LAW COMMISSION OF ONTARIO
COMMISSION DU DROIT DE L'ONTARIO

FROM	Susie Lindsay, Law Commission of Ontario
TO	Civil Rules Committee - Sub-Committee on AI
DATE	December 1, 2025
SUBJECT	**Law Commission of Ontario** **AI and Bias – Additional Submissions**

Thank you for the opportunity to comment on the Subcommittee's proposals for *Rules of Civil Procedure* relating to evidence and AI, and for including the Law Commission of Ontario (LCO) in the Townhall on October 27th, 2025.

In preparation for consultation on AI and Bias on December 2nd, 2025, and in furtherance of the documents circulated by the Sub-Committee today, the LCO prepared additional written comments. These comments are intended as a supplement to the LCO's initial submission dated September 12, 2025.

The LCO wishes to provide background information on the issue of AI and bias out of concern that there was no mention of bias in the original consultation paper and few comments on bias during the Townhall. In addition to our comments, the LCO recommends the Sub-Committee seek the advice of other individuals or organizations, such as the Ontario Human Rights Commission or human rights litigators, who did not participate in the consultation and who may have significant concerns.

1. Introduction

The LCO's understanding of the Sub-Committee position on bias in AI is paraphrased from Justice Lauwers during the Townhall:

> *The CRC recognizes that bias in AI is a concern. However, the complexity of bias makes it unsuitable to entrench in a rule at this time. The complexity is twofold:*
>
> *(1) All AI includes bias – bias is a necessary part of AI. Bias in AI includes issues with human rights and issues with sample bias.*
> *(2) There is no agreement on a method to measure bias in AI.*

> *As a result of these complexities, the subcommittee suggests leaving the issue of bias out of the Rule amendments until there is further research on this topic and there exists a better understanding of how to measure bias in AI.*

In the minutes, this issue was addressed as "To the extent that bias is a concern, it can be very difficult to detect".

The LCO agrees that bias can be difficult to detect but does not agree that the complexity of bias means it should be ignored in the proposed Rules. Bias is a crucial issue in AI. The LCO submits that to create new *Rules of Civil Procedure* that specifically address AI but leave out a requirement to address bias creates a gap in the law that will undermine the effectiveness of the *Rules*, possibly exacerbate human rights violations, and worsen access to justice issues and unfairness in Ontario's legal system.

2. Summary

The LCO recommends that the Sub-Committee amend Rule 1, Disclosure and Rule 3, Admissibility of Expert Evidence as follows:

Rule 1 Disclosure:

> (c) Provide supporting evidence to show that the output or results of the software or program are valid and reliable, **and to provide an audit for bias if a party to the action or the court suggest is necessary.**

Rule 3 Expert Evidence:

- **Amend section (d) to "the evidence is based on valid, reliable and representative facts or data".**
- **Amend section (e) to "the evidence is the product of valid and reliable principles and methods that include auditing the AI system for fairness including biases or assumptions embedded in the design or data, if a party to the action or the court require it. The process and results of the AI bias audit should be producible in court upon request from a party to the action or the court.**

The LCO's rationale for our proposed amendments has several parts:

- AI systems have proven risks to human rights.
- Canadian AI systems must comply with human rights law.
- AI human rights and bias testing is well-established in law, policy and practice.
- Testing for bias is common.
- AI evidence is "high risk" and "high impact" and should meet high standards.
- Testing for human rights and bias in AI should not be excluded from the proposed rules
- What will happen if a bias Rule is not included?

3. AI Systems Have Proven Risks to Human Rights

Human rights have been a transcendent issue in AI design, development, operation, and oversight across the world for many years.[1] AI systems can be biased or discriminatory against individuals on the grounds of race, age, disability, sex, family structure or other grounds protected in the *Charter* and provincial human rights codes. Bias in an AI system can also intersect across multiple grounds at once. Equally troubling, bias is often embedded, unexpected, undetected, and coupled with the perception that machines are objective.

The most common human rights criticism of AI is the potential use of biased data. In these circumstances, because the training data or "inputs" used by AI or an algorithm (such as arrest, conviction, child welfare, education, employment or "fraud" data) may themselves be the result of biased practices, the results or outputs of an AI or algorithmic system may also be biased. Similarly, AI discrimination can occur if the system relies on factors that correlate with bias (such as location data that correlates with race or employment data that correlates with gender),[2] or if the system is designed with developer's personal biases and assumptions embedded within.

The "bias in, bias out" issue is the best-known AI bias issue, but not the only one. Discrimination and bias issues can also arise in questions regarding statistical "metrics of fairness", AI or algorithmic scoring, and automation bias, to name a few. The effect of technology on bias can be subtle but significant. For example, AI may increase barriers for people with disabilities if systems are built without considering accessibility, or if they misinterpret a disability as cheating, an anomaly, or a red flag.

4. Canadian AI Systems Must Comply with Human Rights Law

Canadian governments, agencies, and private sector organizations have a legal responsibility to comply with Canadian human rights law, including, where applicable, the *Canadian Charter of Rights and Freedoms,* the *Canadian Human Rights Act*, and provincial human rights legislation.[3] This responsibility applies to both public and private AI systems that may be developed or deployed in Canada.

Every party with human rights obligations has a duty not only to respond to complaints about discrimination and barriers, but to take reasonable steps to remove them when it is told or has reason to believe they exist.

The centrality of human rights in AI governance has been recognized repeatedly by Canadian governments. For example, the Province of Ontario's *Responsible Use of Artificial Intelligence Directive* states:

> *AI may also exacerbate existing biases and stereotypes, potentially determining access to benefits or services in a discriminatory manner and infringing on human rights. These issues are compounded when individuals over rely on data or decisions produced by AI without sufficient human oversight, also known as technological deference or automation bias, which is the tendency to favour results generated by automated systems, even in the presence of contrary information from non-automated sources.*[4]

The Directive goes onto to state that a key principle is that AI use is "human rights affirming and non-discriminatory:"

> *AI is used in ways that respect and protect equity, human rights and fundamental freedoms and ensure fairness consistent with applicable legislation including the Canadian Charter of Rights and Freedoms and the Ontario Human Rights Code. Community-informed context, including an understanding of potential discriminatory outcomes and their mitigations, as well as inclusive design, are the foundations of determining if and how AI is used.*[5]

Similarly, the Government of Canada's recent 30 Day National Sprint on Canada's National AI Strategy committed the federal government to AI systems that "protect human rights, serves the public good and inspires trust."[6]

5. AI Human Rights and Bias Testing Is Well-Established In Law, Policy And Practice

Human rights and bias testing are features of contemporary AI governance strategies that have been adopted by governments, many private sectors organizations, and international institutions. For example,

- The OECD states that ensuring AI systems are trained on representative data is crucial for delivering accurate and relevant outcomes.[7] OECD further discusses the importance of Algorithmic Impact Assessments and AI audits as governance mechanisms.[8]

- Microsoft lists fairness as one of six key principles that should guide AI development and use. "AI systems should treat all people fairly." They go to say that the only way to do this is to measure AI. "Measurement is the key to keeping AI on tract" [9]

- Google's AI Ethics policy states: "Implementing appropriate human oversight, due diligence, and feedback mechanisms to align with user goals, social responsibility, and widely accepted principles of international law and human rights." and "Employing rigorous design, testing, monitoring, and safeguards to mitigate unintended or harmful outcomes and avoid unfair bias."

- The Vector Institute, Canada's premier AI research institute, states that:

  > *We are committed to building appropriate safeguards into AI systems to ensure they uphold human rights, the rule of law, equity, diversity, and inclusion, and contribute to a fair and just society. AI systems should comply with laws and regulations…*[10]

  As a result, Vector's Playbook for Responsible AI Product Development includes a series of questions on the representativeness of the data and testing AI for fairness and biases.[11]

- Meta's "Responsible Use Guide: Resources and best practices for responsible development of products built with large language models" states "focusing on the representativeness of the data can help prevent a fine-tuned model from perpetuating biases in its generated outputs…"[12]

- The United Nations Educational, Scientific and Cultural Organization's (UNESCO) Recommendations on the Ethics of AI state, in part, [13]

> *Human rights and fundamental freedoms must be respected, protected and promoted throughout the life cycle of AI systems. Governments, private sector, civil society, international organizations, technical communities and academia must respect human rights instruments and frameworks in their interventions in the processes surrounding the life cycle of AI systems. New technologies need to provide new means to advocate, defend and exercise human rights and not to infringe them.*[14]

The LCO can provide more examples upon request.

6. Testing AI For Bias Is Common

It appears the Sub-Committee is suggesting that testing for bias should be left out of the Rules pending further research on this topic until there exists a better understanding of how to measure bias in AI.

With respect, the LCO suggests this statement is out of step with contemporary AI governance frameworks. AI human rights and bias testing is neither new nor unusual. Rather, it is a common feature in AI governance models, especially in Canada.

In Canada, the Federal Government requires federal departments to assess for bias[15], the Province of Ontario advises government departments and agencies to conduct AI bias assessments,[16] and by international agreement, Canadians have an obligation to implement measures to ensure that AI systems are consistent with our domestic human rights framework. Relevant Canadian examples include:

Government of Canada

The Government of Canada currently requires every Federal department, that is subject to the Treasury Board Secretariat, to evaluate all AI system for bias and discrimination if the AI system is used to make an administrative decision or related assessment about a client.[17] Among the many questions to address bias, deployers of AI must answer whether they have

> *…assessed system performance for clients with a range of personal and intersectional identity factors (for example, gender, age, race, language, ethnicity, disability) to verify that decisions and outcomes are fair for a diverse group of people, and have the identified disparities been addressed?* [18]

The federal government has also attempted to regulate AI systems in the private sector as well. The *Artificial Intelligence and Data Act* (AIDA)[19] would have applied to private sector organizations responsible for the "development, deployment, use or making available of AI systems" and not government institutions.[20] *AIDA* would have required persons responsible for AI systems to assess whether their systems were high-impact and to "establish measures to identify, assess and mitigate the risks of harm or biased output" in accordance with *AIDA* regulations.[21]

As the Sub-Committee knows, AIDA was criticized on many grounds and did not pass. Even so, the federal government has not withdrawn from either AI governance or the need to protect human rights in those systems: The Government of Canada's recent 30 Day National Sprint on Canada's

National AI Strategy committed the federal government to AI systems that "protect human rights, serves the public good and inspires trust."[22]

Province of Ontario

The Province of Ontario's *Public Service AI Playbook*, which is a feature of the Province's *Responsible Use of Artificial Intelligence Directive,* advises parties to perform a review to identify potential for bias and legal exposure under the *Ontario Human Rights Code*. The *Playbook* describes different measures that can be used to assess for bias depending on the use case and whether the AI system is a "commercial product using pre-trained models", "limited or not access to model and training data" or "direct access to model with training data".[23]

Framework Convention on AI and Human Rights, Democracy and the Rule of Law

Canada is a signatory to the recent (2024) *Framework Convention on AI and Human Rights, Democracy and the Rule of Law.*[24] The *Framework Convention* applies to private and public entities and covers "activities within the lifecycle of artificial intelligence systems that have the potential to interfere with human rights, democracy and the rule of law.[25] The Framework Convention requires signatory states to:

> *[A]dopt or maintain measures to ensure that the activities within the lifecycle of artificial intelligence systems are consistent with obligations to protect human rights…*[26]
>
> *[A]dopt or maintain measures with a view to ensuring that activities within the lifecycle of artificial intelligence systems respect equality, including gender equality, and the prohibition of discrimination, as provided under applicable international and domestic law…"*[27]
>
> *[A]dopt or maintain measures aimed at overcoming inequalities to achieve fair, just and equitable outcomes, in line with its applicable domestic and international human rights obligations, in relation to activities within the lifecycle of artificial intelligence systems…*[28]

Finally, the Framework Convention requires states to adopt or maintain measures to identify, assess, prevent and mitigate risks of artificial intelligence by "considering actual and potential impacts to human rights, democracy and the rule of law" and to ensure adverse impacts of AI systems to human rights are addressed.[29]

AI in the Criminal Justice System

In the criminal justice system, issues of data bias and discrimination in criminal justice AI systems are acute and have been discussed extensively in many reports.[30] For example,

> *Studies on [facial recognition technology] have clearly demonstrated that racial and gender biases, meaning women and people of colour, are more likely to be misidentified by FRT and, therefore, potentially more likely to be wrongfully accused by police who use FRT than light-skinned men.*[31]

Many predictive policing systems have also been shown to be biased and discriminatory.[32]

Concerns about bias are the foundation for many proposals to strictly regulate police and court-based AI systems.[33]

As a result, there is a growing number of Canadian policing organizations that require human rights or bias testing. Examples include:

- The Toronto Police Services "Use of AI Technology" Policy does not allow the adoption of any AI application that is likely to cause harm "due to bias or other flaws".[34]

- The Durham Region Police Services AI Policy states police use of AI "must foster fairness in the application of AI technologies by: Ensuring equality and non-discrimination in AI operation; Protecting vulnerable groups from potential biases or adverse impacts"[35]

- The RCMP's National Technologies Onboarding Program (NTOP) policy requires that any RCMP unit considering the use of a technology-based tool, technique, device software, application or dataset used to support investigations or intelligence gathering must consult the NTOP before testing, purchasing, developing or deploying any operational technology that is primarily intended to collect or use personal for investigation and/or intelligence gathering. Artificial intelligence and privacy intrusive technologies are NTOP's highest priorities.[36]

Notably, many other jurisdictions have also implemented requirements for bias audits into AI governance frameworks.

European Union

The European Union's (EU) *AI Act* requires any AI system considered "high risk"[37] to fulfill obligations including:

- Conduct data governance, ensuring that training, validation and testing datasets are relevant, sufficiently representative. Parties must take appropriate measures to detect, prevent, and mitigate possible biases.[38]
- Perform an assessment of the impact on fundamental rights that the use of such system may produce.[39]
- Establish a risk management system throughout the high-risk AI system's lifecycle.[40]
- Create and maintain documentation and record keeping to ensure compliance.[41]

United States

There are many examples of American legislation and policy that requires human rights testing on AI systems. For example:

- In Colorado, developers and deployers of "high-risk" AI systems have a duty to avoid algorithmic discrimination.[42] Among numerous obligations, developers of AI systems must evaluate an AI system for algorithmic discrimination[43] before making it available to a deployer. Deployers of "high-risk" AI systems must conduct impacts assessments that include an analysis of the risk of algorithmic discrimination.[44] According to the AI Watch, Global Regulatory Tracker, the Colorado AI Act is emerging as a key template for state AI regulation. For example, state legislatures in Connecticut, Massachusetts, New Mexico, New York, and Virginia are considering bills that would generally track the Colorado AI Act and impose safeguards against bias by AI systems.[45]

- New York City requires employers that use automated employment decision tools to audit those tools for potential race and gender bias, publish the audit results and notify employees and candidates about the use of those tools.[46]

- In October 2025, the California Civil Rights Department's regulations applying to employers who use automated decision-making systems, went into effect. The regulations clarify that automated decision-making systems that produce discriminatory results will be in violation of the *Civil Rights Code*, unless they have an available defence. Conducting bias testing prior to deployment is a valid defence.[47]

7. Admission of AI Evidence is High Risk and Should Meet High Regulatory Standards

It is well established that expert evidence can have a significant impact on individual's rights, freedoms and interests and as such is an important factor in access to a fair and just legal system.
One of the key frameworks in AI governance is the "risk regulation" model. In this model, AI systems that present high risks to individual rights and interests attract the greatest regulatory scrutiny. By all accounts, the admission of expert evidence into a court of law is high risk or high impact. This is shown clearly in many contemporary AI governance models.

The Federal Government's draft legislation to regulate AI, the *Artificial Intelligence and Data Act*, explicitly included "The use of an artificial intelligence system by a court or administrative body in making a determination in respect of an individual who is a party to proceedings before the court or administrative body" as high impact.[48]

Similarly, the EU *AI Act* categorizes AI systems "intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts, or to be used in a similar way in alternative dispute resolution;" as high risk.[49]

The Sub-Committees proposed Rules are consistent with this approach: AI evidence in civil proceedings is potentially "high impact" and thus should be subject to greater regulatory scrutiny.

8. Testing for Human Rights and Bias in AI Should Not be Excluded from the Proposed Rules

The LCO agrees that auditing AI for bias is challenging. The LCO also agrees that harmful bias is not going to be an issue in every case. However, these are not compelling reasons to ignore the issue of AI bias.

The lack of a standard test for AI bias, does not render AI bias audits less crucial.

It is true there are different ways to assess an AI system for bias. However, there is no single, universal scientific consensus on a method to test the validity or reliability of AI systems either. The lack of

scientific consensus on validity and reliability has not dissuaded the drafters of the proposed Rules to exclude this as a requirement. The same can be said for testing for bias in AI.

Differing methods of testing for bias should not lead the CRC to abandon their obligation to create rules that protect human rights. It is incongruent to require parties to test for validity and reliability and not test for bias. Testing for validity and reliability does not cover testing for bias. Establishing validity and reliability as issues to be assessed in the *Rules*, while ignoring bias is drawing an arbitrary line. Further, to introduce the issue of bias into *Rule* 2 (deep fake evidence) and not add it to *Rules* 1 and 3 is inconsistent and appears unusual. There is no clarity as to why it is an issue in Rule 2 and not Rules 1 and 3.

Testing of AI systems for validity, reliability and bias will evolve overtime. Courts will be the judge of what methods of testing for validity, reliability and bias are acceptable. Our court system is designed for the trier of fact to make the call as to what expert evidence to admit and what expert evidence to follow. There is also not a standard to quantify discrimination in law.[50] This has not prevented the Federal and provincial governments from passing laws that protect human rights or prevented courts from assessing and determining discrimination.

Bias has long been recognized as a crucial issue with expert evidence. There are safeguards built into the procedure of retaining an expert and presenting expert evidence in court to minimize the potential for harmful biases. Experts must swear that they are impartial (Form 53), the instructions from the party retaining the expert must be disclosed (53.03(3)), the expert must provide a description of the factual assumptions and list of every document relied on in forming the opinion (53.03(6) and the expert can be cross-examined. AI systems cannot be cross-examined, but an AI audit could disclose information about the AI system that would allow the trier of fact to assess whether the AI system contains harmful biases relevant to the issue at hand.

The more challenging aspect of bias in AI is how to correct or minimize harmful bias. In this circumstance, we are not suggesting that the court require parties to solve bias issues in AI. The LCO's submission is purely for disclosure and transparency so that the trier of fact can weigh the evidence appropriately. Disclosure of harmful biases creates the potential to prevent human rights harms.

Harmful bias is not an issue in every case

The LCO agrees with the Civil Rules Committee that harmful biases are not an issue in every case. However, the *Rules* can be drafted to account for this. As a result, the LCO recommends the proposed Rules be amended as follows:

Rule 1 Disclosure

> (c) Provide supporting evidence to show that the output or results of the software or program are valid and reliable, **and to provide an audit for bias if a party to the action or the court suggest is necessary.**

Rule 3 Expert Evidence:

- Amend section d to “the evidence is based on valid, reliable and representative facts or data”.
- Amend section e to “the evidence is the product of valid and reliable principles and methods that include auditing the AI system for fairness including biases or assumptions embedded in the design or data, **if a party to the action or the court require it.** The process and results of the AI bias audit should be producible in court **upon request from a party to the action or the court.**

9. What Will Happen Without A Bias Rule?

The LCO believes that adopting new *Rules* legitimizing AI evidence in Ontario courts but deferring the bias issue pending “further research” will likely worsen bias and discrimination in Ontario’s court system.

To avoid introducing such a rule out of concern for “the practicalities” of testing for bias, is forfeiting the court’s responsibility to protect human rights and other types of unfairness to technology companies. Rules and regulations can be hard, and can require change, but this rule is necessary. Further, testing for bias is not always a challenge. If a party makes a submission that in a certain context testing for bias is impossible, that is an issue courts can address on a case-by-case basis.

In Ontario, parties, governments, organizations and individuals have an obligation to make reasonable efforts to comply with Canadian human rights laws. Knowing that all AI systems are biased, knowing the preponderance of harmful discriminatory AI systems, and still permitting parties to submit AI evidence that has not been tested for biases is to risk perpetuating and worsening discrimination and human rights violations into Ontario’s court system. Private and public entities have an obligation to take steps when they know or have reason to know that their policy may create a discriminatory obstacle for the people they provide service to; why would the court not be concerned about this issue?

Further, if a requirement to test for bias is not created in the proposed *Rules*, it is not clear what opportunities or remedies parties will have to challenge AI evidence for harmful bias. Absent a clear obligation in the *Rules*, litigants will need to bring motions to challenge an AI system for bias. Absent a clear requirement, it is not clear they will have a legal ground to do so, nor are they likely to have information about an opposing party’s AI system. Finally, failing to address these risks will put greater harms and onus on poor and unrepresented populations in Ontario. Needless to say, this legal burden will fall disproportionately on self-represented or under-represented individuals or organizations, including racialized communities, Indigenous communities, and low-income communities.

There is a further, perhaps underappreciated, relationship between our recommendations and AI litigation: Effective and consistent Rules reduces litigation risk. This is because appropriate Rules will increase the likelihood that parties design, deploy and monitor their AI systems with an eye to legal principles and requirements.

10. More Information

The LCO appreciates the opportunity to comment on the proposed *Rules*. The LCO is willing to discuss any of these issues at any time and is willing to share any resources or information with the Subcommittee on AI.

For further information or to contact the LCO, please contact Susie Lindsay, Policy Counsel, Project Lead AI in the Civil Justice System (slindsay@lco-cdo.org).

---

[1] The LCO's analysis of AI in the civil/administrative justice systems is set out in the following LCO Reports: *LCO/OHRC AI Human Rights Impact Assessment* (2024) and *LCO/OHRC AI Human Rights Impact Assessment: Backgrounder* (2025); *Accountable AI* (2022), *Regulating AI: Critical Issues and Choices* (2021), and the LCO's *Bill 194 Submission* (2024). These reports are available online at https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/. A summary of LCO's analysis in AI in the Canadian criminal justice system is included in LCO, *Introduction to the LCO Criminal AI Project: Evaluating Trustworthy AI In Canada* [LCO Criminal AI Introduction] (2025), online at https://www.lco-cdo.org/en/our-current-projects/crimai/.

[2] Even if we remove the discriminatory factor such as race or sex, the correlated factors can unintentionally produce bias. For example, an algorithm used to assess suitability for a loan application could unintentionally be bias against women if it is trained to weigh factors such as specific previous employment (since there are some jobs more likely occupied by women) and gaps in employment (since women are more likely to take parental leave), or part-time employment (since women are more likely to work part-time). See Jacquelyn Burkell, *The Challenges of Algorithmic Bias* (2019), Autonomy Through Cyberjustice Technologies Working Paper, Law Society of Ontario at 5, online at www.ajcact.org/en/publications/the-challengesof-algorithmic-bias/. The LCO can provide other sources as well.

[4] The *Responsible Use of Artificial Intelligence Directive* (the "Directive") sets out the requirements for the transparent, responsible and accountable use of AI. The *Directive* applies to all Ontario Ministries and provincial agencies. It requires the application of AI risk management by ministries and provincial agencies that are seeking to use AI systems, or use services that include AI functionality (including procured, ministry/provincial agency developed and publicly available tools), as part of the development or delivery of, or decision-making for, a Government of Ontario policy, program, or service (referred to as a "use case"). Government of Ontario, *Responsible Use of AI Directive* [Ontario Responsible Use of AI Directive] (2024), online at https://www.ontario.ca/page/responsible-use-artificial-intelligence-directive, section 1.

[5] Ontario Responsible Use of AI Directive, section 5.4.

[6] "Vision Statement", National AI Strategy, online at https://ised-isde.canada.ca/site/ised/en/public-consultations/help-define-next-chapter-canadas-ai-leadership.

[7] Organization of Economic Cooperation and Development, *Governing with Artificial Intelligence* [OECD](2025), online at https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/06/governing-with-artificial-intelligence_398fa287/795de142-en.pdf at 115.

[8] OECD at 137-141.

[9] Microsoft, *Measurement is the key to helping keep AI on track*, by Susanna Rey, September 9, 2024. Online at https://news.microsoft.com/source/features/ai/measurement-is-the-key-to-helping-keep-ai-on-track/.

[10] Vector Institute, *The Vector Institute's AI Trust and Safety Principles* (2023), online at https://vectorinstitute.ai/ai-trust-and-safety-principles/, section 2.

[11] Vector Institute, *Principles in Action: A Playbook for Responsible AI Product Development*, "Development: Where should you get your data from and how do you evaluate it?" (2024), online at https://principlesinaction.vectorinstitute.ai/.

[12] Meta, *Responsible Use Guide: Resources and best practices for responsible development of products built with large language models*, (April 2024) at 11.
[13] UNESCO, *Ethical impact assessment: a tool of the Recommendation on the Ethics of Artificial Intelligence* [UNESCO] (2023), online at https://unesdoc.unesco.org/ark:/48223/pf0000386276 at 21.
[14] UNESCO at 18.
[15] Canada, *Directive on Automated Decision-Making* [Canada ADM Directive] (2019), online: https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592; and Algorithmic Impact Assessment Tool [Canada AIA], online: https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html.
[16] See generally, *Ontario Responsible Use of Artificial Intelligence Directive* and the accompanying Ontario Public Service AI Playbook [Ontario AI Playbook] (2024), Appendix 13. The Ontario AI Playbook is not available publicly. The LCO has a copy on file.
[17] The Canada ADM Directive requires every automated decision-making system that is used to make or support administrative decisions to complete the Canada AIA. The Canada AIA consists of questions, the answers to which must be posted to a public portal.
[18] Canada AIA at 9. Pages 6, 7, 8 and 9 of the Canada AIA include several questions to address bias. For example, the deployer of the AI system must answer the following questions:

- Does the algorithm consider protected characteristics to make its decisions or recommendations?
- Have you evaluated whether variables that the system bases its decisions or recommendations on could be proxies for protected characteristics?
- Have you assessed system performance for clients with a range of personal and intersectional identity factors (for example, gender, age, race, language, ethnicity, disability) to verify that decisions and outcomes are fair for a diverse group of people, and have the identified disparities been addressed?
- Are there clients or groups of clients that will experience the most significant negative impacts from the system being used?
- Is the training and testing data for the system representative of the clients being served?
- Are there biases in the training data that could increase the likelihood of discriminatory outcomes or lead to other impacts on human rights?

[19] *Digital Charter Implementation Act*; *1st Sess. 44th Parliament, 2022, Part 3 "Artificial Intelligence and Data Act"*, [*AIDA*], online: *https://www.parl.ca/legisinfo/en/bill/44-1/c-27*.
[20] *AIDA*, s. 3.
[21] *AIDA*, sections 7 and 8.
[22] "Vision Statement", National AI Strategy, online at https://ised-isde.canada.ca/site/ised/en/public-consultations/help-define-next-chapter-canadas-ai-leadership.
[23] Ontario AI Playbook, Appendix 13.
[24] The Council of Europe *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law* [Council of Europe AI Convention] (September 5, 2024), online at https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence.
[25] Council of Europe AI Convention, Article 3 (1) and 3(1)(a).
[26] Council of Europe AI Convention, Article 4.
[27] Council of Europe AI Convention, Article 10(1).
[28] Council of Europe AI Convention, Article 10 (2).
[29] Council of Europe AI Convention, Article 16 (1), (2) (a)-(g), 3 and 4.
[30] For an extensive discussion of bias in criminal AI systems, see the Introduction and four background papers in the LCO's AI in the Criminal Justice System project (2025). Available online at https://www.lco-cdo.org/en/our-current-projects/crimai/.
the LCO's and issues, see LCO American Lessons at 20-26.
[31] International Network of Civil Liberties Organizations, *Eyes on the Watchers: Challenging the Rise of Police Facial Recognition Technology* [INCLO Challenging FRT] (2025), online: https://inclo.net/pillars/surveillance-and-digital-rights/principles-for-use-of-frt/ at 25. The best-known FRT bias study is a 2019 report by the National Institute of Standards and Technology study which found that "[t]he majority of commercial facial-recognition systems exhibit bias" and "falsely identified African-American and Asian faces 10 to 100 times more than Caucasian faces."

National Institute of Standards and Technology (NIST), *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects* [NIST FRT](2019), online: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf at 3. NIST also identified concerns regarding false negatives false positives, gender, and age.

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

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

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

[35] Durham Regional Police Services "Use of Artificial Intelligence" policy https://durhampoliceboard.ca/wp-content/uploads/2025/03/3b2-Policy-Use-of-AI.cleaned.pdf.

[36] RCMP Communication with the Law Commission of Ontario, on file with the LCO.

[37] As discussed above, the *EU AI Act* Annex III classifies AI systems that are used for "administration of justice" as high-risk AI system:
(a) AI systems intended to be used by a judicial authority or on their behalf to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts, or to be used in a similar way in alternative dispute resolution;

[38] *EU AI Act*, Article 10 (e) and (d) and Article 26 s.4.

[39] *EU AI Act*, Article 27.

[40] *EU AI Act*, Article 9.

[41] *EU AI Act*, Articles 11 and 12.

[42] *An Act Concerning Consumer Protections for Interactions with Artificial Intelligence* [Colorado AI Act], Colorado Senate Bill 24-205 (SB24-205), signed into law May 2024 and takes effect February 1, 2026.

[43] Colorado AI Act at 6-1-1702.

[44] Colorado AI Act at 6-1-1703.

[45] White & Case, *AI Watch, Global Regulatory Tracker*, online at https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-united-states.

[46] New York City's Local Law 144, S 5-301, Bias Audit https://rules.cityofnewyork.us/wp-content/uploads/2023/04/DCWP-NOA-for-Use-of-Automated-Employment-Decisionmaking-Tools-2.pdf

[47] See CALIFORNIA CODE OF REGULATIONS Title 2. Administration Div. 4.1. Department of Fair Employment & Housing Chapter 5. Fair Employment & Housing Council Subchapter 2. Discrimination in Employment, 11009(f) https://calcivilrights.ca.gov/wp-content/uploads/sites/32/2025/06/Notice-of-Approval-regulations-automated-employment-decision-systems.pdf.

[48] See Amendments to Bill C-27, November 28, 2023, Class 6 https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12751351/12751351/MinisterOfInnovationScienceAndIndustry-2023-11-28-Combined-e.pdf

[49] EU *AI Act*, Annex 3, High-Risk AI Systems referenced in section 6(2) https://artificialintelligenceact.eu/annex/3/

[50] See, *R v. Fraser* 2011 SCC 20, at para 59. There is no "universal measure" for what level of statistical disparity is necessary to demonstrate disproportionate impact. The statistics must show a pattern that is significant and not just "the result of chance".