National Sprint on Canada's AI Strategy

Law Commission of Ontario Submission

October 2025

LAW COMMISSION OF ONTARIO
COMMISSION DU DROIT DE L'ONTARIO

1. Introduction

This is the Law Commission of Ontario's (LCO) submission to the Government of Canada's 30 Day National Sprint on Canada's National AI Strategy.

2. About the LCO

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 issues. The LCO is independent of stakeholder interests and is committed to a "public interest" perspective for every project.

The LCO has unparalleled experience analyzing trustworthy AI governance, including AI and the *Charter*, human rights, procedural fairness, and access to justice. Recent LCO reports addressing these issues include:

- *AI in Criminal Justice Project* (2025)
- *Human Rights AI Impact Assessment* (with the Ontario Human Rights Commission, 2024)
- *Submission to Government of Ontario Re Bill 194* (2024)
- *Accountable AI* (2022)
- *Regulating AI: Critical Issues and Choices* (2021)
- *Legal Issues and Government AI Development* (2021)

This work is part of the LCO's ongoing AI and the Justice System project.

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

3. LCO Contact

Questions or comments about this submission, the LCO, or the LCO's AI projects can be directed to Nye Thomas, LCO Executive Director, at athomas@lco-cdo.org or 416-402-7267.

4. Summary of LCO Submission

The LCO's submission considers how the National AI Strategy can fulfill its commitment to AI systems that "protect human rights, serves the public good and inspires trust."[1] More specifically, the LCO's submission addresses two important consultation questions:

> ***How can Canada build public trust in AI technologies while addressing the risks they present? What are the most important things to do to build confidence?***
>
> ***What frameworks, standards, regulations and norms are needed to ensure AI products in Canada are trustworthy and responsibly deployed?***

The LCO's recommendations focus on AI systems used in the federal public service and by federal agencies. This is because the majority of the LCO's has focused on AI in the public sector. However, "building trust in AI" will require a similar approach to private sector AI systems. The LCO's recommendation for a trustworthy AI legislation governing federal public sector AI systems should be a model and foundation for an equivalent framework to apply to private sector AI systems.

It is widely acknowledged that public sector AI systems can affect the most significant rights and interests in Canadian's lives, including their personal liberty; *Charter* rights; human rights; privacy rights; child welfare; and access to employment, health care, education, housing, economic opportunities, and income security.[2] It is also widely acknowledged that public sector AI risks fall disproportionately on low-income, Indigenous, racialized or otherwise vulnerable communities and individuals.[3]

Over the last several years, the LCO has developed comprehensive frameworks to ensure AI systems are beneficial, legal and trustworthy.[4] Our submission distills this analysis into four key recommendations that should be incorporated into Canada's renewed National AI Strategy:

Recommendation #1

Canada's National AI Strategy should commit to establishing comprehensive trustworthy AI legislation governing federal public sector AI systems. This legislation should include:

- Mandatory disclosure of AI systems, including public "AI registers".
- An explicit commitment that AI systems must protect human rights, privacy, and procedural fairness.
- An explicit commitment to risk-based regulation, including mitigation requirements and explicit criteria to identify authorized, high-risk, and prohibited AI systems.
- Mandatory AI impact assessments.
- A duty to measure, correct and audit bias in AI systems.
- Auditing and evaluation requirements.
- Remedial requirements.
- Independent oversight of both specific AI systems and AI systems generally.

Recommendation #2

Canada's National AI Strategy should commit the Government of Canada to address AI systems used in the Canadian criminal justice system, including systems used by law enforcement agencies and in criminal courts.

Recommendation #3

Canada's National AI Strategy should commit the Government of Canada to developing comprehensive "human rights by design" and "fairness by design" strategies to protect human rights and procedural fairness in Canadian AI systems.

Recommendation #4

Canada's National AI Strategy should commit the Government of Canada to public consultations identifying criteria, contexts or uses of AI systems that may be prohibited, pre-emptively identified as high-risk, or otherwise subject to higher regulatory standards.

The LCO believes these recommendations are the foundation necessary to "protect human rights, serve the public good and inspire public trust" in Canadian public sector AI systems. The LCO submits the benefits and outcomes of these recommendations would include:

- Establishing a comprehensive, consistent baseline for Canadian public sector AI systems to ensure they protect human rights, serve the public good and inspire public trust.
- Mitigating the most serious AI risks and protecting the legal rights of the most vulnerable Canadians, including racialized communities, Indigenous communities, low-income Canadians and others.
- Providing clear regulatory guidance to Canadian governments, AI innovators, investors and others to promote responsible development and adoption of AI in public sector AI systems.
- Establishing a principled but flexible national public sector AI governance standard that could be adopted or adapted by other governments, public agencies, and the private sector.
- Establishing a Canadian AI governance framework that is consistent with emerging international standards.

The balance of this submission discusses our recommendations in detail.

5. Trustworthy AI

The LCO commends the Government of Canada for developing a renewed National AI Strategy. The LCO also fully supports the stated goals to:

- Accelerate safe adoption of AI across the economy and public services.
- Scale Canadian AI champions and attract investment.
- Strengthen sovereign infrastructure (compute, data, cloud).
- Build public trust, skills, and safety.

The LCO believes the fourth goal – "build public trust, skills, and safety" – is a precondition to achieving the first three.

The relationship between "trustworthy AI" and economic development is widely acknowledged. For example, a recent global study by KPMG stated that:

> *The public's trust in AI technologies and its responsible and ethical use is central to sustained acceptance and adoption and in realizing the full societal and economic benefits of these technologies.*[5]

The KPMG study also found that "trust remains a critical challenge" and concluded that to drive "sustainable innovation and growth" needed leadership, AI literacy, trust and governance.[6]

Finally, the KPMG report confirmed the need for swift and effective action in Canada, finding that Canada has one of the lowest levels of trust of AI systems (34%) and acceptance (19%).[7]

The LCO has written extensively about how to achieve trustworthy and accountable AI through governance mechanisms, including:

- Transparency, disclosure and explainability requirements.
- Compliance with human rights, privacy and procedural fairness.
- Risk categories and mitigation strategies.
- Impact assessments.
- Bias and data requirements.
- Audit and evaluation requirements.
- Remedial requirements
- Independent oversight and public engagement.[8]

The LCO's analysis and recommendations have been confirmed in many other studies.[9]

The LCO's submission focuses on four fundamental building blocks and priorities for mitigating risk and building trust in Canadian AI systems:

- Federal trustworthy AI legislation (Recommendation #1).
- AI in the criminal justice system (Recommendation #2).
- Human rights and procedural fairness (Recommendation #3).
- AI "red-lines" and pre-emptive regulation (Recommendation #4).

Together, our recommendations represent a comprehensive, integrated strategy to "protect human rights, serve the public good, and inspire public trust" in federal public sector AI systems.

While our recommendations focus on federal public sector AI systems, the LCO believes that many of the duties and principles included in our recommendations should apply to Canadian private sector AI systems as well. For example, our recommendations addressing human rights, risk management, impact assessments and AI "red lines" are equally applicable to private sector AI systems. Our submission discusses Canadian private sector AI systems where it is appropriate to do so.

Recommendation #1 Federal Trustworthy AI Legislation

Canada's National AI Strategy should commit to establishing comprehensive trustworthy AI legislation governing federal public sector AI systems. This legislation should include:

- Mandatory disclosure of AI systems, including public "AI registers".
- An explicit commitment that AI systems must protect human rights, privacy, and procedural fairness.
- An explicit commitment to risk-based regulation, including explicit criteria to identify authorized, high-risk, and prohibited AI systems.
- Mandatory AI impact assessments.
- A duty to measure, correct and audit bias in AI systems.
- Auditing and evaluation requirements.
- Remedial requirements.
- Independent oversight of both specific AI systems and AI systems generally.

Introduction

Many governments have responded to AI risks and challenges by adopting "trustworthy AI" legislation, frameworks, and policies. These initiatives are intended to assure the public and stakeholders that government AI development and use will be beneficial, lawful, and accountable.

The National AI Strategy should commit to establishing a comprehensive legislative trustworthy AI "baseline" to effectively address government AI risks and build public trust in Canada. Federal public sector AI regulation should become the model and foundation for promoting trust and accountability in private sector AI systems.

Issue

It is widely acknowledged that public sector AI systems can affect the most significant rights and interests in Canadian's lives, including their personal liberty; *Charter* rights; human rights; privacy rights; child welfare; and access to employment, health care, education, housing, economic opportunities, and income security.[10] It is also widely acknowledged that public sector AI risks fall disproportionately on low-income, Indigenous, racialized or otherwise vulnerable communities and individuals.[11]

Internationally, the most comprehensive and significant "trustworthy AI" framework is the European Union's *Artificial Intelligence Act*.[12] Many other national, regional and municipal governments across the world have also established comprehensive legislative regimes in specific jurisdictions or sectors.[13]

There have been several important trustworthy AI initiatives in Canada, including the Government of Canada's Directive on Automated Decision-making ("the Canada ADM Directive")[14], the proposed

federal *Artificial Intelligence and Data Act* (*AIDA*)[15], and Ontario's *Enhancing Digital Security and Trust Act, 2024* (EDSTA).[16]

These initiatives, while important, are also incomplete. For example, Canada ADM Directive is a government directive, not legislation. Nor does the Canada ADM Directive establish a right to context AI decision-making.[17] *AIDA* would have only applied to public sector AI systems indirectly.[18] And Ontario's *EDSTA* fails to address AI systems used in the criminal justice system and does not include provisions respecting human rights, public AI registries, risk categories, or impact assessments.[19] As a result, the LCO and others have concluded that the Canada ADM Directive, *AIDA,* and *EDSTA* fall short of establishing "trustworthy AI" in Canadian public sector AI systems.

The National AI Strategy gives the Government of Canada the opportunity to establish a truly comprehensive, effective and accountable public sector AI governance framework. In order to do so, however, the National Strategy cannot rely on vague, incomplete or unaccountable commitments to "ethical AI" and/or exclude key sectors of government decision-making.

Fortunately, key elements of the LCO's proposed federal public sector AI regulatory framework are both grounded in existing Canadian law, initiatives and proposals and consistent with international standards.[20] These elements include:

- Mandatory disclosure of federal public sector AI systems, including public "AI registers".
- An explicit commitment that federal public sector AI systems must protect human rights, privacy, and procedural fairness.
- An explicit commitment to risk-based regulation, including explicit criteria to identify authorized, high-risk, and prohibited AI systems.
- Mandatory AI impact assessments.
- A duty to measure, correct and audit bias in AI systems.
- Auditing and evaluation requirements.
- Remedial requirements.
- Public engagement.
- Independent oversight of AI systems.

The LCO believes these commitments should be established in legislation. Legislation (and accompanying regulations) is necessary to establish a level of public and legal accountability commensurate with the rights and risks at stake. Most significantly, properly designed federal legislation would mitigate the most serious AI risks and protect the legal rights of the most vulnerable Canadians, including racialized communities, Indigenous communities, low-income Canadians and others. By way of contrast, ethical AI policies or guidelines are insufficient to mitigate the risks and harms caused by government AI systems due to their lack of specificity, lack of legal accountability, and reliance on voluntary compliance.

The LCO further recommends that federal trustworthy AI legislation should not be too prescriptive or detailed. Legislation should, rather, establish trustworthy AI principles and objectives, leaving operational details to be set out in a mixture of "hard" and "soft" legal instruments, tailoring each to their appropriate purpose and context. Ethical guidelines, directives, "playbooks" and best practices have significant potential to *supplement* legislation and regulations but are not a substitute.

Finally, the LCO recommends that federal public sector AI regulation become the model and foundation for promoting trust and accountability in private sector AI systems. It is crucial that the federal government not rely exclusively on "ethical AI" guidelines or standards to "protect human rights, serve the public good and inspire trust" in private sector AI systems. This is because many of the risks, harms and legal duties present in private sector AI systems are the same risks, harms and legal duties present in public sector systems. For this reason, the LCO emphasizes that many of the legal requirements and principles governing Canadian public and private sector AI systems should be the same, including:

- Legal duty to comply with human rights and privacy laws.
- Risk-based regulation.
- AI impact assessments.
- Duty to measure, correct and audit bias in AI systems.
- Auditing and evaluation requirements.

That said, there are important differences between public and private sector AI governance. For example, public sector AI systems have a greater obligation for transparency and must with the *Charter* with administrative law legal procedural fairness requirements.[21]

Benefits/Outcomes

If adopted, LCO Recommendation #1 would:

- Establish a comprehensive, consistent baseline for Canadian AI systems to ensure they protect human rights, serve the public good and inspire public trust.
- Mitigate the most serious AI risks and protect the legal rights of the most vulnerable Canadians, including racialized communities, Indigenous communities, low-income Canadians and others.
- Provide clear regulatory guidance to Canadian governments, AI innovators, investors and others on how to promote responsible development and adoption of AI in public sector AI systems.
- Establish a principled but flexible national public sector AI governance standard that could be adopted or adapted by other governments, public agencies and the private sector.
- Establish a Canadian AI governance framework consistent with emerging international standards.

The key elements of our proposed trustworthy AI legislation are set out on the next two pages.

Key Elements of Comprehensive Public Sector Trustworthy AI Legislation

Mandatory Disclosure Of AI Systems, Including Public AI Registers.

Disclosure and transparency are key principles of trustworthy AI. One of the most effective and common strategies for promoting disclosure and transparency is an AI registry.[22]

The federal government should enshrine the principles established in the Canada ADM Directive and federal AIA, including a mandatory disclosure requirement for AI systems and appropriate notice and explanations to individuals for decisions made by or with the assistance of an AI system.[23] The specific information to be disclosed should be applied on a sliding scale depending on each system's risk.

Commitment To Protect Human Rights, Privacy, And Procedural Fairness.

Human rights, privacy and procedural fairness have been transcendent issues in AI design, development, regulation, and oversight across the world for many years.[24] These rights are enshrined in the *Charter*, Canadian human rights and privacy legislation, and administrative law.[25] Human rights and privacy rights must be addressed in all AI systems, while procedural fairness must be upheld in public sector systems. Ensuring AI systems respect these rights is foundational to trustworthy AI. As a result, protecting human rights, privacy and procedural fairness should be explicit objectives in Canada's national AI legislation.

Risk-Based Regulation, Including Criteria to Identify Authorized, High-Risk, and Prohibited AI Systems.

Federal legislation should identify the risks, principles, categories, or criteria used to assess public sector AI system risk. Risk-based AI regulation is explicit in the Canada ADM Directive[26]; *AIDA*[27]; the EU *AI Act*[28]; American federal AI regulations[29], the U.S. *AI Bill of Rights*[30]; and other AI governance regimes.

Risk-based regulation is both a practical response to the risks and harms of AI systems and responsive to the principles and requirements of Canadian law. A risk-based approach allows for the most optimal balance between encouraging innovation and safeguarding rights. Risk-based AI governance ensures regulatory obligations are tailored proportionately and the most onerous regulatory obligations attach only to the highest risk AI systems. Clear and consistent risk assessment categories also discourage risk assessment "ethics washing" and promote public trust and accountability.

Mandatory AI Impact Assessments.

AI impact assessments (AIAs) and human rights impact assessments (HRIAs) are proactive tools to identify and mitigate AI risks. AIAs and HRIAs help IT professionals and organizations build better AI systems by minimizing foreseeable risks/harms and providing a level of due diligence compliance with legal and other important obligations.[31]

AIAs and HRIAs are increasingly being required by legislation or adopted by governments, public institutions, and private enterprises to demonstrate and implement "trustworthy AI."[32] The leading AI impact assessment tool in Canada is the federal government's *Algorithmic Impact Assessment*.[33]

Another leading example is the LCO's AI Human Rights Impact Assessment, developed in partnership with the Ontario Human Rights Commission.[34]

Duties to Measure, Correct and Audit Bias in AI Systems.

AI systems can be biased or discriminatory against individuals on the grounds of race, age, disability, sex, family structure or other grounds protected by the *Charter* or federal or provincial human rights law. Canadian governments, public sector agencies and the private sector have a legal duty not to discriminate.[35]

Mandatory Auditing And Evaluation Requirements.

There is a broad consensus that AI systems should be subject to regular oversight and evaluations. Audit and evaluations are needed to ensure AI systems are "fit for purpose", do not discriminate, do not "drift", and are fulfilling their original objectives.

The Canada ADM Directive, *AIDA*, and other trustworthy AI frameworks link the frequency and type of audit or evaluation to risk.[36] High risk AI systems should be subject to periodic independent reviews, including representatives from a broadcross-section of experts and stakeholders, including data scientists, legal representatives, and members of the communities most affected by the AI system.

Remedial Requirements.

Access to meaningful remedies is a key principle of legal accountability and access to justice. Trustworthy AI legislation should include dedicated AI remedial provisions to ensure the ability to challenge both AI systems generally and individual AI decisions specifically.[37]

Public Engagement.

Public trust and good governance in AI systems is dependent on meaningful and ongoing public engagement. Participation must include technologists, the private sector, public agencies, academics, NGOs, legal professionals, and, most crucially, the communities of Canadian who are likely to be most affected by AI.

Independent Oversight Of AI Systems.

Many trustworthy AI proposals and AI legislative regimes include provisions creating independent oversight of AI systems, designating officials responsible for overseeing AI systems within their organizations, and/or procedures to enforce AI regulatory requirements.[38] For example, *AIDA* included provisions creating an AI and Data Commissioner who would have been largely responsible for enforcing the Act.[39] Similar requirements are included in *EDSTA*, the EU *AI Act*, and other legislation.[40]

Recommendation #2 AI in the Canadian Criminal Justice System

Canada's National AI Strategy should commit the Government of Canada to address AI systems used in the Canadian criminal justice system, including systems used by law enforcement agencies and in criminal courts.

Introduction

Establishing federal trustworthy AI legislation is a necessary but incomplete first step to address serious AI risks and build trust in Canadian AI systems. A second foundation of this strategy should be to develop a comprehensive plan to address AI systems used in the criminal justice system.

The National AI Strategy should address AI in criminal justice for two reasons: First, criminal justice is the sector where AI systems have been adopted most quickly and most widely. Second, criminal justice AI systems potentially have the greatest impact on individual rights, including the right to liberty, *Charter* rights, human rights, and privacy rights.

Issue

The LCO's AI in the Criminal Justice Project is a groundbreaking survey and analysis of AI in the Canadian criminal justice system.[41] Over several months we have engaged hundreds of criminal justice experts, professionals, and advocates in the question of how AI may be responsibly deployed in Canadian criminal justice.

Our research shows how criminal justice systems across the world are at the forefront of AI adoption. Criminal jurisdictions outside of Canada employ AI to improve police investigations, analyze evidence, assist judicial decision-making, improve data analysis, and target resources. Our research also shows that AI raises novel, complex and consequential issues at each stage of a criminal proceeding.[42]

AI technologies used in criminal justice today include predictive policing, facial recognition technology (FRT) and biometric surveillance, social media analysis, object tracking, licence plate readers, bail and sentencing algorithms, drones, body cam videos, voice analysis, and many other applications.[43] As reported in the LCO's detailed project papers, many of these systems have been used in Canada.

AI technology is seen as particularly beneficial in policing, where many commentators see AI as transformative. For example, facial recognition technology has been described as a "game-changer" in criminal investigations that allows police services "to respond swiftly to emerging threats and prevent crimes before they occur."[44]

It is widely recognized that the use of AI in criminal justice raises profound risks to fundamental legal rights. For example,

- Studies of FRT systems "have clearly demonstrated that racial and gender biases, meaning women and people of colour, are more likely to be misidentified by FRT and, therefore,

potentially more likely to be wrongfully accused by police who use FRT than light-skinned men."[45] Many predictive policing and bail/sentencing algorithms have also been shown to be biased and discriminatory.[46]

- Privacy and surveillance risks are widely acknowledged in criminal AI systems, particularly FRT systems, including the risk of mass surveillance, racial profiling, and individual tracking.[47]
- Criminal AI systems are frequently criticized for their lack of disclosure and transparency, which can significantly undermine public trust.[48] The RCMP's use of Clearview AI is the best-known Canadian AI disclosure controversy.[49]
- FRT, predictive policing and other criminal justice AI systems have been subject to strident criticisms about the accuracy, reliability and validity of their training data.[50]
- Criminal AI systems raise several oversight risks. Absent clear and consistent legal policies or guardrails, each police service could adopt its own individual AI policy, creating wide gaps in AI governance, trust, and accountability.
- Finally, criminal AI systems raise individual and systemic access to justice risks.[51]

Any of these risks could lead to miscarriages of justice for individual accused, including risks of false arrest and false imprisonment; risks to *Charter* rights and civil liberties; and risks to personal privacy.

It is well-established that criminal AI risks fall disproportionately on low-income, Indigenous, racialized or otherwise vulnerable communities and individuals. As a result, failure to address these risks could compound the existing overrepresentation of low-income, racialized, and Indigenous communities in the Canadian criminal justice system. Failure to address these risks could also undermine public trust in important public institutions, including the police and courts.

The benefits and risks of AI in the criminal justice system are well-known. As a result, a wide range of laws, policies and frameworks have been developed based on the principle that criminal AI benefits depend on dedicated and sophisticated rules to minimize risks and harms.

Internationally, the European Union's *Artificial Intelligence Act* (EU *AI Act*) includes prohibitions on several criminal AI systems, including real time biometric surveillance and certain predictive policing systems.[52] The EU *AI Act* also identifies several AI tools in "law enforcement" and the "administration of justice" as being presumptively high-risk and thus subject to more detailed regulatory requirements.[53] In the United States, detailed criminal justice AI legislation, executive orders, policies, and rules have been adopted or proposed by the federal government, states, municipalities, police services and NGOs.[54]

There have been many positive developments in criminal AI governance in Canada as well. To their credit, several Canadian police services, Privacy Commissioners and others have taken important initiatives to address criminal AI risks. Important examples include the RCMP's National Technologies Onboarding Program (NTOP)[55], the Toronto Police Service's "Use of AI Policy" [56], and several reports and guidances from Canadian Privacy Commissioners.[57]

Notwithstanding these initiatives, there are still wide and consequential gaps in the legal framework governing Canadian criminal AI systems, including:

- Lack of mandatory and consistent disclosure requirements. Most police services in Canada could implement predictive policing, FRT or other forms of AI without disclosing them publicly.
- Lack of criminal AI prohibitions, "guardrails" or consistent risk criteria. In Canada, there are no legal "guardrails" prohibiting or regulating the highest risks criminal AI systems, such as real time mass surveillance or predictive policing. Nor are there transparent and consistent risk categories to consistently identify criminal AI risks and mitigation strategies.
- Lack of mandatory impact assessments. There is no federal or provincial obligation for any actor to assess the impact of a criminal AI system on *Charter* rights, human rights, or privacy.
- Lack of procedural and evidential protections. In Canada, there are no explicit procedural protections governing police or court use of high-risk criminal AI systems, such as warrant requirements. Nor are there dedicated rules governing AI evidence, including "deep fakes."
- Lack of mandatory obligation to audit or evaluate AI systems. A police service could adopt an AI system without a duty to audit or evaluate its accuracy, bias, reliability, or effectiveness.
- Lack of dedicated AI access to justice protections.

The Government of Canada has constitutional responsibility for criminal law in Canada. As a result, the LCO recommends Canada's National AI Strategy explicitly address AI systems used in the Canadian criminal justice system. Unlike Recommendation #1, however, the LCO does not recommend specific criminal AI legislative principles or provisions at this point. This analysis will be available shortly, however, as we expect to release our Criminal AI Project report in the Spring of 2026.

Benefits/Outcomes

If adopted, LCO Recommendation #2 would:

- Promote comprehensive, consistent governance standards for Canadian criminal justice AI systems to ensure they promote public safety, protect fundamental rights, and build public trust.
- Provide clear regulatory guidance to government ministries, law enforcement agencies, Crown Attorneys and courts to promote the responsible development and adoption of AI.
- Mitigate serious criminal AI risks and protect the legal rights of the most vulnerable Canadians, including racialized communities, Indigenous communities, low-income Canadians and others.
- Reduce the risks of false arrest, false imprisonment, inappropriate prosecutions, violation of *Charter* rights, civil liberties, and privacy.
- Reduce the risk of compounding the existing overrepresentation of low-income, racialized, and Indigenous communities in criminal justice.
- Establish a principled but flexible national criminal AI governance standard that could adapted by other governments, law enforcement agencies and criminal justice institutions.
- Establish a Canadian criminal AI governance framework that is consistent with emerging international standards.

Recommendation #3 Human Rights and Procedural Fairness

Canada's National AI Strategy should commit the Government of Canada to developing comprehensive "human rights by design" and "fairness by design" strategies to protect human rights and procedural fairness in Canadian AI systems.

Introduction

Questions about AI risks to human rights and rights to procedural fairness are central to trustworthy AI.[58] These rights are protected in Canadian law by the *Charter,* federal and provincial human rights codes, and administrative law.

Canadian AI systems are subject to these laws but there are outstanding questions about how these rights can be protected in AI systems. Accordingly, the National AI Strategy should commit to developing a comprehensive plan to promote "human rights by design" and "fairness by design" in AI Canadian AI systems.

Human Rights

Human rights have been a transcendent issue in AI design, development, operation, and oversight across the world for many years.[59]

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.

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.

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.[60] This responsibility applies to both public and private AI systems that may be developed or deployed in Canada.

LCO Recommendations #1 and #2 address human rights compliance in part. Recommendation #1 would establish an explicit commitment that federal AI legislation will protect human rights. Recommendation #2 would commit the Government of Canada to address AI systems used in the Canadian criminal justice system, a sector where human rights issues are paramount.

The LCO's third recommendation would commit the National AI Strategy to take further steps to operationalize the commitments in Recommendations #1 and #2. For example, governments, technologists, legal organizations, academics, technologists, civil society organizations, and industry associations around the world have developed many promising examples, best practices and regulatory regimes to address bias, including disclosure requirements, validity/reliability/representativeness requirements, and testing and evaluations requirements.[61] The National AI Strategy should commit the Government of Canada to work with stakeholders to evaluate these practices and to develop "human rights by design" standards that could be adopted or adapted by Canadian governments, public agencies and the private sector. Topics addressed could include:

- AI human rights impact assessments.
- Data standards.
- Bias testing or auditing requirements.
- Human rights mitigation requirements.
- Guidance for policymakers to identify which AI systems or applications should be prohibited or preemptively identified as "high risk" on human rights grounds.

Administrative Law and Procedural Fairness

Unlike human rights obligations, administrative law and procedural fairness obligations only apply to decisions made by governments and public sector organizations.[62]

Government decisions range from minor, inconsequential decisions to major decisions affecting significant personal rights and interests. Government decisions affecting significant rights and interests could include decisions about government licenses, social benefits, health care, securities regulation, refugee or immigration determinations, education or employment opportunities, access to housing, and child welfare determinations, to name a few.[63] The Supreme Court of Canada has stated that administrative decision-making is "one of the principal manifestations of state power in the lives of Canadians."[64]

Administrative law is the area of law that holds governments accountable for these decisions. Governments, agencies and departments have a legal duty to be fair, transparent and accountable to Canadians.[65]

A decision by government that affects the rights, privileges or interests of an individual triggers a duty of fairness. This duty has been held to translate into an entitlement to fair procedure, which is founded on open decision-making and transparency. Fair procedure is achieved through:

- Notice of the case one needs to meet.
- Participation in the form of an oral hearing and/or written submissions.
- A decision by an open-minded decisionmaker considering relevant factors.
- An explanation or reasons for the decision.

Governments, including the Government of Canada, are very interested in accelerating the use of AI to assist in government decision-making. AI has the potential to make government decision-making faster, more efficient, more consistent, and fairer.

Government AI decision-making will be subject to administrative law.[66] AI systems will have to be designed, administered and evaluated to ensure compliance with two dimensions of administrative law: procedural fairness and substantive fairness. Unfortunately, as noted by administrative law expert Jennifer Raso, "administrative law is more gap than law when it comes to algorithmically-driven decision-making."[67]

One of the most common and important strategies for addressing concerns about AI accountability, transparency and fairness is to establish mandatory disclosure obligations and frontload AI systems with procedural fairness safeguards. These safeguards protect and promote trust in government AI systems.

Fortunately, the Government of Canada has taken important steps in this regard. The Canada ADM Directive and the federal AIA are leading examples of trustworthy AI tools and strategies that incorporate procedural fairness protections into the design and operation of AI and automated government decision-making.

The Canada ADM Directive and federal AIA are a good start but not a complete solution. Many features of the Directive raise the standard of administrative governance, which is clearly a positive step. However, the Directive also has gaps and shortcomings, even within the realm of federal administrative law. For example, the Directive has limitations on its scope and is thus less inclusive than administrative law generally.[68] Nor does the Directive have the legal status of a statute or regulation which would create actionable rights for individuals, limiting its impact/utility as a tool for protecting rights.[69]

As in the area of human rights, LCO recommends the National AI Strategy commit the Government of Canada to develop comprehensive "fairness by design" safeguards across federal public sector AI systems.

Benefits/Outcomes

If adopted, LCO Recommendation #3 would:

- Establish national standards for Canadian AI systems to ensure they protect human rights, protect procedural fairness, serve the public good, and inspire public trust.
- Mitigate the most serious AI risks and protect the human rights of the most vulnerable Canadians, including racialized communities, Indigenous communities, low-income Canadians and others.
- Ensure administrative law procedural fairness obligations were embedded and expanded in federal public sector administrative decision-making.
- Establish "human rights by design" and "fairness by design" standards that could be adopted or adapted by other Canadian governments, public agencies and the private sector.
- Establish a Canadian trustworthy AI governance framework that is consistent with emerging international standards.

Recommendation #4 AI "Red-Lines" and Pre-emptive Risk Regulation

Canada's National AI Strategy should commit the Government of Canada to engage in public consultations to identify criteria, contexts and uses of AI systems that may be prohibited, pre-emptively identified as high-risk, or otherwise subject to higher regulatory standards.

Introduction

AI system "red-lines", prohibitions, use case restrictions, and pre-emptive risk identification are probably the most consequential topic of trustworthy AI legislation and regulation.

The National AI Strategy should commit to studying AI system "red-lines", prohibitions, use case restrictions, and pre-emptive risk identification to determine if, and how, these rules could be used to minimize AI risks and build public trust.

Issue

AI "red lines" and pre-emptive risk identification is probably the most consequential and high-profile strategy to build trust in AI systems and reduce AI risks. These strategies are a feature of many, if not most, emerging trustworthy AI regulatory frameworks. This is because AI "red lines" and pre-emptive risk identification have the potential to eliminate or mitigate the most serious and high-profile AI risks. For example, AI red-lines or prohibitions on police use of real time facial recognition technology could drastically minimize the risks of FRT-enabled mass surveillance, over-policing of racialized communities, and mass privacy violations. Similarly, a pre-emptive "high risk" designation for AI systems used to aid hiring or determine social benefits could ensure these systems are subject to higher bias and discrimination mitigation requirements.

In Canada, AI "red-lines" and pre-emptive risk identification are included in the Canada ADM Directive, *AIDA*, Ontario's *EDSTA*, and several other trustworthy AI frameworks in Canada.

AIDA, for example, stated that "high-impact systems" were those that met criteria "that are established in regulations."[70] *AIDA* then established requirements for persons responsible for high-impact AI systems to "establish measures to identify, assess and mitigate the risks of harm or biased output" in accordance with *AIDA* regulations.[71]

As originally proposed, *AIDA* did not pre-emptively identify "high-risk" systems. In November 2023, however, the federal Minister subsequently committed to amendments that would define seven "classes of systems that would pre-emptively be considered high impact", including

Class 1: The use of an artificial intelligence system in matters relating to determinations in respect of employment, including recruitment, referral, hiring, remuneration, promotion, training, apprenticeship, transfer or termination.

Class 2: The use of an artificial intelligence system in matters relating to:
a. the determination of whether to provide services to an individual;
b. the determination of the type or cost of services to be provided to an individual; or
c. the prioritization of the services to be provided to individuals.

Class 3: The use of an artificial intelligence system to process biometric information in matters relating to
a. the identification of an individual, other than in cases in which the biometric information is processed with the individual's consent to authenticate their identity; or
b. the assessment of an individual's behaviour or state of mind.

Class 4: The use of an artificial intelligence system in matters relating to:
a. the moderation of content that is found on an online communications platform, including a search engine or social media service; or
b. the prioritization of the presentation of such content.

Class 5: The use of an artificial intelligence system in matters relating to health care or emergency services.

Class 6: 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.

Class 7 The use of an artificial intelligence system to assist a peace officer, as defined in section 2 of the Criminal Code, in the exercise and performance of their law enforcement powers, duties and functions.

The Minister's letter included detailed explanations for why each class of system should be pre-emptively identified as "high impact."[72]

Another Canadian example of AI "red lines" and pre-emptive risk identification is the Toronto Police Service's "Use of AI Policy," described above. This policy identifies both "extreme risk technologies" which "may not be considered for adoption" (such as mass surveillance or predictive policing), and "high risk technologies" (including applications that link biometric technologies to personal information) that are subject to higher oversight requirements.[73]

Internationally, many governments have enacted or proposed bans on certain technologies or their use in specific circumstances. Most notably, Chapter II, Article 5 of the EU *AI Act* sets out several "unacceptable risks" and prohibitions on specified AI systems. These provisions came into force in February 2025. These systems are deemed "unacceptable" because they are a clear threat to European values and fundamental rights, including:

- **Subliminal or Manipulative Techniques:** Using subliminal or manipulative techniques to distort decision-making leading to significant harm.
- **Vulnerability Exploitation:** Exploiting vulnerabilities due to age, disability, or social or economic situations, causing significant harm.
- **Biometric Categorization:** Inferring sensitive personal attributes such as race, political, religious or philosophical belief, trade union membership, through biometric systems, except for lawful law enforcement purposes.
- **Social Scoring:** Evaluating or classifying individuals based on social behaviour or personal characteristics, leading to unfair or disproportionate treatment.
- **Real-time Biometric Identification:** 'Real-time' remote biometric identification in public spaces for law enforcement, with specific necessary exceptions.
- **Predictive Policing:** Assessing the risk of criminal offences based solely on profiling or personality traits, except to support human assessments based on verifiable facts.
- **Database Creation through Scraping:** Creating or expanding facial recognition databases through untargeted scraping from the internet or CCTV footage.
- **Emotion Inference:** Inferring emotions in workplaces or educational institutions, except for medical or safety reasons.[74]

In addition to outright prohibitions, Article III of the EU *AI Act* pre-emptively defines several systems as "high-risk" due to their significant risk to rights and freedoms, including bail and sentencing algorithms and AI-generated evidence in trials.[75] The EU *AI Act* also sets out important accountability safeguards if police or governments want to deploy high-risk systems, including requirements respecting:

- Risk management throughout the system's lifecycle.
- Data governance, validation, and testing.
- Technical documentation.
- Record-keeping for identifying national level risks.
- Human oversight.
- Accuracy, robustness, and cybersecurity.
- Quality management to ensure compliance.[76]

Other examples of emerging AI bans or pre-emptive risk identification include:

- **Facial Recognition and Other Biometric Technologies.** More than 20 American jurisdictions have enacted bans and limits on FRT use, especially in law enforcement.[77]
- **Elections.** A bill in Alaska would prohibit the use of synthetic media, which means content manipulated by AI, in elections communications that attempt to influence election outcomes.[78]
- **Children.** California has introduced legislation prohibiting software developers from knowingly or recklessly training certain software products by using the personal information of a child.[79]
- **Pricing.** A bill in Maine would have prohibited landlords who determine rent prices from using AI or other algorithmic systems to establish rent prices.[80]

The LCO believes that AI system "red lines", prohibitions, use case restrictions, and pre-emptive risk identification could have significant implications for AI governance, protection of fundamental rights, and building public trust in Canadian AI systems.

To address these issues proactively, the LCO recommends that Canada's National AI Strategy should commit the Government of Canada to engage in public consultations identify criteria, contexts and uses of AI systems that may be prohibited, pre-emptively identified as high-risk, or otherwise subject to higher regulatory standards. This commitment would mirror comparable initiatives in the European Union and elsewhere to study these important AI governance tools.[81]

Public consultations on this initiative should involve a wide range of stakeholders including legal professionals, IT developers, industry, NGOs, community groups, and representatives from public agencies, law enforcement, social services, the justice system, and client communities.

The Government of Canada should note that the LCO will be beginning its own AI "red-line" and pre-emptive risk regulation project in early 2026.

Benefits/Outcomes

If adopted, LCO Recommendation #4 would:

- Promote the development of a comprehensive, consistent governance standard for Canadian AI systems to ensure they protect fundamental rights and build public trust.
- Provide clear regulatory guidance to Canadian governments, public agencies, law enforcement agencies, and the private sector about the highest risk AI systems, including which systems were prohibited or otherwise subject to higher regulatory standards and mitigation requirements.
- Mitigate the most serious AI risks and protect the legal rights of the most vulnerable Canadians, including racialized communities, Indigenous communities, low-income Canadians and others.
- Establish a principled but flexible "high risk" AI governance standard that could adapted by other governments, public agencies, and private sector organizations.
- Establish a high risk AI governance framework that is consistent with emerging international standards.

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

[2] For a good description of how governments are using AI systems and their impact on rights, see generally, Law Commission of Ontario, *Accountable AI*, [Accountable AI] (2022), online at https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/ai-and-adm-in-the-civil-administrative-justice-system/ at 12-19 and 40-49 and Law Commission of Ontario, *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/ at 20-24.

[3] *Ibid*. See also our discussion in LCO Recommendation #3.

[4] The LCO's trustworthy AI analysis is set out in four main LCO reports and submissions, including *Accountable AI; LCO Criminal AI Introduction*; Law Commission of Ontario, *Bill 194, Law Commission of Ontario Submission* [LCO Bill 194 Submission] (2024), online at https://www.lco-cdo.org/en/lco-releases-bill-194-submission/; and Law Commission of Ontario, *Regulating AI: Critical Issues and Choices* [Regulating AI] (2022), online at https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/regulating-ai-critical-issues-and-choices/.

[5] University of Melbourne/KPMG International, *Trust, attitudes and the use of artificial intelligence, A Global Study 2025* [KPMG] (2025), online at: https://kpmg.com/xx/en/our-insights/ai-and-technology/trust-attitudes-and-use-of-ai.html at 4.

[6] KPMG at 5.

[7] KMPG at 32.

[8] See the LCO reports listed in fn 4.

[9] For example, a recent OCED report stated that guardrails are a key factor in building trust in AI:

> *Guardrails help to ensure the trustworthy deployment, development and use of AI in government. They can be binding and non-binding policy levers, transparency processes and accountability mechanisms, such as monitoring and oversight bodies. Guardrails are essential for managing the risks associated with AI and deploying AI according to legal boundaries and social values. This ultimately helps to build public trust in government*.

OECD, *Governing with Artificial Intelligence*, September 2025, https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en/full-report/enablers-guardrails-and-engagement-for-unlocking-trustworthy-ai_2f817983.html#section-d1e17781-90fb51a114

[10] See the references in fns 4 and 5.

[11] *Ibid*.

[12] European Union, *AI Act (Regulation (EU) 2024/1689 of the European Parliament and of the Council of Europe laying down harmonized rules on Artificial Intelligence* [EU AI Act] (2024), online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689. For a good summary of the EU AI Act, see the European Commission's EU AI Act webpage at https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.

[13] There are many compendiums of "trustworthy AI" statutes and frameworks available on several websites, including: UNESCO, Global AI Ethics and Governance Observatory, *Global Hub,* online: https://www.unesco.org/ethics-ai/en/global-hub; IAPP, *Global AI Law and Policy Tracker*, online: https://iapp.org/resources/article/global-ai-legislation-tracker/; and Fairly AI, *Global AI Regulation Tracker*, online: https://www.fairly.ai/blog/map-of-global-ai-regulations, to name a few.

[14] 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.

[15] *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*.
[16] *Enhancing Digital Security and Trust Act*, S.O. 2024, c. 24, [*EDSTA*], online: https://www.ontario.ca/laws/statute/24e24.
[17] For a complete analysis of the Canada ADM Directive, see *Regulating AI* at 17-49 and *Accountable AI* at 57-66.
[18] *AIDA*, s. 3.
[19] Nor does *EDSTA* include provisions addressing human rights, civil liberties, non-discrimination, equality, or fairness. See generally, LCO Bill 194 Submission.
[20] See fn 13 for examples.
[21] See generally, *Accountable AI* at 56-66. The similarities and differences between public and private AI systems are discussed in more detail in our discussion of Recommendation #3.
[22] LCO Bill 194 Submission at 17-19.
[23] Canada ADM Directive, s.6.2.1. and 6.2.2.
[24] For an extensive discussion of AI, human rights, privacy, and procedural fairness, see LCO Accountable AI.
[25] *Ibid.*
[26] Canada ADM Directive, Appendix B – Impact Assessment Levels.
[27] See generally, Canada, *The Artificial Intelligence and Data Act (AIDA) – Companion Document* [*AIDA* Companion Document], online: https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document#s6.
[28] See generally, European Commission, "*Shaping Europe's Digital Future, AI Act*", online: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai.
[29]United States, Office of the President, Executive Order 14110 "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" [Executive Order 14110] (November 1 2023), online: https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence; Office of Management and Budget, Executive Order M-24-10 "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence" [Executive Order M-24-10] (March 2023].
[30] The White House, *Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People* (2022), online: https://www.whitehouse.gov/ostp/ai-bill-of-rights/.
[31] Law Commission of Ontario, *Human Rights AI Impact Assessment: Backgrounder* [LCO HRIA Backgrounder], (2025), online at https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/human-rights-ai-impact-assessment/ at 9-12.
[32] LCO HRIA Backgrounder at 9-10.
[33] Federal AIA.
[34] Law Commission of Ontario and Ontario Human Rights Commission, *Human Rights AI Impact Assessment* [LCO HRIA], (2025), online at https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/human-rights-ai-impact-assessment/.
Human
[35] *Accountable AI* at 40-55.
[36] See generally, Canada, *The Artificial Intelligence and Data Act (AIDA) – Companion Document* [*AIDA* Companion Document], online: https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document#s6.
[37] LCO Regulating AI at 47-48.
[38] For a good summary of AI oversight models, see New Zealand Law Foundation, *Government Use of Artificial intelligence in New Zealand* [NZ Government AI] (2020), online: https://www.researchgate.net/publication/338701988_Government_Use_of_Artificial_Intelligence_in_New_Zealand at 4. See also LCO Bill 194 Submission at 21-23.
[39] *AIDA*, s. 33.

[40] For example, see *ETSDA* s. 6(2)(b), EU *AI Act* EU *AI Act*, Chapter VII: Governance, online at https://artificialintelligenceact.eu/chapter/7/; and New York City, Executive Order 50, *Establishing An Algorithms Management And Policy Officer* (2019), online at https://www.nyc.gov/office-of-the-mayor/news/554-19/mayor-de-blasio-signs-executive-order-establish-algorithms-management-policy-officer at 1. Note that this role has been updated by the current New York City administration in a "New York City Artificial Intelligence Action Plan" which includes a new Office of the Technology and Innovation. See generally, New York City, "Mayor Adams Releases First-of-Its-Kind Plan for Responsible Artificial Intelligence Use in NYC Government" (October 16, 2023), online: https://www.nyc.gov/office-of-the-mayor/news/777-23/mayor-adams-releases-first-of-its-kind-plan-responsible-artificial-intelligence-use-nyc#/0.
[41] All project materials are available at https://www.lco-cdo.org/en/our-current-projects/crimai/.
[42] For a summary, see LCO Criminal AI Introduction at 25-28.
[43] For a summary, see LCO Criminal AI Introduction at 13-19.
[44] Brandon Epstein, "Navigating the Future of Policing" in Police Chief Magazine [Police Chief Magazine] (April 2024), online: https://www.policechiefmagazine.org/navigating-future-ai-chatgpt/.
[45] I 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* (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.
[46] National Academies of Sciences, Engineering, and Medicine, *Law Enforcement Use of Predictive Policing Approaches: Proceedings of a Workshop – In Brief* [NAS Predictive Policing] (2024), online: https://nap.nationalacademies.org/catalog/28037/law-enforcement-use-of-predictive-policing-approaches-proceedings-of-a at 2: "…in practice, predictive algorithms have fueled hot spots policing that too often results in the over-policing of communities and residents, imposing biases that have detrimental impacts on people of color." See also, Partnership on AI (PAI), *Report on Algorithmic Risk Assessment Tools in the U.S. Criminal Justice System*, (April 2019), online: https://www.partnershiponai.org/report-on-machine-learning-in-risk-assessment-tools-in-the-u-s-criminal-justice-system/.
[47] See generally, INTERPOL Policy Framework and INCLO Challenging FRT as illustrative examples.
[48] See the LCO's American Lessons report for a good summary of these issues.
[49] Office of the Privacy Commissioner of Canada, *Report of findings: Investigation into the RCMP's collection of personal information from Clearview AI (involving facial recognition technology)* (June 10, 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/ at para. 7.
[50] See INCLO Challenging FRT, Ferguson 2019, and LCO American Lessons for representative examples of this analysis.
[51] See generally, LCO Criminal AI Introduction at 24 and the LCO's detailed criminal AI project background papers.
[52] European Union, *AI Act (Regulation (EU) 2024/1689 of the European Parliament and of the Council of Europe laying down harmonized rules on Artificial Intelligence* [EU AI Act] (2024), online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R1689. Chapter II, Article 5 of the EU *AI Act* sets out several "unacceptable risks" and prohibitions on specified AI systems. These systems are deemed "unacceptable" because they are a clear threat to European values and fundamental rights.
[53] The EU *AI Act*, Chapter III, Annex III list of "high risk" systems include:

Law Enforcement

- Used to assess an individual's risk of becoming a crime victim.
- Polygraphs.
- Evaluating evidence reliability during criminal investigations or prosecutions.

- Assessing risk of an individual offending or re-offending not solely based on profiling or assessing personality traits or past criminal behaviour.

Administration of Justice

- AI systems used in researching and interpreting facts and applying the law to concrete facts or used in alternative dispute resolution.

[54] American initiatives are discussed at length in the LCO Criminal AI Introduction. See also generally, United States, Office of the President, Executive Order 14110 "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" (November 1 2023), online: https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence; Office of Management and Budget, Executive Order M-24-10 "Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence" (March 2023); AINow Institute, "A Taxonomy of Legislative Approaches to Face Recognition in the United States" in *Regulating Biometrics: Global Approaches and Open Questions* (Sept 2020), online: https://ainowinstitute.org/publication/regulating-biometrics-global-approaches-and-open-questions; New York Police Department, Facial Recognition Technology Policy, P.G. 212-129, (2020), online: https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page; and Policing Project, New York University School of Law, *Regulating Police Use of Facial Recognition Technology – Resources for Legislators* (2025), online: https://www.policingproject.org/regulating-police-use-of-face-recognition-technology.

[55] Royal Canadian Mounted Police, *RCMP Publishes Transparency Blueprint: Snapshot of Operational Technologies* [RCMP Transparency Blueprint] (September 2024), online: https://rcmp.ca/en/news/2024/09/rcmp-publishes-transparency-blueprint-snapshot-operational-technologies.

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

[57] [57] Important trustworthy AI reports and guidances from Canadian Privacy Commissioners include: Office of the Privacy Commissioner of Canada, Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta (2021), online at https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/; Office of the Privacy Commissioner of Canada, *Police use of Facial Recognition Technology in Canada and the Way Forward* (2021), online at https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/; Information and Privacy Commissioner of Ontario, *Facial Recognition and Mugshot Databases: Guidance for Police in Ontario* (2024), online at https://www.ipc.on.ca/wp-content/uploads/2024/01/2024-01-19-facial-recognition-and-mugshot-databases-guidance-for-police-in-ontario-e.pdf; and *Guidance on the Use of Automated Licence Plate Recognition Systems by Police Services* [IPC ALPR Guidance] (2024), online: https://www.ipc.on.ca/en/resources-and-decisions/guidance-use-automated-licence-plate-recognition-systems-police-services.

[58] Accountable AI at 40-70.

[59] For an extensive discussion of AI and human rights, see LCO Accountable AI at 40-56.

[60] *Ibid.*

[61] *Ibid.*

[62] Accountable AI at 56-71.

[63] For a comprehensive list of how governments are using AI systems, see Accountable AI at 13-16.

[64] *Canada (Minister of Citizenship and Immigration) v Vavilov*, 2019 SCC 65 [*Vavilov*] at para 4.

[65] For an extensive discussion of AI and administrative law, see LCO Accountable AI at 56-71.

[66] *Ibid.*

[67] Jennifer Raso, "AI and Administrative Law" in Florian Martin-Bariteau & Theresa Scassa, eds, *Artificial Intelligence and the Law in Canada* (2021) at 16.

[68] LCO Regulating AI at 10 and 19-20
[69] LCO Regulating AI at 21 and 25
[70] *AIDA*, s. 5(1).
[71] *AIDA*, sections 7 and 8.
[72] Canada. Innovation, Science and Economic Development Canada, "Letter to the Chair of the Standing Committee on Industry and Technology on Bill C-27" (November 28, 2023), online: https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12751351/12751351/MinisterOfInnovationScienceAndIndustry-2023-11-28-Combined-e.pdf.
[73] TPS Use of AI Policy.
[74] EU *AI Act*, Chapter II, Article 5, s. 1.
[75] EU *AI Act*, Chapter III, and Annex III.
[76] EU *AI Act*, Chapter III, Articles 8-17.
[77] These initiatives are documented comprehensively in the LCO Criminal AI Project Issue Papers.
[78] US, SB 64, A BILL FOR AN ACT ENTITLED An Act relating to elections; relating to voters; relating to voter registration; relating to election administration; relating to the Alaska Public Offices Commission, Relating to Campaign Contributions; Relating to Crimes of Unlawful Interference with Voting in the First Degree, Unlawful Interference with an Election, and Election Official Misconduct; Relating to Synthetic Media in Electioneering Communications; Relating to Campaign Signs; Relating to Voter Registration on Permanent Fund Dividend Applications; Relating to the Redistricting Board; Relating to the Duties of the Commissioner of Revenue; and Providing for an Effective Date, 34th Leg, 1st Session, Alaska, 2025
[79] US, AB 1064, AN ACT to Add Chapter 25.1 (Commencing with Section 22757.20) to Division 8 of the Business and Professions Code, Relating to Artificial Intelligence, 2025-2026, Reg Sess, Cal, 2025.
[80] US, LD 1552, AN ACT to prohibit landlords from setting rents through the use of artificial intelligence, 132nd Leg, 1st Spec Sess, Me, 2025.
[81] See generally, European Commission, "Commission launches consultation on AI Act prohibitions and AI system definition" (2024), online at https://digital-strategy.ec.europa.eu/en/news/commission-launches-consultation-ai-act-prohibitions-and-ai-system-definition.