 272 at 283.

151 Leah Wisser, "Pandora's Algorithmic Black Box: The Challenges of Using Algorithmic Risk Assessments in Sentencing" (2019) 56:4 Am Crim L Rev. 1811 at 1824.

152 Law Commission of Ontario, *The Rise and Fall of AI and Algorithms in American Criminal Justice: Lessons for Canada* (Toronto: LCO, 2020) at 26.

153 David M Paciocco, Palma Paciocco & Lee Stuesser, *The Law Of Evidence*, 8th ed (Toronto: Irwin Law, 2020) at 275, quoting *R. v. Abbey* (2009 ONCA 624) at para 91.

154 Law Commission of Ontario, *The Rise and Fall of AI and Algorithms in American Criminal Justice: Lessons for Canada* (Toronto: LCO, 2020) at 25.

155 Doaa Abu Elyounes, "Bail or Jail? Judicial versus Algorithmic Decision Making in the Pretrial System" (2020) 24:2 Science & Tech L Rev. 376, DOI: https://doi.org/10.7916/stlr.v21i2.6838 at 380.

156 *R. v. Kanagasivam* (2016 ONSC 2250) at para 42.

157 *R. v. Kanagasivam* (2016 ONSC 2250) at para 41.

158 *R. v. Kanagasivam* (2016 ONSC 2250) at para 44.

159 *R. v. Hoggard* (2022 ONSC 713) at para 50.

160 *R. v. Hoggard* (2022 ONSC 713) at para 50.

161 Doaa Abu Elyounes, "Bail or Jail? Judicial versus Algorithmic Decision Making in the Pretrial System" (2020) 24:2 Science & Tech L Rev. 376, DOI: https://doi.org/10.7916/stlr.v21i2.6838 at 392.

162 Julia Angwin et al, "Machine Bias," *ProPublica* (23 May 2016), online: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. See also Danielle Citron, "(Un)fairness of Risk Scores in Criminal Sentencing," *Forbes* (13 July 2026), online: https://www.forbes.com/sites/daniellecitron/2016/07/13/unfairness-of-risk-scores-in-criminal-sentencing/?sh=5e5e2a94ad21.

163 See for example, *R. v. Charlette (JJ)* (2015 MBCA 32) at paras 31, 51; *R. v. Fehr* (2013 MBQB 274) at para 28; *R. v. CG* (2022 ABKB 696) at para 58; *R c Gordon* (2021 QCCQ 12998) at para 27.

164 *Criminal Code* (RSC 1985, c C-46), online: https://laws-lois.justice.gc.ca/eng/acts/c-46/ at s 718.

165 *Criminal Code* (RSC 1985, c C-46), online: https://laws-lois.justice.gc.ca/eng/acts/c-46/ at s 718.1.

166 *R. v. Jackson* (2018 ONSC 2527) at para 3 (emphasis added).

167 *R. v. Jackson* (2018 ONSC 2527) at para 103.

168 *State v. Loomis* (881 NW2d 749 (Wis 2016)).

169 *State v. Loomis* (881 NW2d 749 (Wis 2016)).

170 Kelly Hannah-Moffatt, "Actuarial Sentencing: An 'Unsettled' Proposition," (2013) 30:2 Justice Quarterly 270, DOI: https://doi.org/10.1080/07418825.2012.682603 at 277

171 Kelly Hannah-Moffatt, "Actuarial Sentencing: An 'Unsettled' Proposition," (2013) 30:2 Justice Quarterly 270, DOI: https://doi.org/10.1080/07418825.2012.682603 at 278.

172 Laurel Eckhouse et al, "Layers of Bias: A Unified Approach for Understanding Problems with Risk Assessment" (2019) 46:2 Crim Justice & Behavior 185 at 198.

173 *Criminal Code* (RSC 1985, c C-46), online: https://laws-lois.justice.gc.ca/eng/acts/c-46/ at s 718.1.

174 Laurel Eckhouse et al, "Layers of Bias: A Unified Approach for Understanding Problems with Risk Assessment" (2019) 46:2 Crim Justice & Behavior 185 at 192.

175 Laurel Eckhouse et al, "Layers of Bias: A Unified Approach for Understanding Problems with Risk Assessment" (2019) 46:2 Crim Justice & Behavior 185 at 193.

176 See Cassie Spohn, *How Do Judges Decide? The Search for Fairness and Justice in Punishment*, 2nd ed (Los Angeles: SAGE, 2009); Cassia Spohn, "Racial Disparities in Prosecution, Sentencing, and Punishment" in Sandra M Bucerius & Michael Tonry, eds, *The Oxford Handbook of Ethnicity, Crime, and Immigration* (Oxford: Oxford University Press, 2014) 166.

177 Laurel Eckhouse et al, "Layers of Bias: A Unified Approach for Understanding Problems with Risk Assessment" (2019) 46:2 Crim Justice & Behavior 185 at 193.

178 Law Commission of Ontario, *The Rise and Fall of AI and Algorithms in American Criminal Justice: Lessons for Canada* (Toronto: LCO, 2020) at 21.

179 Sandra G Mayson, "Bias in, Bias Out" (2019) 128:8 Yale LJ 2218 at 2229.

180 Sandra G Mayson, "Bias in, Bias Out" (2019) 128:8 Yale LJ 2218 at 2234.

181 Sandra G Mayson, "Bias in, Bias Out" (2019) 128:8 Yale LJ 2218 at 2224.

182 Sandra G Mayson, "Bias in, Bias Out" (2019) 128:8 Yale LJ 2218 at 2224.

183 Sandra G Mayson, "Bias in, Bias Out" (2019) 128:8 Yale LJ 2218 at 2221.

184 *R. v. Morris* (2021 ONCA 680).

185 *R. v. Morris* (2021 ONCA 680) at para 1.

186 *R. v. Morris* (2021 ONCA 680) at para 42.

187 *R. v. Morris* (2021 ONCA 680) at para 87.

188 *R. v. Morris* (2021 ONCA 680) at para 97.

189 See *R. v. Morris* (2021 ONCA 680) at para 39.

190 *R. v. Ipeelee* (2012 SCC 13) at para 65.

191 *R. v. Ipeelee* (2012 SCC 13) at para 67.

192 *R. v. Elliott* (2015 BCCA 295) at paras 10, 16.

193 *R. v. Ipeelee* (2012 SCC 13) at para 57.

194 *R. v. Ipeelee* (2012 SCC 13) at para 56.

195 *Criminal Code* (RSC 1985, c C-46), online: https://laws-lois.justice.gc.ca/eng/acts/c-46/ at s 718.2(e).

196 *R. v. Ipeelee* (2012 SCC 13) at para 59.

197 *R. v. Ipeelee* (2012 SCC 13) at para 60.

198 *R. v. Ipeelee* (2012 SCC 13) at para 73.

199 *R. v. Ipeelee* (2012 SCC 13) at para 59.

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

201 *R. v. Natomagan* (2022 ABCA 48) at para 113.

202 Gary Trotter *The Law of Bail in Canada*, 3rd ed (Thomson Reuters: Toronto, 2010) at 5:1.

203 Gary Trotter *The Law of Bail in Canada*, 3rd ed (Thomson Reuters: Toronto, 2010) at 5:1.

204 S Casey Hill, David M Tanovich & Louis P Strezos, *McWilliams' Canadian Criminal Evidence*, 5th ed (Toronto: Thomson Reuters, 2013) at 35:1.

205 *R. v. Antic* (2017 SCC 27) at para 66.

206 *R. v. Antic* (2017 SCC 27) at para 66.

207 *R. v. Myers* (2019 SCC 18) at para 51.

208 Law Commission of Ontario, *The Rise and Fall of AI and Algorithms in American Criminal Justice: Lessons for Canada* (Toronto: LCO, 2020) at 32.

209 Law Commission of Ontario, *The Rise and Fall of AI and Algorithms in American Criminal Justice: Lessons for Canada* (Toronto: LCO, 2020) at 19.

210 Doaa Abu Elyounes, "Bail or Jail? Judicial versus Algorithmic Decision Making in the Pretrial System" (2020) 24:2 Science & Tech L Rev. 376, DOI: https://doi.org/10.7916/stlr.v21i2.6838 at 392.

211 Richard Berk & Jordan Hyatt, "Machine Learning Forecasts of Risk to Inform Sentencing Decisions" (2015) 27:4 Fed Sentencing Reporter 222 at 223.

212 Gary Trotter *The Law of Bail in Canada*, 3rd ed (Thomson Reuters: Toronto, 2010) at 5:20.

213 *Criminal Code* (RSC 1985, c C-46), online: https://laws-lois.justice.gc.ca/eng/acts/c-46/ at s 515(10)(b) (emphasis added).

214 Sandra G Mayson, "Bias in, Bias Out" (2019) 128:8 Yale LJ 2218 at 2252.

215 Sandra G Mayson, "Bias in, Bias Out" (2019) 128:8 Yale LJ 2218 at 2251-2252.

216 Law Commission of Ontario, *The Rise and Fall of AI and Algorithms in American Criminal Justice: Lessons for Canada* (Toronto: LCO, 2020) at 25.

217 Law Commission of Ontario, *The Rise and Fall of AI and Algorithms in American Criminal Justice: Lessons for Canada* (Toronto: LCO, 2020) at 25 (emphasis in original).

218 Gary Trotter *The Law of Bail in Canada*, 3rd ed (Thomson Reuters: Toronto, 2010) at 5:25.

219 *R. v. Downey* ([2018] OJ No 6133 (SCJ)) at para 10.

220 *R. v. Downey* ([2018] OJ No 6133 (SCJ)) at para 10.

221 Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy* (London: Penguin, 2016) at 30.

222 *R. v. Downey* ([2018] OJ No 6133 (SCJ)).

223 Law Commission of Ontario, *The Rise and Fall of AI and Algorithms in American Criminal Justice: Lessons for Canada* (Toronto: LCO, 2020) at 21.

224 *R. v. EB* (2020 ONSC 4383) at para 38.

225 *Criminal Code* (RSC 1985, c C-46), online: https://laws-lois.justice.gc.ca/eng/acts/c-46/ at s 493(2)(a).

226 *R. v. Natomagan* (2022 ABCA 48) at para 108, quoting *R. v. Gladue* ([1999] 1 SCR 68) at para 65.

227 *R. v. Natomagan* (2022 ABCA 48) at para 108.

228 *R. v. EB* (2020 ONSC 4383) at para 38.

229 *R. v. Papequash* (2021 ONSC 727) at para 22.

230 *Criminal Code* (RSC 1985, c C-46), online: https://laws-lois.justice.gc.ca/eng/acts/c-46/ at s 493(2)(b).

231 *R. v. AA,* (2022 ONSC 4310) at para 45.

232 *R. v. AA,* (2022 ONSC 4310) at para 46.

233 *R. v. AA,* (2022 ONSC 4310) at para 49.

234 *R. v. AA,* (2022 ONSC 4310) at para 51.

235 *R. v. AA,* (2022 ONSC 4310) at para 51.

236 *R. v. AA,* (2022 ONSC 4310) at para 70.

237 S Casey Hill, David M Tanovich & Louis P Strezos, *McWilliams' Canadian Criminal Evidence*, 5th ed (Toronto: Thomson Reuters, 2013) at 35:5.

238 S Casey Hill, David M Tanovich & Louis P Strezos, *McWilliams' Canadian Criminal Evidence*, 5th ed (Toronto: Thomson Reuters, 2013) at 35:1.

239 S Casey Hill, David M Tanovich & Louis P Strezos, *McWilliams' Canadian Criminal Evidence*, 5th ed (Toronto: Thomson Reuters, 2013) at 35:14.

240 *Criminal Code* (RSC 1985, c C-46), online: https://laws-lois.justice.gc.ca/eng/acts/c-46/ at s493.1.

241 *R. v. Zora* (2020 SCC 14) at para 6.

242 *R. v. Zora* (2020 SCC 14) at para 6.

243 *R. v. Zora* (2020 SCC 14) at para 88.

244 *R. v. Zora* (2020 SCC 14) at para 85.

245 *R. v. Zora* (2020 SCC 14) at para 100.

246 Law Commission of Ontario, *The Rise and Fall of AI and Algorithms in American Criminal Justice: Lessons for Canada* (Toronto: LCO, 2020) at 15, 18.

247 Law Commission of Ontario, *The Rise and Fall of AI and Algorithms in American Criminal Justice: Lessons for Canada* (Toronto: LCO, 2020) at 18, 27.

248 Megan T Stevenson, "Assessing Risk Assessment In Action" (2018) 103 Minnesota L Rev. 303 at 316.

249 *R. v. Zora* (2020 SCC 14) at para 88.

250 *R. v. Lich* (2022 ONSC 4390) at para 32; Gary Trotter *The Law of Bail in Canada*, 3rd ed (Thomson Reuters: Toronto, 2010) at 5:28.

251 *R. v. Lich* (2022 ONSC 4390) at para 35.

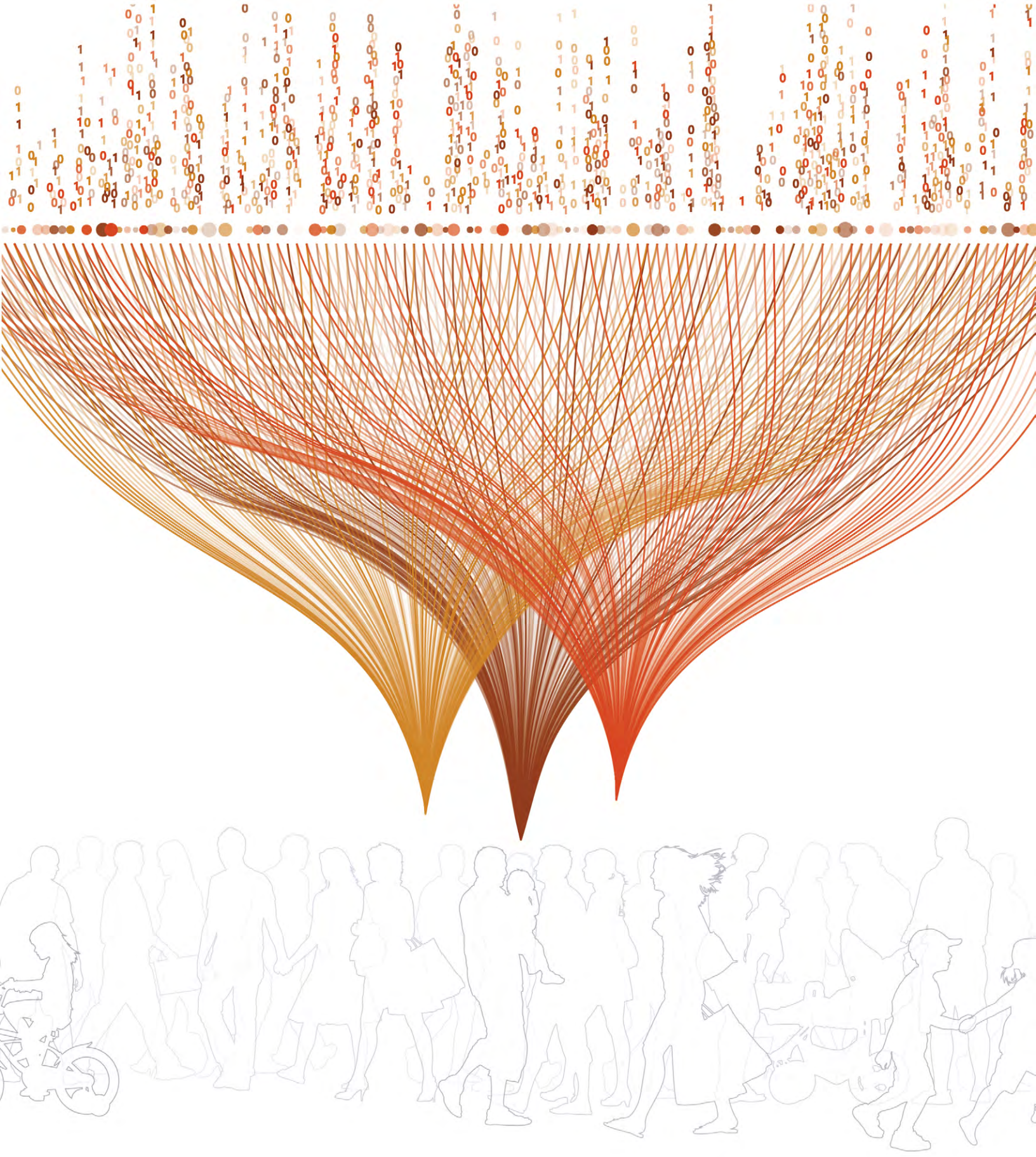
252 S Casey Hill, David M Tanovich & Louis P Strezos, *McWilliams' Canadian Criminal Evidence*, 5th ed (Toronto: Thomson Reuters, 2013) at 35:29.

253 S Casey Hill, David M Tanovich & Louis P Strezos, *McWilliams' Canadian Criminal Evidence*, 5th ed (Toronto: Thomson Reuters, 2013) at 35:29.

254 S Casey Hill, David M Tanovich & Louis P Strezos, *McWilliams' Canadian Criminal Evidence*, 5th ed (Toronto: Thomson Reuters, 2013) at 35:29.

255 S Casey Hill, David M Tanovich & Louis P Strezos, *McWilliams' Canadian Criminal Evidence*, 5th ed (Toronto: Thomson Reuters, 2013) at 35:29.

256 See comments by Rediet Abebe during "Forensic Algorithm: The Future of Technology in the US Legal System, Washington, D.C." (webinar) (12 May 2022), online: https://www.brookings.edu/wp-content/uploads/2021/10/051222-Forensic-Algorithms-Transcript.pdf.



LAW COMMISSION OF ONTARIO
COMMISSION DU DROIT DE L'ONTARIO

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