LCO Issue Paper

Regulating AI: Critical Issues and Choices

April 2021

LCO
CDO

LAW COMMISSION OF ONTARIO
COMMISSION DU DROIT DE L'ONTARIO

About the Law Commission of Ontario

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

The LCO provides independent, balanced, and authoritative advice on complex and important legal policy issues. Through this work, the LCO promotes access to justice, evidence-based law reform and public debate.

The LCO evaluates laws impartially, transparently and broadly. The LCO's analysis is informed by legal analysis; multi-disciplinary research; contemporary social, demographic and economic conditions; and the impact of technology.

The LCO is located at Osgoode Hall Law School, York University, Toronto.

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

Law Commission of Ontario Reports

Legal Issues in the Last Stages of Life (Forthcoming 2021)
Indigenous Legal Issues in the Last Stages of Life (Forthcoming 2021)
AI, Algorithms and Government Decision-Making (Forthcoming 2021)
The Rise and Fall of AI and Algorithms in American Criminal Justice: Lessons for Canada (October 2020)
Defamation Law in the Internet Age (March 2020)
Class Actions: Objectives, Experiences and Reforms (July 2019)
Legal Capacity, Decision-making and Guardianship (March 2017)
Simplified Procedures for Small Estates (August 2015)
Capacity and Legal Representation for the Federal RDSP (June 2014)
Review of the Forestry Workers Lien for Wages Act (September 2013)
Increasing Access to Family Justice (February 2013)
Vulnerable Workers and Precarious Work (December 2012)
A Framework for the Law as It Affects Persons with Disabilities (September 2012)
A Framework for Teaching about Violence Against Women (August 2012)
A Framework for the Law as It Affects Older Adults (April 2012)
Modernization of the Provincial Offences Act (August 2011)
Joint and Several Liability Under the Ontario Business Corporations Act (February 2011)
Division of Pensions Upon Marriage Breakdown (December 2008)
Fees for Cashing Government Cheques (November 2008)

Authors

Nye Thomas, Executive Director, Law Commission of Ontario
Erin Chochla, LCO Student Scholar
Susie Lindsay, Counsel, Law Commission of Ontario

Disclaimer
The opinions or points of view expressed in the LCO's research, findings and recommendations do not necessarily represent the views of the LCO's Advisory Group members, funders (Law Foundation of Ontario, Osgoode Hall Law School, Law Society of Ontario) or supporters (Law Deans of Ontario, York University).

Citation
Law Commission of Ontario, *Regulating AI: Critical Issues and Choices* (Toronto: April 2021).

Contact

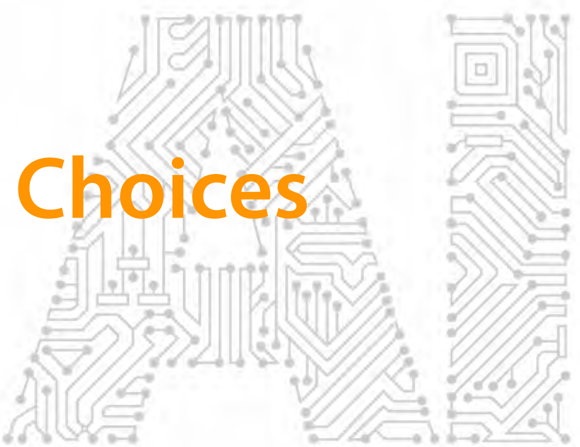
Law Commission of Ontario
2032 Ignat Kaneff Building
Osgoode Hall Law School, York University
4700 Keele Street
Toronto, Ontario, Canada
M3J 1P3

Email: LawCommission@lco-cdo.org
Web: www.lco-cdo.org
Twitter: @LCO_CDO
Tel: (416) 650-8406
Toll-free: 1 (866) 950-8406

Funders

The Law Commission of Ontario is funded by the ***Law Foundation of Ontario,*** the ***Law Society of Ontario***, ***Osgoode Hall Law School,*** and ***York University***. The LCO also receives significant in-kind support from Osgoode Hall Law School and York University.

CONTENTS



Regulating AI: Critical Issues and Choices

April 2021

I. INTRODUCTION

This is the second in a series of Law Commission of Ontario (LCO) Issue Papers considering the use of artificial intelligence (AI), automated decision-making (ADM) and algorithms in the Canadian justice system.

This paper identifies a series of important legal and policy issues that Canadian policymakers should consider when contemplating regulatory framework(s) for AI and ADM systems that aid government decision-making. Some of the issues considered in this paper include:

- Should government regulation of AI and ADM promote innovation, human rights or both?
- How should AI and ADM be defined for regulatory purposes?
- How and when should governments disclose their use of AI and ADM?
- What is the role of "ethical AI" in government regulation of AI and ADM?
- How can government regulation promote compliance with human rights and due process?

Ensuring that AI regulation is responsive to these issues may help Ontario and other Canadian jurisdictions develop a regulatory framework that maximizes AI and ADM's potential benefits, while minimizing potential harm.

Regulation of AI and ADM systems has become a pressing issue in Canada and across the world. The Government of Canada's *Directive on Automated Decision-making* ("the federal Directive") is the most significant initiative to directly regulate AI and ADM in Canada to date.[1] Many other governments, including the Government of Ontario, have begun to consider AI and ADM regulation as well.

The context for this analysis is the extraordinary growth in the use of AI and ADM by governments across the world. This technology promises many benefits, while also raising significant risks to human rights, due process, procedural fairness, access to justice and the trustworthiness of justice-system and government decision-making.

The LCO has concluded that Canadian legal standards and rules governing AI and ADM are insufficient.[2] Moreover, it is clear that the systemic legal issues raised by this technology cannot be addressed through individual litigation, best practices or piecemeal legislation. Comprehensive law reform is required. Proactive law reform supports better public services; economic development; AI innovation and trustworthiness; and fair and legitimate government and justice-system decision-making.

This report focusses considerable attention on the new federal Directive and its accompanying Algorithmic Impact Assessment.[3] Access Now, a leading international digital rights advocacy organization, has described the Directive as "pioneering."[4] The LCO agrees. Compared to many international alternatives, the Directive is a sophisticated and proactive initiative.

The LCO has analyzed the federal Directive and several alternative models in order to answer a series of important questions:

- What issues should AI and ADM regulation address?
- Which model (or models) best ensures AI and ADM transparency, accountability, protection of human rights, due process and "trustworthiness" in governments and related institutions?
- Are there gaps in the Canadian regulatory landscape?
- Is regulation in Canada robust or comprehensive enough to meet the proven challenges of these systems?
- What advice can the LCO give policymakers, stakeholders and the public about the form and content of AI and ADM regulation?

Our analysis is heavily influenced by the experience with AI and ADM systems that are already used by governments in North America, Europe, Australia and New Zealand. The risks of these systems have been well-documented.

This paper directs recommendations to the Governments of Canada and Ontario. Nevertheless, the LCO believes our analysis and recommendations are equally applicable to other provinces and a wide range of public agencies and institutions, including but not limited to municipal governments, school boards, police services, independent agencies, universities, hospitals, courts and tribunals. AI and ADM regulatory issues can and will arise in these contexts as well. Federal and provincial leadership in this field will help establish common rules and expectations across the country.

The LCO is mindful of the fact that AI and ADM regulation is a new and evolving area. The federal Directive itself effectively came into force on April 1st, 2020.[5] As a result, many of the law reform issues and questions in this area are not widely-understood. This paper is intended, in part, to be a primer on these topics for government officials, justice professionals, IT professionals, community organizations, academics and others who wish to engage in these ongoing discussions.

Readers should note that this review addresses what are sometimes described as "horizontal" or "framework" regulations. The federal Directive is an example of this kind of regulation. The paper does not address "vertical regulation." For example, implementation of AI or ADM tools in the criminal justice system should be accompanied by reforms to laws of evidence and criminal procedure. This paper does not address that level of specificity. Rather, the paper considers systemic issues that should be considered as part of a general regulatory framework for government use of AI or ADM systems. Nor does this paper consider regulation of AI and ADM in the private sector. Notwithstanding these limitations, the LCO believes the issues identified here are an important starting point.

Finally, as noted above, this is the second of a series of LCO reports addressing these issues. The LCO's first Issue Paper, published in October 2020, *The Rise and Fall of Algorithms in the American Justice System: Lessons for Canada*, provides Canadians with insights and lessons about the use of AI and ADM in criminal justice.[6] The LCO's third Issue Paper, *AI, ADM and Government Decision-Making,* will consider legal and policy issues when governments use AI and ADM in the civil and administrative justice systems.[7] The LCO's fourth Issue Paper, *Probabilistic Genotyping DNA Tools in Canadian Criminal Courts,* will be a detailed case study of an AI tool currently in use in Canadian courts.[8] The LCO has also published workshop reports, backgrounders and other materials on these topics.[9]

II. THEMES, LESSONS LEARNED AND RECOMMENDATIONS

There are several important themes, lessons and recommendations in this Issue Paper:

- **AI, algorithms and automated decision-making are a significant new frontier in human rights, due process and access to justice.** Government use of AI and ADM is expanding rapidly across the world. AI and ADM systems are increasingly being used to make decisions affecting personal liberty, government benefits, regulatory compliance and access to important government services.
- **Governments must respond to the well-documented risks of AI and ADM systems.** Government AI and ADM systems have a track record. Experience with government AI and ADM systems across North America, Europe, Australia and New Zealand proves the risks of these systems. Questions about racial bias, "data discrimination," "black box" decision-making and public participation will surface quickly, repeatedly and urgently when AI and ADM systems are used more extensively by Canadian governments.
- **Proactive law reform is the best strategy to mitigate these risks.** The risk of AI and ADM cannot be comprehensively addressed through individual litigation, best practices, existing or piecemeal legislation. Law reform is needed to ensure AI and ADM systems meet high legal standards regarding disclosure, legal accountability, equality, procedural fairness/due process and access to remedies.
- **Proactive law reform will help Ontario and other Canadian jurisdictions maximize AI and ADM's potential benefits, while minimizing potential harm.** Proactive regulation supports AI and ADM innovation, "trustworthiness", better public services, economic development, and the fairness and legitimacy of government and justice-system decision-making.
- **At present, there is an extraordinary regulatory gap in Canada.** The federal Directive is a significant initiative to regulate AI and ADM in Canada. Unfortunately, there is no equivalent regulatory framework in Ontario or any other Canadian province. As a result, some of the most consequential potential uses of AI and ADM by provinces, municipalities, police services, child welfare agencies and/or many other important public institutions are under- or unregulated.
- **The best approach to AI and ADM regulation is to adopt a mixture of "hard" and "soft" law instruments, tailoring each to their appropriate purpose and context.** Comprehensive regulation of AI and ADM systems can be achieved through what is sometimes called a "smart mix" or "mixed model." This model assumes that no one single statute, rule or practice will be sufficient to govern AI and ADM systems. AI and ADM regulation should also be a shared responsibility between government departments and agencies.
- **Legislation and regulations are needed; ethical AI guidelines are not sufficient.** Ethical AI guidelines are insufficient to mitigate the harms caused by the use of AI and ADM systems due to their lack of specificity and reliance on voluntary compliance. Ethical guidelines, directives, "playbooks" or best practices and other "soft law" instruments have significant potential to supplement mandatory legal obligations and requirements.

- **The key elements of a comprehensive regulatory regime can be identified.** A comprehensive regime should include:
    - Baseline requirements for all government AI and ADM systems, irrespective of risk.
    - Strong protections for AI and ADM transparency, including disclosure of both the existence of a system and a broad range of data, tools and processes used by a system.
    - Mandatory "AI Registers."
    - Mandatory, detailed and transparent AI or algorithmic impact assessments.
    - Explicit compliance with the *Charter* and appropriate human rights legislation.
    - Data standards.
    - Access to meaningful remedies.
    - Mandatory auditing and evaluation requirements.
    - Independent oversight of both individual systems and government use of AI and ADM generally.

- **There must be broad participation in the design, development and deployment of these systems.** Unequal access to information and participation in AI and algorithmic decision-making can significantly worsen existing biases and inequality. Broad participation must include technologists, policy makers, legal professionals, and, crucially, the communities who are likely to be most affected by this technology.

The LCO's forthcoming third Issue Paper, *AI, ADM and Government Decision-Making,* will address many of these issues in greater detail. For example, the paper will continue the LCO's analysis of key issues such as disclosure, transparency, explainability, discrimination and accuracy. The paper will analyze these issues through the lens of existing laws in Ontario.

III. 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 law reform and public debate.

LCO reports are a practical and principled long-term resource for policymakers, stakeholders, academics and the general public. LCO's reports have led to legislative amendments and changes in policy and practice. They are also frequently cited in judicial decisions, academic articles, government reports and media stories. ·

This report is part of the LCO's ongoing ***AI, ADM and the Justice System*** project. The first phase of this project brings together policymakers, legal professionals, technologists, NGOs and community members to discuss the development, deployment, regulation and impact of AI and algorithms on access to justice, human rights, and due process. The LCO's project considers this technology in both the criminal and civil/administrative law justice systems. Completed initiatives within this project include:

- LCO/Ontario Digital Service Workshop;[10]
- *The Rise and Fall of Algorithms in the American Justice System: Lessons for Canada*;[11]
- LCO Forum on AI and ADM in the Civil and Administrative Justice System;[12]
- LCO Forum on AI in Ontario's Criminal Justice System (with The Citizen Lab, Criminal Lawyers Association and the International Human Rights Program, Faculty of Law, University of Toronto);[13]
- ***AI, Automated Decision-Making: Impact on Access to Justice and Legal Aid***;
- ***AI for Lawyers: A Primer on Artificial Intelligence in Ontario's Justice System*** with Element AI and Osgoode Hall Law School; and,
- ***Roundtable on Digital Rights and Digital Society*** with the Mozilla Foundation.

The LCO is also undertaking projects respecting protection orders, the ***Last Stages of Life***, the ***Indigenous Last Stages of Life***, and ***environmental accountability***.

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

IV. WHY SHOULD GOVERNMENTS REGULATE AI AND AUTOMATED DECISION-MAKING?

There are many reasons why governments should regulate AI and ADM. The LCO discusses these reasons extensively in our Criminal AI Issue Paper[14] and our forthcoming Issue Paper addressing AI and ADM in the civil and administrative justice systems.[15] For introductory purposes, the need for government regulation of AI and ADM can be summarized as follows:

AI and ADM technologies have great potential to improve the accuracy, fairness, transparency and efficiency of government decision-making. Unfortunately, experience demonstrates that AI and ADM systems also raise significant, novel and systemic legal risks that have not – and cannot – be comprehensively addressed through individual litigation, best practices, existing or piecemeal legislation. For example:

- Many AI and ADM systems are credibly described as being racist, sexist, ageist or discriminatory on other grounds. Regulation is needed to ensure these systems comply with anti-discrimination laws and are transparent about data issues.
- "Black box" AI and ADM systems often embed, and obscure, important legal and policy choices that have far-reaching consequences for human rights and fairness in government decision-making. Regulation is needed to ensure these choices and systems are transparent, explainable and accountable.
- AI and ADM systems are increasingly being used to make decisions affecting government benefits, regulatory compliance and access to important government services. Regulation is needed to ensure these systems comply with administrative law requirements regarding procedural fairness, notice, transparency, explainability and remedies.

- AI and ADM tools are increasingly being used in the criminal justice system to assist policing and support judicial decision-making in bail and sentencing. Regulation is needed to ensure these operations and proceedings meet high legal standards regarding disclosure, legal accountability, equality and due process.

Regulation in these areas will help ensure these systems comply with appropriate legal standards. Regulation is also needed to establish explicit and consistent legal benchmarks if and when these systems are litigated. The lack of government regulation in these areas risks worsening discrimination against Indigenous, racialized and other vulnerable communities.

The LCO further believes there is an urgency to developing thoughtful AI and ADM regulations:

- Government use of AI and ADM is expanding rapidly in Canada and across the world.
- Growing public anxiety (and controversies) about AI and ADM have led to public expectations about the need for "trustworthy" AI.
- The Government of Canada's Directive on Automated Decision-making is the most significant initiative to regulate AI and ADM in Canada to date. The federal Directive is a positive initiative, but its scope is limited.
- More importantly, there is no legislative or regulatory framework governing AI or ADM accountability in Ontario, other Canadian provinces, or many other important public institutions likely to develop and deploy AI and ADM systems. This is an extraordinary gap in public accountability.
- Many governments, including the Government of Ontario, have begun to consider AI and ADM regulation. There is an opportunity for governments and stakeholders to work together to address these issues in a comprehensive, collaborative and multi-disciplinary manner.
- Proactive government regulation supports innovation, "trustworthiness", better public services, economic development, and the fairness and legitimacy of government and justice-system decision-making.
- Government regulation provides guidance and support to a wide range of organizations currently considering or actively developing AI and ADM systems, including municipalities, government agencies and tribunals. Regulation will also provide important guidance to the technologists, policy professionals, legal counsel, communities and others who are engaged in these efforts.
- Absent regulatory guidance, there is a risk that governments develop or implement AI or ADM systems that deliver poor public service, harm vulnerable citizens, undermine public trust, or are struck down by courts. Proactive regulation is the best strategy to mitigate these risks.

Why Should Governments Regulate AI and ADM?

- **Government use of AI and ADM is expanding rapidly.**
- **AI and ADM systems can raise significant, novel and systemic risks to human rights, due process and access to justice, including:**
  - **Risk that AI and ADM systems are racist and discriminatory in their design or outcomes.**
  - **Risk that "black box" systems obscure legal decisions and choices.**
  - **Risk that systems violate procedural fairness, disclosure, notice, transparency, explainability and remedy requirements.**
- **Regulation is needed to ensure systems are transparent, explainable, accountable and comply with Charter, human rights and administrative law principles.**
- **Regulation supports AI innovation and development by promoting trustworthiness, fairness and legitimacy of government and justice-system decision-making.**
- **Regulation promotes better public services and provides guidance and support to many organizations and individuals currently considering or actively developing AI and ADM systems.**

V. AI AND ADM IN GOVERNMENT DECISION-MAKING

1. Why is AI and ADM Being Used by Governments?

AI and ADM systems can process data and make computations that are more robust, efficient and consistent than humans. They can work evenings, weekends and holidays, and are not adversely affected by sickness, fatigue, or emotional circumstances.[16]

Government interest in AI and ADM systems is growing.[17] The benefits of AI and ADM to aid government decision-making may include increased accuracy, fairness, transparency and efficiency in decision making.[18] According to a recent NYU/Stanford study,

> *Rapid developments in AI have the potential to reduce the cost of core governance functions, improve the quality of decisions, and unleash the power of administrative data, thereby making government performance more efficient and effective.*[19]

There is also a belief among some policymakers, technologists and academics that these tools can make government decision-making fairer and more equitable.[20] This belief is based, in part, on the view that machine-learning algorithms have superior predictive power over conventional analytic tools and subjective human decision-making.[21] Key to this view is the idea that AI and ADM tools are "harnessing the power of data to aid decision-making,"[22] As a result, the protection and promotion of human rights is often identified as an important reason why governments *should* use AI and ADM. As the Australian Human Rights Commission (AHRC) explains, "[n]ew and emerging technologies can improve human rights protections and create new opportunities for human rights promotion in diverse contexts and settings."[23]

Needless to say, not everyone shares this view. Indeed, AI, algorithms and ADM are often referred to as "weapons of math destruction"[24] or as "a sophisticated form of racial profiling."[25] For example, algorithmic risk assessment tools were initially widely supported in the American criminal justice system as an important, progressive reform to combat racist decision-making in US criminal courts. Within a few short years, however, these tools have been swiftly and widely repudiated due to serious concerns about racial bias,[26] lack of transparency,[27] data issues,[28] lack of public participation,[29] and lack of legal accountability.[30] There are many equally compelling examples in the civil and administrative context.[31]

2. How Is AI and ADM Used in Government Decision-Making?

In the US, AI and ADM tools are currently being used to assist government operations "across the full range of governance tasks", including:

- *Enforcing* regulatory mandates centered on market efficiency, workplace safety, health care, and environmental protection.
- *Adjudicating* government benefits, from disability benefits to intellectual property rights.
- *Monitoring and analyzing* risks to public health and safety.
- *Extracting* useable information from the government's massive data streams, from consumer complaints to weather patterns; and
- *Communicating* with the public about its rights and obligations as welfare beneficiaries, taxpayers, asylum seekers, and business owners.[32]

The following table sets out several examples of how AI and ADM are already being used by governments in the US, UK, Australia and New Zealand to support decision-making in a broad range of civil and administrative justice systems.[33]

Examples of AI and ADM in the Civil and Administrative Justice System

In the civil and administrative justice systems, governments are using AI and ADM to:

- **Adjudicate or prioritize government benefits;**
- **Determine or prioritize access to public services, such as housing, education, or health services;**
- **Assess risk of unemployment insurance fraud;**
- **Enforce regulatory mandates;**
- **Assess the risk of child abuse or neglect;**
- **Assess the risk of domestic violence;**
- **Predict whether students are a high risk for school-related violence;**
- **Determine or prioritize immigration eligibility or status;**
- **Recommend prison classification and conditions for inmates; and,**
- **Recommend parole eligibility or conditions.**

Transposed to the Canadian context, the applications in use internationally would affect some of Canada's most important government services and the jurisdiction and workload of many Canadian Superior Courts, provincial courts and administrative tribunals.

The use of AI, ADM and algorithms in government decision-making is growing rapidly. The Stanford/New York University study noted above canvassed the use of AI, ADM and algorithms in 142 of the most significant US federal departments and agencies. The study found that "nearly half of [American] federal agencies studied (45%) have experimented with AI and related machine learning (ML) tools."[34] According to this study,

> *…the top three policy areas were in law enforcement, health, and financial regulation. But … use cases span virtually all other substantive policy areas, such as environment, energy, social welfare, and communications. This highlights the breadth of AI use and impacts.*[35]

The growing use of AI and ADM by administrative agencies is not surprizing. Professor Jennifer Raso notes that

> *…administrative agencies are often early adopters of new technologies that promise to streamline data management and speed up routine decision-making…The front-line decisions they affect are often the main place where individuals interact with government and the legal system.*[36]

Growing use of AI, ADM and algorithms has also been found in government-use studies in the UK, Australia and New Zealand.[37]

The use of AI, ADM and algorithms to support government decision-making is potentially limitless. As the AI Now Institute notes:

> *Automated decision systems can exist in any context where government bodies or agencies evaluate people or cases, allocate scarce resources, focus scrutiny or surveillance on communities, or make nearly any sort of decision.*[38]

At this point, there are significant difficulties in assessing how widespread this technology is being used in Canada. There is not a central list or repository of AI or ADM systems in use in the justice system or other government applications. In Canada (and elsewhere), these systems are often disclosed as a result of freedom of information requests, press reports, or reviews of government procurement websites. Disclosure of AI and ADM is further complicated by the fact that these systems can be used by a variety of government actors, including federal and provincial government ministries, decision-making tribunals, municipal governments, and government agencies (such as school boards, police services, regulators, operational agencies, etc.).

The use of AI and ADM in the criminal justice system is discussed extensively in the LCO's October 2020 Issue Paper, *The Rise and Fall of AI and Algorithms in American Criminal Justice: Lessons for Canada*.[39] This paper analyzed the extraordinarily rapid expansion of AI and ADM tools the US criminal proceedings. The LCO report is one of two major studies to consider AI and ADM in the Canadian criminal justice system. The second is a recent report by The Citizen Lab, *To Surveil and Predict, A Human Rights Analysis of Algorithmic Policing in Canada*.[40] This report analyzes the use and implications of predictive policing in Canada. The Citizen Lab is also responsible for a third major Canadian report, *Bots at the Gate: A Human Rights Analysis of Automated Decision-Making in Canada's Immigration and Refugee System*.[41]

Examples of AI and ADM in the Criminal Justice System

In the criminal justice systems, governments are using AI and ADM for:

- **Photographic and video analysis, including facial recognition;**
- **DNA profiling and evidence, including probabilistic genotyping;**
- **Predictive crime mapping (predictive policing);**
- **Mobile phone and extraction tools;**
- **Data mining and social media intelligence;**
- **Bail algorithms that predict likelihood of being arrested or failure to appear;**
- **Sentencing algorithms that predict likelihood of being arrested;**
- **"Scoring at arrest" algorithms that advise how to charge an individual;**
- **"Scoring suspects" algorithms that analyze an individual's behaviour in the future;**
- **"Scoring victims" algorithms that predict likelihood of being a victim of crime; and,**
- **Correctional algorithms that predict likelihood of offending within an institution.**

VI. REGULATING AI: INTRODUCTION

Experience suggests that issues regarding racial bias, privacy, lack of transparency, "data discrimination" and public participation will surface quickly, repeatedly and urgently in Canada if and when AI and ADM systems are used by Canadian governments. Ensuring that AI and ADM regulation is responsive to these will help Ontario and other Canadian jurisdictions develop a regulatory framework that maximizes this technology's potential benefits, while minimizing potential harms.

Before addressing these issues in depth, it is important to establish the LCO's groundwork:

First, as a law reform agency dedicated to promoting law reform and access to justice, the LCO's analysis focusses on issues such as transparency, accountability, human rights, due process and public participation.

Second, notwithstanding that this paper directs recommendations to the Governments of Canada and Ontario, the LCO believes our analysis and recommendations are equally applicable to a wide range of public agencies and institutions, including school boards, police services, independent agencies, universities, hospitals, courts, tribunals and municipal governments. AI and ADM regulatory issues can – and will – arise in these contexts as well. Federal and provincial leadership in this field will help establish common rules and expectations across all these areas.

Third, the LCO is mindful of the difficulty in achieving many of recommendations in this report. "Operationalizing" new ideas is challenging in all law reform projects, but particularly so in this area. Many of these challenges are discussed in LCO's recent report, *Legal Issues and Government AI Development.*[42] This report summarizes eight major themes and practical insights from a series of innovative, multidisciplinary workshops organized by the LCO in partnership with the Government of Ontario's Ontario Digital Service.

Workshop participants noted that governments (and government staff) are often asked to implement reforms in the face of competing pressures, ambitious timelines, sprawling bureaucracies, imperfect data, existing (and sometimes antiquated) regulations, unclear legal rules and limited resources. Nevertheless, workshop participants demonstrated a wide and deep commitment to human rights, effective public services, and public participation.

The LCO's key "takeaway" from the workshops is that the challenges of regulation, while significant, are not insurmountable. Nor can they stand in the way of government's overarching obligations to ensure these systems comply with human rights, due process/procedural fairness requirements and public accountability.

Fourth, the LCO is mindful that initiatives like the federal Directive and AIA are *new*. The Directive itself effectively came into force on April 1st, 2020.[43] As a result, there is little practical or legal experience to draw upon so far. Notably, the federal government has committed to review the Directive periodically.

Finally, a word about vocabulary: The LCO will use the word "regulation" to include a wide range of legal instruments, potentially including legislation, regulations, policy guidance, practice directions, best practices and/or other "soft law" instruments. Second, the LCO will use the words "AI" and "automated decision-making" ("ADM") to encompass a broad range of technologies, even though these technologies may, in practice, raise different issues and concerns.[44]

VII. THE STARTING POINT: PUBLIC ENGAGEMENT

The LCO believes the starting point for AI/ADM regulation (and development) is robust and ongoing public participation. More specifically, the LCO believes that governments must engage with technologists, policymakers, government managers, frontline staff, lawyers, industry associations, community organizations and, crucially, the stakeholders and communities who are likely to be most affected by this technology.

The LCO emphasizes that communities (including Indigenous, racialized or otherwise marginalized communities) may be better positioned than academics, advocates or regulators to identify some of the risks and benefits of this technology. These communities have both experience and expertise that is crucial to thoughtful regulation.

The LCO believes it is essential the public be invited to provide input before, during and after the initial development and regulation of AI and ADM systems. Proactive participation is likely to promote good governance, thoughtful regulations and engender public trust in AI and ADM systems and government regulation.

A related issue is that marginalized communities may face barriers to participation. Inviting and *supporting* public participation at all stages of AI and ADM development and regulation may help ensure these valuable perspectives are incorporated throughout the process.

The LCO's first Issue Paper discussed the pitfalls of insufficient public engagement when introducing ADM systems in criminal justice.[45] The experience of the New York City Automated Decisions Task Force ("NYC Task Force") confirms this analysis.[46] The NYC Task Force report was subject to blistering criticisms from many community advocates and NGOs, including many criticisms centred on the perceived lack of community input, lack of trust and insufficient public participation.[47] Recent public controversies in Canada regarding police carding[48] and Sidewalk Labs[49] raised many of the same criticisms.

Public participation issues will come to the forefront in Ontario and across Canada when AI and ADM tools are more widely introduced here. Canadian policymakers would be well advised to take steps to address the need for meaningful public participation thoughtfully and proactively.

VIII. CRITICAL ISSUES AND CHOICES — SUMMARY

Regulating AI and ADM is a novel and daunting undertaking: Governments will need to develop rules governing complex and rapidly evolving technology across a wide range of public sector operations, all the while ensuring compliance with the *Charter*, human rights legislation, administrative law and privacy obligations, to name but a few.

This section identifies important legal or policy issues that Canadian policymakers should consider when contemplating regulatory frameworks to achieve these goals. These issues can be divided into the following themes or categories:

1. **Purpose, Definition and Scope of Regulations**
2. **Ethical AI, Hard Law, the "Mixed Model" and Risk-Based Regulation**
3. **Accountability and Transparency**
4. **Bias and Fairness**
5. **Oversight and Remedies**

This section highlights alternative regulatory approaches and illustrates the range and depth of legal questions and options raised by this technology.

As noted earlier, this review is not definitive. There may be additional issues that arise over time and in specific contexts.

Regulating AI: Critical Issues and Choices

Purpose, Definition and Scope

- Will AI and ADM regulation promote innovation, rights protection or both?
- How should AI and ADM be defined?
- Are regulations mandatory?
- What institutions or activities will be regulated?

Ethical AI, Hard Law, the Mixed Model and Risk-Based Regulation

- Commitment to comprehensive regulation?
- What form(s) will regulation take?
- Is there a statutory framework?
- Will regulation be risk-based?

Accountability and Transparency

- Commitment to comprehensive accountability and transparency?
- Mandatory AI and ADM registers?
- Mandatory AI and ADM impact assessments?
- What will be disclosed?
- What rules govern AI and ADM procurement?

Bias and Fairness

- How will regulations address bias and discrimination?
- How will regulations ensure procedural fairness and due process?

Oversight and Remedies

- Is there independent oversight of AI and ADM systems?
- Are there remedies for rights violations?
- Are independent audits and evaluations required?

IX. PURPOSE, DEFINITION AND APPLICATION OF REGULATIONS

1. Will AI Regulation Promote Innovation, Rights Protection or Both?

A fundamental issue facing governments is whether to prioritize the speed of government implementation of AI and ADM, the protection of rights and interests likely affected by AI and ADM, or to integrate the two.

A notable example of regulations that prioritize AI innovation and rapid government implementation is former US President Trump's 2019 *Executive Order on Maintaining American Leadership in Artificial Intelligence,*[50] which states

> *[i]t is the policy of the United States Government to sustain and advance the scientific, technological, and economic leadership position of the United States in AI R&D and deployment… guided by five principles…which include that the United States must drive technological breakthroughs in AI across the Federal Government, industry, and academia in order to promote scientific discovery, economic competitiveness, and national security.*[51]

Significantly, the "Memorandum for the Heads of Executive Departments and Agencies" accompanying this Executive Order states "Federal agencies must avoid regulatory or non-regulatory actions that needlessly hamper AI innovation and growth," clearly prioritizing innovation over rights protection.[52] The Executive Order even states that "agencies must avoid a precautionary approach."[53]

In contrast, the proposed *Data Accountability and Transparency Act,* introduced by Democratic Senator Sherrod Brown, focusses primarily and perhaps exclusively on rights protection.[54]

Similarly, the proposed US *Algorithmic Accountability Act*,[55] introduced in 2019 by Senators Booker, Wyden, and Clarke, has the goal of preventing hidden discrimination facilitated by AI and ADS.[56] The *Act* is aimed at regulating the activities of corporations that control huge amounts of data and might viewed as a template for similar provisions designed to apply to government entities. The *Act* would:

- Require the Federal Trade Commission to create regulations mandating that covered entities conduct data protection and automated decision impact assessments of new and existing high-risk AI systems;[57]
- Require covered entities to conduct data protection impact assessments of those systems;[58]
- Invite the participation of independent auditors and technology experts during the assessment process;[59] and
- Require covered entities to address the results of completed impact assessments.[60]

Notably, the publication of impact assessments would be voluntary.[61]

A third approach is the European Union (EU) concept of "Trustworthy AI." The European Commissions' High-Level Expert Group (HLEG) on Artificial Intelligence states that

> *A trustworthy approach is key to enabling 'responsible competitiveness', by providing the foundation upon which all those using or affected by AI systems can trust that their design, development and use are lawful, ethical and robust.*[62]

The HLEG's "Ethics Guidelines for Trustworthy AI" further specify that:

> *…trustworthy AI has three components, which should be met throughout the system's entire life cycle: (1) it should be **lawful**, complying with all applicable laws and regulations (2) it should be **ethical**, ensuring adherence to ethical principles and values and (3) it should be **robust**, both from a technical and social perspective since, even with good*

> *intentions, AI systems can cause unintentional harm. Each component in itself is necessary but not sufficient for the achievement of Trustworthy AI. Ideally, all three components work in harmony and overlap in their operation. If, in practice, tensions arise between these components, society should endeavour to align them (Emphasis in original).*[63]

The Government of Canada's federal Directive is similar. The federal Directive explicitly aligns innovation with public trust and rights protection, rather than conceptualizing them in conflict with one another. The federal government's description of the Directive states:

> *The Government of Canada is increasingly looking to utilize artificial intelligence to make, or assist in making, administrative decisions to improve service delivery. The Government is committed to doing so in a manner that is compatible with core administrative law principles such as transparency, accountability, legality, and procedural fairness. Understanding that this technology is changing rapidly, this Directive will continue to evolve to ensure that it remains relevant.*[64]

The LCO believes that any Canadian government considering AI and ADM regulation should adopt this approach. It is important for regulation to explicitly align innovation, public trust and rights protection.

2. Defining AI and ADM Systems

Governments will have to decide how to define AI or ADM systems for regulatory purposes. A further, related issue is how to define "decision-making."

AI and ADM systems are incredibly diverse and malleable. As a result, it has proven extraordinarily difficult to define these systems for the purpose of regulation. The New York City Automated Decisions Task Force is a particularly vivid example.[65] Task Force members could not agree on either a specific definition or whether, in principle, AI and ADM systems should be defined broadly or narrowly.[66] Some Task Force members worried that certain definitions could be interpreted to potentially include " tools as general as internet searches or spreadsheets."[67] Members also debated whether ADM or algorithmic tools already in use in New York City, such as actuarial risk assessments, should be included in definitions of AI or ADM.

The following table includes samples of alternative definitions that have been adopted or proposed in various instruments:

Examples of Definitions of AI and Automated Decision-making

Canada, Directive on Automated Decision-Making, (2019)

> ***"…any technology that either assists or replaces the judgement of human decision-makers. These systems draw from fields like statistics, linguistics, and computer science, and use techniques such as rules-based systems, regression, predictive analytics, machine learning, deep learning, and neural nets."***

US, Future of Artificial Intelligence Act of 2017

(A) "Any artificial systems that perform tasks under varying and unpredictable circumstances, without significant human oversight, or that can learn from their

Continued on next page

Examples of Definitions of AI and Automated Decision-making

experience and improve their performance. Such systems may be developed in computer software, physical hardware, or other contexts not yet contemplated. They may solve tasks requiring human-like perception, cognition, planning, learning, communication, or physical action. In general, the more human-like the system within the context of its tasks, the more it can be said to use [AI].

(B) Systems that think like humans, such as cognitive architectures and neural networks.

(C) Systems that act like humans, such as systems that can pass the Turing test or other comparable test via natural language processing, knowledge representation, automated reasoning, and learning.

(D) A set of techniques, including machine learning, that seek to approximate some cognitive task.

(E) Systems that act rationally, such as intelligent software agents and embodied robots that achieve goals via perception, planning, reasoning, learning, communicating, decision making, and acting.

US, Algorithmic Accountability Act of 2019

"…a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision or facilitates human decision making, that impacts consumers";

US, Bill HR 2202, Growing Artificial Intelligence Through Research Act (2019-2020)

"…intelligent machines that use algorithms, computer programs, and other techniques to behave in ways commonly thought to require intelligence [and includes] forms such as machine learning, computer vision, and natural language processing."

Many definitions are even more complex than these excerpts suggest. For example, the European Commission's HLEG recently published "A Definition of AI: Main Capabilities and Scientific Disciplines" takes *six pages* to define AI.[68]

Finally, some jurisdictions and proposals do not include a definition of AI at all.[69]

This situation has led some regulators, including the NYC Task Force, to propose "frameworks" for identifying and categorizing systems according to their characteristics, rather than a specific definition.[70]

A related issue is the definition of "decision." The scope of the federal Directive is specifically limited to "any system, tool or statistical models used to recommend or make an administrative decision about a client."[71] Representatives from the federal Government have stressed the importance – and difficulty – of determining what constitutes a "decision." A key issue is the threshold at which a system is said to aid or support the human decision-maker. Federal representatives have provided the LCO with the following table to help developers, operational staff and policymakers address these issues. The list of questions in the table are intended to help determine whether an AI or ADM system plays a significant role in administrative decision-making or, rather, if the system is simply an IT tool that digitizes the workflow of decision-makers.

Recommendations and Decisions

Recommendations

- present relevant information to the decision-maker,
- alert the decision-maker of unusual conditions,
- present information from other sources ("data matching")
- provide assessments, for example by generating scores, predictions or classifications,
- recommend one or multiple options to the decision-maker,
- make partial or ntermediate decisions as part of a decision-making process, or
- make the final decision.

Decisions

A close look at the table illustrates the challenge and importance of definitions.

AI or algorithmic systems that "recommend one or more multiple options to the decision-maker", "make partial or intermediate decisions…", or "make the final decision" would appear to fall into a common-sense definition of a "decision" for regulatory purposes. Conversely, systems that "present relevant information," "alert the decision-maker of unusual conditions" could appear, without more, to be more in the nature of policy "recommendations" rather than decisions.

The remaining categories ("present information from other sources" and "provide assessments… scores, predictions, or classifications") may sound innocuous, but are not. Some of the most controversial and consequential systems in use today are data matching or predictive "scoring" tools, including fraud detection systems (System Risk Indication (SyRI)), predictive policing systems (PredPol), pretrial risk assessments (Public Safety Assessment (PSA),COMPASS)), or child protection risk assessment tools (Allegheny County Family Screening Tool).[72] These and equivalent systems must be included in any regulatory definition.

In sum, LCO believes it is important to include an expansive definition (or definitions) of AI and/or ADM in governing regulations. Explicit definitions are key to establishing which systems (or types of systems) are subject to regulation. Simply stated, explicit and expansive definitions are key to public and legal accountability.

The LCO does not underestimate the difficulty of this task. The LCO notes, however, definitional challenges are common in legal policymaking, especially in areas of rapid technological development. The purported risks of adopting a fixed definition of AI or ADM for regulatory purposes (including the risk of overbreadth or the risk that a definition "lags" technological developments) are real, but not insurmountable.

Finally, Professor Teresa Scassa reminds us why we cannot forget the impact of systems that are *outside* of formal definitions:

> *[The federal Directive] focusses on decision-making…[It] is important to retain sight of the fact that there may be many more choices/actions that do not formally qualify as decisions and that can have impacts on the lives of individuals or communities. These fall outside the [Directive] and remain without specific governance."* [73]

3. Scope, Exemptions, Prohibitions and Jurisdictional Gaps

In addition to the definitional questions discussed above, governments will have to decide important issues about the scope and application of AI and ADM regulations. Important questions to be determined include:

- Is AI and ADM regulation mandatory or permissive?
- Do AI regulations apply to all government agencies/sectors or are exceptions provided and under what circumstances?
- What government activities do regulations apply to? Does regulation differ depending on the use of the technology?
- Will regulations prohibit government use of high-risk AI and ADM technologies (such facial recognition) or in certain areas of government activity (such as criminal profiling)?

Needless to say, these choices will have significant influence on the scope, effectiveness and the perceived fairness of AI and ADM use by government.

Scope of Regulation

The US *Algorithmic Accountability Act* employs both mandatory and permissive language. While the purpose of the Bill is to "direct the Federal Trade Commission to require entities that use, store, or share personal information to conduct automated decision system impact assessments and data protection impact assessments,"[74] those assessments must be conducted only "if reasonably possible, in consultation with external third parties, including independent auditors and independent technology experts."[75] Further, the publication of those assessments is merely permissible.

The federal Directive also employs both mandatory and permissive language: Most federal departments and agencies must comply with the Directive. Further, the scope of the federal Directive includes "any system, or statistical models used to recommend or make an administrative decision about a client."[76] These provisions give the Directive potentially very broad application. Nevertheless, the Directive's scope and application is subject to a number of important exceptions and limitations:

- The federal Directive does not apply to systems that support government non-administrative decisions and/or decisions that are not "about a client." These exclusions could have significant consequences. The Directive appears to exclude systems that support policy decisions, for example.
- The Directive's focus on "administrative decisions" suggests that the Directive may not apply to ADM systems that could be deployed in the criminal justice system or criminal proceedings. As a result, it appears the federal government could adopt predictive policing algorithms, facial recognition technology, and/or automated risk assessments in bail and sentencing proceedings without having to comply with the Directive.[77]
- National security applications are explicitly exempt from the Directive,[78] as are the the Offices of the Auditor General, the Chief Electoral Officer, the Information Commissioner of Canada and the Privacy Commissioner of Canada and others.[79]
- Several agencies, crown corporations, and Agents of Parliament outside the core federal public service may enter into agreements with the Treasury Board to adopt the Directive's requirements, but are not required to do so.[80]
- The Directive is limited to ADM systems that "provide external services."[81]
- The Directive "only applies to systems in production" at the time the Directive came into effect.[82]

In the long term, these exemptions and limitations could be very significant. For example, the criminal justice tools identified above are among the most controversial AI and ADM applications with potentially the most significant impact on human rights.

The LCO believes that future iteration(s) of the Directive, or any provincial equivalent, must be much broader in scope. In this regard, it is important to recall that governments around the world are currently using AI and ADM to:

- Adjudicate or prioritize government benefits.
- Determine or prioritize access to public services, such as housing education, or health.
- Assess the risk of unemployment insurance fraud.
- Assess the risk of child abuse or neglect.
- Assess the risk of domestic violence.
- Predict whether students are a high risk for school-related violence.
- Determine or prioritize immigration eligibility or status.
- Make hiring decisions/evaluate employee performance.
- Recommend prison classification and conditions for inmates.
- Conduct mass surveillance and photographic/video analysis, including facial recognition.
- Support DNA profiling and evidence, including probabilistic genotyping.
- Support predictive crime mapping (predictive policing).
- Support bail decision-making.
- Support sentencing decision-making.

This is a seemingly broad and unrelated list of government activities and applications. These systems are connected, however, in at least two important respects: First, each of these are "high impact" systems with the potential to decide or influence important individual rights. Second, as noted earlier, many of these systems have well-documented risks for relying on inaccurate, unreliable or racialized data; for being opaque; or for targeting poor, racialized or vulnerable communities. Future regulations should be written to account for all of these systems.

Prohibitions

Governments will have to consider whether there are certain AI or ADM technologies that should be prohibited outright. These areas are sometimes referred to as "red lines."[83] For example, new methods of mass profiling and surveillance – including facial recognition, biometric identification, predictive policing, social network behavioural analysis, and "smart cities" – have been cited as "red line" AI and ADM technologies. Some of these technologies are already being used in Canada. For example, the use of facial recognition software has already been confirmed in police services including Toronto, Calgary, Edmonton, Ottawa, and five additional regional police forces in Ontario covering the majority of the provincial population.[84]

Leading legal public interest groups – including the The Citizen Lab and the Canadian Civil Liberties Association[85] – warn that such technologies, left unregulated, may trigger a fundamental shift in Canadian civil and political rights in the private and public realms alike:

> *Study after study has demonstrated that facial recognition technology is most accurate on white male faces, and gets worse for women, youth, and people of colour, particularly Black individuals. Indeed, many companies who make this technology, including IBM, Microsoft, and Amazon, have voluntarily chosen to stop selling it because they recognize it may do terrible social harm.*

> *Yet in Canada, facial recognition technology has been deployed by police forces without notice, meaningful consultation, or public oversight and accountability.*[86]

Some governments have already enacted or proposed bans on the use of specific AI or ADM systems, particularly facial recognition technology. Examples include:

- The San Francisco Board of Supervisors of San Francisco banned city agencies' use of facial recognition technology;[87]
- A similar, unanimously-passed ban by the Boston City Council;[88]
- A proposed ban on facial recognition and other biometric surveillance by California law enforcement;[89] and,
- A proposed ban on facial recognition technology by US federal law enforcement.[90]

Jurisdictional Gaps

AI and ADM systems are likely to be used by governments and public institutions far beyond the reach of the federal Directive, including provincial governments, municipalities, school boards, child welfare agencies, police services, universities, hospitals, courts, tribunals, and many others. This means that the most consequential and controversial AI and ADM applications in use today could be deployed by literally hundreds (if not thousands) of public institutions across Canada without any dedicated regulatory framework.

This is an alarming jurisdictional gap in AI and ADM regulation in Canada. The principles of AI and ADM transparency, accountability, human rights, fairness and "trustworthiness" are important in all high-impact applications and in all public institutions.

The LCO recommends that governments and stakeholders begin addressing these gaps urgently. Provincial governments (including the Government of Ontario), municipalities and other important public institutions need to begin developing their own policies, rules, regulations and statutes governing AI and ADM systems.

Fortunately, the federal Directive is a good framework to begin these discussions. Canadian governments and institutions have a unique opportunity to work together to develop a shared (or at least consistent) regulatory framework across the country. The benefits of this approach include regulatory harmonization, consistent rights protection, and more efficient and effective policy development.

X. ETHICAL AI, HARD LAW, THE MIXED MODEL AND RISK-BASED REGULATION

1. Form(s) of Regulation: Ethical AI vs. "Hard" Law

Governments will need to determine what form or forms AI regulation will take. Options include statutes, regulations, regulatory "sandboxes", "principle-based regulations", best practices, ethical frameworks, procurement standards or a combination of approaches. As will be seen, the arguments in favour and against various approaches are well-known to legal policy-makers.

Early efforts to "regulate" AI were typically in the form of "ethical AI" guidelines or best practices developed by a range of governments, NGOs or industry associations. Indeed, the growth of "ethical AI" models has been astounding. Access Now has described the "boom" in AI ethics guidelines, particularly since 2016.[91] AlgorithmWatch, a German NGO, maintains a searchable "AI Ethics Guidelines

Global Inventory" that has identified more than 160 "frameworks and guidelines that seek to set out principles of how systems for automated decision-making (ADM) can be developed and implemented ethically." This inventory lists a range of instruments, guidelines, directives and binding instruments as of April 2020, including at least six from Canada.[92]

Ethical AI guidelines and frameworks vary considerably in scope and detail. Some examples stand out, however, for their sophistication and apparent commitment to human rights, transparency and AI accountability. A particularly high-profile guideline/ethical framework is the "Ethics Guidelines for Trustworthy AI", recently published by the European Commission's High-Level Expert Group (HLEG) on Artificial Intelligence.[93] The HLEG Guidelines strive to promote "Trustworthy AI", with trustworthiness in an AI system being defined as:

1. Lawful - respecting all applicable laws and regulations
2. Ethical - respecting ethical principles and values
3. Robust - both from a technical perspective while taking into account its social environment

The HLEG Guidelines set out detail on what it means for an AI system to respect ethical principles and values by outlining seven "key requirements that AI systems should meet in order to be deemed trustworthy," including:

1. Human agency and oversight.
2. Technical robustness and safety.
3. Privacy and data governance.
4. Transparency.
5. Diversity, non-discrimination, and fairness.
6. Societal and environmental well-being; and,
7. Accountability.[94]

The Guidelines are accompanied by a detailed "Assessment List" to be used by organizations, including governments, to help organisations identify how proposed AI systems might generate and mitigate risks.[95]

Importantly, the HLEG Guidelines do not purport to be, or aspire to become, binding legal standards. They are rather, explicitly identified as a tool for "self-assessment…intended for flexible use: organizations can draw on elements [from the Assessment List]...as they see fit."[96]

The EU process is not the only significant European AI governance framework. The Council of Europe has been making ongoing efforts to establish international legal measures to mitigate the risks AI systems could pose to democracy, human rights, and the rule of law. The Council's Ad-hoc Committee on AI (CAHAI) recently adopted a feasibility study that lays out potential elements of an international legal framework.[97] While Canada is only an observer at the Council of Europe, the instrument resulting from this process is expected to exert a global influence on the laws and norms governing AI and ADM.

Many governments and industry organizations tend to recommend the creation of "global voluntary, industry-led, consensus-based standards and best practices."[98] These groups often encourage regulators to "use caution before adopting new laws, regulations, or taxes that may inadvertently or unnecessarily impede the responsible development and use of AI."[99]

There appear to be several reasons for preferring "ethical AI" approaches, including:

- A belief that detailed regulations may discourage investment and innovation.
- A belief that the technology is evolving so rapidly that detailed regulations may prove ineffectual or counter-productive.
- A belief that that it is too soon to codify AI-specific regulation.

- A desire to avoid regulation; and/or,
- A preference for deregulation, self-regulation or market-driven governance.

The "Ethical AI" approach has been subject to many deep and significant criticisms. These critiques emphasize that ethical guidelines are insufficient to mitigate the harms caused by the AI systems due to their lack of specificity and reliance on voluntary compliance. For example, an ethical guideline may say that AI systems should be lawful, but not specify which laws and regulations should apply. Critics also argue that ethical guidelines are unlikely to have real legal force: If a government violates an ethical guideline, there is typically no enforcement mechanism to ensure compliance or a remedy. More pointedly, many critics believe that AI ethics may "become a smokescreen for an unregulated technical environment."[100] As a result, governments and other organizations that adopt ethical guidelines – without more – are often criticized as "ethics washing."[101]

An alternative approach is found in Washington State legislation. Washington State House Bill 1655 (and its companion Washington Senate Bill 5527) includes detailed, mandatory and statutory requirements governing the use of ADM systems by the Washington State government and public agencies.[102] These requirements include provisions:

- Prohibiting Washington State public agencies from developing, procuring or using ADM systems that "discriminate against an individual, or treats an individual less favourably than another…";
- Requiring detailed algorithmic accountability reports;
- Giving notice to individuals of the use of ADM systems;
- Setting data requirements and management policies, including disclosure of data;
- Establishing explainability requirements and remedy/appeal mechanisms; and,
- Establishing external review and approval of systems by the Washington State Chief Privacy Officer.[103]

The Washington State proposal will be discussed further in later sections of this report.

The federal Directive falls somewhere between these two examples. The federal Directive is clearly not a voluntary, self-assessing "ethical AI" guideline or best practise. At the same time, a federal Directive does not have the legal status of a statute or a regulation. As Professor Teresa Scassa notes in her paper analyzing the Directive,

> *While directives are important policy documents within the federal government, and while there are accountability frameworks to ensure compliance, the requirements to comply with directives are internal to government, as are the sanctions. Directives do not create actionable rights for individuals or organizations.*[104]

2. The "Mixed Model"

The LCO believes that the choice between "ethics," directives, "playbooks" and "hard law" is too simplistic. The LCO has concluded that the best approach to AI and ADM regulation is to adopt a mixture of "hard" and "soft" law instruments, tailoring each to their appropriate purpose and context. This view is consistent with the LCO's belief that comprehensive government regulation of AI and ADM systems can be achieved through what is sometimes called a "smart mix" or "mixed model."[105]

The American experience with algorithmic risk assessments, documented in the LCO's first Issue Paper, refutes the argument that "ethical guidelines" or best practices are a sufficient substitute for comprehensive legal regulation. That example, and many others, demonstrate that the legal issues and rights at stake when AI or ADM is used by governments are simply too significant to rely on vague, opaque and/or unenforceable guidelines. Even the most sophisticated and well-intentioned ethical guidelines, such as the HLEG Guidelines, are insufficient. Similarly, the federal Directive, while a significant improvement on voluntary or self-assessing ethical guidelines, lacks the legal status necessary to ensure public and legal accountability.

In the LCO's view, legislation is clearly needed to provide the foundational governance framework for these systems. In this respect, the Washington State model is much preferable to an ethical AI or directive model. A legislative framework would provide consistent direction and accountability requirements to all actors, departments and/or agencies within its scope. It would also ensure changes to the governance framework were subject to legislative review. Finally, legislation would establish a level of public and legal accountability commensurate with the issues and rights at stake.

That said, the LCO does not discount the use or importance of ethical guidelines, directives, "playbooks" or best practices. Indeed, the LCO believes these instruments have significant potential to supplement or expand mandatory legal obligations and requirements. For example, the federal Government's new Directive on Service and Digital establishes important requirements for federal enterprise systems that will influence federal AI and ADM development.[106]

Internationally, there have been many important initiatives to develop AI or ADM-specific "soft" legal instruments. Notable examples include the UK Office of Artificial Intelligence's "Guidelines for AI Procurement," which establishes detailed and important rules for AI procurement,[107] and the standards developed by the Institute of Electrical and Electronics Engineers (IEEE).[108]

The LCO wants to highlight one type of standard or best practice that should be given high priority: best practices or standards to prevent data discrimination. Simply stated, data issues and choices are foundational to the success and legitimacy of any AI or ADM tool used by any governments, agencies, courts or tribunals.[109] As a result, best practices and/or standards for identifying, mitigating or eliminating data discrimination should be prioritized.[110]

The LCO emphasizes that no one single statute, rule or practice will be sufficient to appropriately govern AI and ADM systems. Nor should AI and ADM regulation be the responsibility of any one government department or agency. Compliance with legislative standards must be a shared responsibility or mandate across government. The federal Directive is structured in this manner. The federal Treasury Board is responsible for the Directive, while other government departments are responsible for ensuring their systems comply with the Directive.

The LCO's *Criminal AI Issue Paper* outlined the potential elements of a "cascading" strategy to regulate the use of AI and ADM tools in criminal justice.[111] In the criminal context, the LCO suggested a comprehensive regulatory regime would likely include both federal and provincial initiatives (to account for each government's jurisdiction in criminal justice) and would include both "horizontal" instruments (addressing systemic AI and ADM governance issues) and "vertical" instruments (addressing AI and ADM tools used specifically in criminal proceedings).[112]

The chart on the next page is a very preliminary outline of a potential framework of a comprehensive regime to regulate government use of AI and ADM. The LCO is presenting this chart for discussion purposes only. Each jurisdiction and subject area will have unique issues, stakeholders and concerns that cannot be captured in a general review. Moreover, there are undoubtedly many issues that are not identified. Further, identifying the *types* of legal reforms needed is one task; identifying the *content* of those reforms is quite another.

Potential "Cascading" Framework for a Comprehensive Regime Regulating Government Use of AI and ADM

- General legislation or regulations governing the development, disclosure and use of AI and ADM by governments and government agencies, including provisions addressing:
  - Definition and scope of AI and ADM systems
  - Disclosure of government AI and ADM systems
  - Impact assessments
  - Non-discrimination
  - Due process/procedural fairness
  - Remedies
  - Privacy and data protection
  - Audits and evaluation
- Dedicated instruments establishing rules for use for AI and ADM in specific areas or proceedings, including
  - Regulations, directives, "playbooks" or practice directions establishing how AI or ADM tools can and should be used by specific ministries, agencies, courts or tribunals.
  - Dedicated statutes, regulations or rules of practice to ensure procedural and evidential safeguards in legal proceedings.
- Standards, directives or best practices addressing key AI and ADM accountability issues, including:
  - Public participation
  - Procurement
  - Data collection and standards
  - Auditing and evaluation standards

3. Risk-Based Regulation

Many regulatory models used risk-based approaches to determine whether, and to what degree, an AI or ADM system should be regulated. For example, in February 2020, the European Commission published a "White Paper on Artificial Intelligence: a European Approach to Excellence and Trust."[113] The White Paper presented a new regulatory framework to address specific concerns about AI, embracing a risk-based approach focusing on high-risk applications. The White Paper proposed adding legal regulation only if an AI system was determined to be "high risk," based on two criteria:

- Whether "the AI application is employed in a sector where, given the characteristics of the activities typically undertaken, significant risks can be expected to occur"; and,
- Whether "the AI application in the sector in question is, in addition, used in such a manner that significant risks are likely to arise."[114]

For applications not classified as high-risk, the White Paper proposes a voluntary labelling scheme.

This approach was heavily criticized, particularly from a human rights perspective. The European Data Protection Supervisor, for example, argued that the White Paper's proposed risk-based approach is "too narrow, as it would seem to exclude individuals from being adequately protected from AI applications that could infringe on their fundamental rights".[115] Similarly, Access Now argued that the model reverses priorities: "the primary objective of a regulation on AI should be protect and promote fundamental rights…to avoid individual and societal harms, not to promote AI uptake and then to try and mitigate any harms caused."[116] Critics also focussed on the potentially wide interpretation of "low" risk, who gets to determine risk levels, if or how "low" risk applications will be human rights-protected, and how to protect human rights in the grey area between binary high/low categorisations.[117]

By way of contrast, Washington State House Bill 1655 would establish detailed requirements for *all* ADM systems in that state, irrespective of the level of risk. Washington State House Bill 1655 states that Washington State's Chief Privacy Office "shall" adopt rules regarding the development, procurement and use of ADM systems by public agencies and these rules "must incorporate the minimum standards and procedures" set out in the legislation.[118] (As will be seen below, these "minimum standards" are very comprehensive.)

The federal Directive represents a different model again. It is risk-based, but the risk levels are more sophisticated and nuanced. Rather than having two levels of risk (high/low), the federal Directive establishes four levels, judged by a system's impact. The Directive then establishes requirements for each impact level, including greater or lesser levels of

- Notice before ADM decisions and explanations after ADM decisions;
- Peer review;
- Employee training; and,
- Human intervention.[119]

In this manner, the federal Directive effectively establishes a sliding-scale of requirements and due diligence depending on the level of risk identified. The federal government has created an innovative and sophisticated Algorithmic Impact Assessment (AIA) tool to help federal officials assess and determine the impact of a system.[120] The Assistant Deputy Minister responsible for the program using an ADM system is responsible for completing the AIA prior to production of any ADM system and for applying the requirements appropriate to the level of risk determined by the AIA.[121]

Importantly, this model is grounded in basic principles of Canadian administrative law and practise. Canadian scholars are beginning to analyze the administrative law implications of the federal Directive, including thoughtful articles by Professor Scassa,[122] discussed above, and Professor Jennifer Raso.[123]

Significantly, the Directive establishes baseline requirements that apply to all ADM systems, regardless of their impact level,[124] including:

- Access, diligence, testing and auditability requirements for licensed software.
- Release of custom source code that is owned by the Government of Canada.
- Quality assurance and monitoring requirements, including:
  - Testing "before launching into production…[to ensure ADM systems] are "tested for unintended data biases and other factors that may unfairly impact outcomes."[125]

  - – Monitoring "outcomes of ADM Systems to safeguard against unintentional outcomes and verify compliance with institutional and program legislation."[126]

- Validating the quality of data collected and used.
- Consultations with government legal services to ensure the use of the ADM complies with applicable laws.
- Providing individuals with "recourse options that are available to challenge the administrative decision."[127]
- Reporting information on effectiveness and efficiency.

In principle, the LCO agrees with risk-based regulation. Risk-based regulation is both a practical response to the wide variety of AI and ADM systems and responsive to the principles and requirements of administrative law. This view is subject to three qualifications and comments:

> First, it is crucial that governments are publicly accountable for their decisions about the potential impact or risk of an AI or ADM system. As a result, it is crucial that a government's risk assessment determination be transparent. This is to guard against the possibility that governments understate (through intention or inadvertence) the level of risk of an AI or ADM system, and thus avoid the appropriate level of regulation and governance.
>
> Second, the LCO rejects binary high/low classifications. The nuanced risk assessment levels in the federal Directive and the accompanying AIA are clearly preferable to the EU White Paper's binary and extremely vague criteria. Experience will determine whether the federal Directive's four risks levels and the AIA represent an appropriate range or hierarchy of risk. Over time, the levels and AIA may be adjusted. The LCO emphasizes, however, that the federal government must be publicly accountable for any adjustments to the levels or risk assessment criteria.
>
> Finally, the LCO strongly supports the federal Directive's model of establishing baseline requirements for all AI and ADM systems, irrespective of the level of risk. At present, the baseline requirements set out in the Directive include a broad range of technical principles ("validating the quality of data collected and used"), best practices ("consultations with government legal services…"), and quasi-legal requirements ("recourse options that are available to challenge the administrative decision.").

The federal government is to be commended for mandating these requirements in its ADM systems, particularly in the first iteration of the Directive. Nevertheless, as will be seen below, the LCO believes the Directive and/or equivalent instruments at other levels of government could be improved by providing more clarity in key areas.

XI. ACCOUNTABILITY AND TRANSPARENCY

Many commentators have emphasized that the most important legal issues at this stage of AI and ADM development are the principles of accountability and transparency.[128]

Many of the ideas regarding how to ensure AI and algorithms are legally accountable are organized within a broad range of issues sometimes called "algorithmic transparency." Algorithmic transparency is intended to remedy, or at least mitigate, concerns about the opacity of algorithmic systems and decision-making. As noted by Deven Desai and Joshua Kroll,

> *Transparency has been proposed as a solution to mitigating possible undesired outcomes from automated decision-making… A related fear is that the human designer of a program could have bad intent and seek to discriminate, suppress speech, or engage in some other prohibited act. Transparency in this context is the claim that someone "ought to be able to 'look under the hood' of highly advanced technologies like... algorithms" as a way to police such behavior.*[129]

The Government of Ontario's Data Catalogue website provides a good explanation of why it is important to publicly disclose algorithms and AI systems*:*

> *We all follow steps to make decisions. In government, these steps are sometimes formalized into an algorithm, tool (like a calculator) or system. The outputs of these algorithms, tools or systems can inform a decision made by a human or make a decision on behalf of a human. This shift away from fully human made decisions allows greater opportunity for efficiencies and equality, but also risks augmenting existing inequalities. Transparency of use allows all of us to be aware of when, how and why decisions are automated, so we can all discuss the merits or appropriateness of use, availability of recourse options and necessary improvements to these tools, systems or algorithms to ensure they are benefiting everyone without causing harm.*
>
> *Artificial Intelligence or AI, is a class of technology that can solve problems by being able to learn and develop solutions without human intervention. Automated Decision-making Systems (ADS) are a type of AI. By including algorithms, including those that support automated decision-making, the government of Ontario is providing public notice of the use of AI / ADS by the government.*
>
> *Public notice is key to people's ability to inform, question and hold accountable the unseen AI used to make government services simpler, faster, better. Starting with transparent use we are working towards a governance framework for AI in Ontario that is responsive, adaptive and fair.*[130]

Methods and strategies for achieving algorithmic transparency typically include 1) disclosure, 2) impact assessments and 3) procurement rules.

1. Disclosure

It is widely acknowledged that some form of disclosure should be a feature of AI and ADM regulatory models, guidelines or best practices. Disclosure is a complex topic, but is typically framed around questions of *how* to disclose government AI and ADM systems and *what* information should be disclosed about those systems.

As a first step, the LCO strongly recommends the adoption of what are sometimes called "AI Registers." These are websites that identify and document AI and ADM systems used by governments. The purpose of AI Registers is to centralize disclosure of AI and ADM systems, promote public and legal accountability, and to be a resource for developers, stakeholders, researchers and the general public.

The best-known AI Register to date is the model jointly developed by the cities of Amsterdam and Helsinki.[131] According to the Helsinki website,

> *AI Register is a window into the artificial intelligence systems used by the City of Helsinki. Through the register, you can get acquainted with the quick overviews of the city's artificial*

> *intelligence systems or examine their more detailed information based on your own interests. You can also give feedback and thus participate in building human-centred AI in Helsinki.*[132]

A less well-known but more important AI Register is the Government of Ontario's public catalogue for "algorithms, tools and systems powered by data across the Ontario Public Service."[133] As of March 2021, the Ontario's data catalogue included descriptions of eight "tools," including the COVID Self-Assessment Tool, the COVID-19 Courthouse Screening Tool and several tools used by the Ministry of Agriculture, Food and Rural Affairs.

Ontario's data catalogue provides an easy-to-read summary of key elements of these tools. For example, the data catalogue summary for the COVID-19 Courthouse Screening Tool includes the following information:

Government of Ontario Disclosure for COVID-19 Courthouse Screening Tool

This screening is only meant for entering Ontario courthouses and cannot diagnose you. If you have medical questions, consult a health care provider or your local public health unit.

Purpose

The COVID-19 Courthouse Screening Tool provides a user-friendly interface with a decision tree. People can answer the questions to determine whether it is safe for them to enter a courthouse in Ontario, and what to do next. They can do it themselves or on behalf of others. It provides users with an easy-to-display result on their mobile device, indicating if they should or should not enter a courthouse due to possible COVID-19 exposure or symptoms. They can also print out their result.

Reach

This screening tool is part of Ontario's approach to re-opening courthouses. The tool allows people to complete the online screening before going to court. The results must be shown to enter a courthouse. Paper screening options in multiple languages are also available at the courthouse.

Potential Impacts

Decisions made based on the results of the tool can impact the access to courthouses for people in Ontario.

Internal Use Policies

This is a tool made for public use and is not used as part of internal decision or policy making.

Technical Description

The tool is implemented using Gatsby, which is a React-based, GraphQL powered static site generator. Because Gatsby compiles into static HTML/CSS/JS, it enables blistering performance and simple deployments.

The Government of Ontario's data catalogue is a good start and demonstrates a significant commitment to algorithmic transparency. In the LCO's view, this initiative would be significantly improved if the disclosure requirement were a mandatory obligation across the provincial government.

The federal Directive includes a mandatory disclosure requirement. The Directive requires notice on websites when decisions will be made by or with the assistance of AI or ADS, regardless of the applicable impact level.[134] Those notices must be in plain language and prominently displayed.[135] Agencies are similarly required to provide meaningful explanations of their ADS-informed decisions to affected individuals.[136] In addition, systems with Impact Levels of III or IV, agencies must "publish documentation on relevant websites about how the [systems] works, in plain language, describing:

- How the components work;
- How it supports the administrative decision;
- Results of any reviews or audits; and
- A description of the training data, or a link to the anonymized training data if this data is publicly available.[137]

The LCO recommends governments across Canada develop mandatory AI Registries for their respective jurisdictions. Precedents exist for equivalent programs in other areas. For example, the Government of Ontario's Open Data Directive requires the Chief Data and Digital Officer to

> 1. *…coordinate and maintain a comprehensive government-wide data inventory. This data inventory will be published online and will be accessible to the public.*
> 2. *The Chief Digital and Data Officer will identify common core metadata elements and data standards, where applicable, to describe items listed in the inventory.*
> 3. *Each ministry and provincial agency must create an inventory of datasets within its custody and control.*
> 4. *Each ministry who has custody and control of datasets must contribute to the government-wide data inventory by providing to the Chief Digital and Data Officer a listing of all datasets or categories of data.*
> 5. *Provincial agencies must publish their inventories on a new web page on their site or, in its absence, another government website in accordance with the Open Data Guidebook and provide the link to their inventory to the Chief Digital and Data Officer.*
> 6. *Ministries and provincial agencies are responsible for keeping their inventory list up-to-date on an ongoing basis.*[138]

The provincial inventory of datasets is accessible through a comprehensive and user-friendly online catalogue.[139] A national, provincial or municipal AI Registry could adopt a similar format.

In addition to creating a public inventory or mandatory AI Register, governments need to consider whether AI Registry disclosure requirements should be variable. This approach would be consistent with the risk-based impact assessment model discussed earlier. It is also true that there may be little need to disclose or post information about AI and ADM systems with no impact on rights or interests.

The LCO believes disclosure should include disclosure of both the *existence* of a system and disclosure of a broad range of tools and processes *used by the system*. For example, many of the systems described in this report have significant impacts and raise important issues regarding data discrimination and/or data validity, accuracy or reliability. In these circumstances, it is appropriate to provide extensive disclosure of a system's source and use of data, including:

- Training data.
- Description of design and testing policies and criteria.
- List of factors that tools use and how they are weighted.
- Thresholds and data used to determine labels for scoring.
- Outcome data used to validate tools.
- Definitions of what the instrument forecasts and for what time period.
- Evaluation and validation criteria and results.[140]

Given the centrality of data to AI and ADM systems, the LCO supports mandatory and broad data disclosure as a necessary means to ensure public and legal accountability and transparency. Readers should note, however, that many government officials believe data disclosure requirements need to be balanced against the risk of "gaming" or external scrutiny or manipulation, at least in some circumstances. As a result, many officials are wary of disclosing source code.

2. Impact Assessments

Another important tool to ensure AI and ADM transparency and accountability are AI or algorithmic impact assessments. Indeed, the LCO's research suggests that impact assessments have become perhaps the most widely-promoted tool for ensuring AI and ADM transparency and accountability.

Impact assessments take many forms, have varying levels of detail, and may or may not be mandatory. Impact assessments can be limited in scope (focussing on privacy or data protection, for example), focused on human rights (known as human rights impact assessments (HRIA)), or broader. For example, the proposed US *Algorithmic Accountability Act* would require the Federal Trade Commission to pass regulations requiring entities "to conduct automated decision system impact assessments" and "data protection impact assessments" of all existing and new high-risk automated decision systems.[141] A more comprehensive model is the AINow's Algorithmic Impact Assessment, which is a sophisticated framework for assessing, evaluating and monitoring AI and algorithmic systems in use by government.[142]

Many current impact assessment proposals take the form of guidelines or best practices, consistent with an "ethical AI" approach. The HLEG's recent "Assessment List for Trustworthy AI" is a comprehensive example. The HLEG's Assessment List includes a set of self-assessment criteria for AI developers, including criteria addressing:

- Human agency and oversight
- Technical robustness and safety
- Privacy and data governance
- Transparency
- Diversity, non-discrimination, and fairness
- Societal and environmental well-being
- Accountability[143]

For the purposes of this discussion, the HLEG Assessment List is notable for two reasons: First, as discussed earlier, the HLEG Assessment List is a voluntary, self-assessment model, not a mandatory or binding requirement. As a result, its use as an accountability tool is diminished significantly. Second, the HLEG's self-assessment criteria and questions are detailed but lack specificity in key areas, including legal compliance.

The federal Directive and the accompanying Algorithmic Impact Assessment (AIA) tool are a significant improvement on the HLEG self-assessment model. The Directive requires an Algorithmic Impact Assessment for every automated decision-making system within the Directive's scope, including an assessment of "the impact on rights of individuals or communities." The Directive further requires that Algorithmic Impact Assessments be released publicly.[144]

The AIA is a fundamental component of the federal Directive. The AIA asks persons or organizations considering an ADM system to address approximately 60 questions designed to evaluate the appropriate risk level for a proposed system.[145] The questions address issues such as project details, the impact of a system and proposed mitigation measures. Once responses to these questions have been input into the AIA, a report is produced indicating the proposed systems' Impact Level and associated requirements for peer review, notice, explanation, and other factors. A final version of the AIA is then required to be publicly posted on Government of Canada websites, or as may be required by the federal Directive on Open Government. The following table includes a sample of some of the questions asked on the AIA.

Sample of Questions Asked on the Federal Algorithmic Impact Assessment

- **Capabilities of system?**
- **Factor(s) motivating introduction of automation into decision-making process?**
- **Is project in area of intense public scrutiny and/or frequent litigation?**
- **Are clients in the relevant "line of business particularly vulnerable?"**
- **Are stakes of decisions very high?**
- **Will project have major impacts on numbers of staff or their roles?**
- **Will project require new policy authority?**
- **Whether algorithm used is a (trade) secret?**
- **Whether the algorithmic process is difficult to interpret or explain?**
- **Will system assist or replace human decision-maker?**
- **Impact of system on the rights and freedoms of individuals, the health and well-being of individuals, the economic interests of individuals, and the ongoing sustainability of an environmental ecosystem?**
- **Is impact reversible and how long will impact last?**
- **Who collected data?**
- **De-risking and mitigation data quality measures, including existence of "documented processes in place to test datasets against biases and other unexpected outcomes."**
- **De-risking and mitigation procedural fairness measures, including audit trails.**
- **Is system capable of producing reasons for its decisions/recommendations when required?**
- **"Recourse process" planned or established for clients that wish to challenge the decision?**
- **Human override of system decisions?**
- **Extent of consultation? With whom?**

Washington State House Bill 1655 includes similarly comprehensive requirements for impact assessments. The original version of this Bill stated that an agency proposing to use an ADM system must complete a detailed "algorithmic accountability report" to be submitted to Washington State's Chief Privacy Officer for approval prior to deployment. [146] A substitute version of the Bill would require the Chief Privacy Officer to prepare an annual "algorithmic impact inventory" of "all automated decision systems that are being used, developed, or procured by state agencies."[147] This inventory would include "clear and understandable statements" of a wide range of materials for each ADM system.[148] The table on the next page sets out the extraordinary detail and range of information to be included in these reports.

In the LCO's view, impact assessments are a fundamental tool for ensuring public and legal accountability of AI and ADM systems. The LCO further believes that impact assessments must be mandatory, detailed and transparent. As a result, the LCO does not believe ethical AI self-assessments are sufficient to ensure public accountability of these systems. Finally, the LCO believes AI and ADM impact assessments should be publicly available on the comprehensive AI Register described in the previous section.

Once again, the federal Directive, Algorithmic Impact Assessment and Washington State House proposals are an important step in the right direction. The federal Directive would be improved, however, if it required more explicit assurances (and thus more accountability) on several key issues. For example, the LCO believes impact assessments should also include:

- A clear description of the purpose and objectives of the AI or ADM system, including how the system will be used to fulfill specified statutory objectives;
- Assurances on compliance with *Charter* and human rights legislation and a description of potential impacts on constitutional, human rights or privacy rights;
- A clear description of how an individual may challenge or appeal a decision based in whole or part on an AI or ADM system;
- Assurances on compliance with best practices in data collection, retention, management and testing; and,
- Assurances regarding public participation in design, development, and evaluation of AI and ADM systems.

The LCO reiterates that the risks of AI and ADM systems extend far beyond the federal government and the scope of the current federal Directive. Transparency, accountability, human rights, fairness and "trustworthiness" are important principles in all high-impact AI and ADM applications and in all public institutions. As a result, the LCO strongly recommends that the Government of Ontario, municipalities and other public institutions adopt mandatory impact assessments consistent with the analysis above.

Washington State House Substitute Bill 1655 Algorithmic Accountability Report Summary of Requirements

Each algorithmic accountability inventory report must include clear and understandable statements of the following:

a) ADM system's name, vendor, and version;

b) Description of system's general capabilities, including reasonably foreseeable capabilities outside the scope of the agency's proposed use;

c) Type or types of data inputs used; how data is generated, collected, and processed; type or types of data system is reasonably likely to generate;

d) Whether the system tested by an independent third party, has known bias, or is untested for bias;

e) Description of the purpose and proposed use of the system, including decision or decisions it will be used to make or support and intended benefits, including research demonstrating benefits;

f) Whether the system makes decisions affecting constitutional or legal rights, duties, or privileges of any Washington resident;

g) Whether the system gives notice to an individual of:

(i) The system's name, vendor, and version;

(ii) Decision or decisions system makes or supports;

(iii) Whether system is final decision system or support decision system;

(iv) Policies and guidelines apply to its deployment;

(v) Whether a human verifies or confirms decisions made by system; and

(vi) How an individual can contest any decision made by system;

h) Whether system ensures agency can explain decision to impacted individuals in terms understandable to a layperson;

i) Whether system is subject to appeal, immediate suspension if a legal right, duty, or privilege is impacted by the decision, and potential reversal by a human decision maker through a timely process clearly described and accessible to an individual impacted by the decision;

j) Description of potential impacts of the system on civil rights and liberties and potential disparate impacts on marginalized communities, and a mitigation plan;

k) A clear use and data management policy, including protocols for the following:

(i) How and when the system will be deployed or used and by whom; factors that will be used to determine where, when, and how the technology is deployed;

(ii) How system data will be securely stored and accessed, and whether agency intends to share access to system or data with any other entity, and why; and,

l) Description of fiscal impact of the system, including acquisition costs; ongoing operating costs and cost savings achieved by system.

3. Procurement

Governments must consider whether AI systems will be developed within government, procured from outside contractors, or some form of partnership between the two.

Procurement has become a high profile and controversial AI and ADM disclosure and regulatory issue. This is because of concerns that proprietary AI or ADM tools may rely on trade secret claims to prevent disclosure and transparency.[149] Many of these concerns were crystallized in a 2016 Wisconsin state court decision, *State v. Loomis,*[150] in which the Wisconsin Supreme Court refused to order disclosure of a proprietary algorithmic risk assessment tool, COMPAS, that a trial judge had relied upon, in part, in sentencing Loomis to six years in prison.[151]

Trade secrets or proprietary software should not be used as a shield to prevent, or limit, public accountability and transparency of AI and ADM systems. It is also worth noting that outsourcing AI and ADM design does not absolve a government from their legal obligations respecting human rights, due process and/or procedural fairness. As a result, the LCO believes governments should adopt (or amend) procurement rules to ensure these legal requirements are met.

There are many valuable best practices to draw lessons from. For example, the UK Office for Artificial Intelligence's "Guidelines for AI Procurement" sets out ten considerations for government bodies procuring AI systems, including:

1. Include your procurement within a strategy for AI adoption.
2. Make decisions in a diverse multidisciplinary team.
3. Conduct a data assessment before you start your procurement process.
4. Assess the benefits and risks of AI deployment.
5. Engage effectively with the market from the start.
6. Establish the right route to market and focus on the challenge rather than a specific solution.
7. Develop a plan for governance and information assurance. You must establish appropriate oversight mechanisms to allow scrutiny of AI systems throughout their lifecycle.
8. Avoid Black Box algorithms and vendor lock in.
9. Focus on the need to address technical and ethical limitations of AI deployment during your evaluation.
10. Consider the lifecycle management of the AI system. [152]

Under the federal Directive, custom source code owned by the Government of Canada is required to be released according to the applicable requirements of the *Directive on Management of Information Technology* unless the source code is processing data classified as secret, top secret, or falls into other defined categories.[153]

XII. BIAS AND FAIRNESS

1. Discrimination

Arguably the most significant risk associated with government use of AI and ADM systems is their potential to amplify existing bias and discrimination. The Partnership on AI notes

> *A central concern with the rise of artificial intelligence (AI) systems is bias. Whether in the form of criminal "risk assessment" tools used by judges, facial recognition technology deployed by border patrol agents, or algorithmic decision tools in benefits adjudication by welfare officials, it is now well known that algorithms can encode historical bias and wreak serious harm on racial, gender, and other minority groups.*[154]

To many critics, AI and ADM systems represent nothing more than "a sophisticated form of racial profiling."[155]

The LCO Criminal AI Issue Paper discusses discrimination within the context of criminal proceedings at length. The report addressed the many ways in which an AI or ADM system can be biased and the pressing need for law reform. For example, many AI and ADM systems rely on historically racist, discriminatory or biased data. Discrimination and bias issues also arise in discussions regarding statistical "metrics of fairness," scoring, automation bias, due process, access to justice and the accuracy, reliability and validity of datasets.[156] In the LCO's view, the issues and lessons from the criminal context are applicable to other areas of government decision-making.

Given this context, governments must consider how to effectively prevent, disclose and/or remedy bias and discrimination in government AI and ADM systems.

Governments, technologists, legal organizations, academics, civil society organizations, community organizations and industry associations around the world have committed to addressing bias and discrimination issues in AI and ADM systems. As a result, there are many promising examples, best practices and regulatory regimes that Canadian policymakers can draw upon.

To its credit, the Government of Ontario has addressed this issue forthrightly: The government's 2019 discussion paper, *Promoting Trust and Confidence in Ontario's Data Economy*,[157] establishes promoting trust and confidence in the government's use of AI systems as the first of three pillars of the Ontario Data Strategy.[158] The paper notes bias and discrimination as a threat or risk associated with "data-driven practices" and links issues related to bias with the 'black box' problem.[159] The paper provides the following two examples of algorithmic bias:

- "An algorithm used to make an administrative decision assigns undue weight to a characteristic leading to discrimination against a certain group… [and]
- A machine learning algorithm optimizes for numerically dominant groups in a training dataset, excluding data at the margins which represent a marginalized group…"[160]

The options for addressing bias in AI and ADM are extensive. What follows below are highlights or examples of several complementary approaches:

Constitutional or Human Rights Provisions

Several jurisdictions have adopted or considered explicit legislative commitments to ensure AI and ADM systems are compliant with constitutional law or anti-discrimination statutes. These provisions may include legislative findings, preambles or explicit provisions stating that an AI or ADM system must comply with constitutional principles or anti-discrimination legislation.

For example, Washington State House Bill 1655 includes provisions that

> *A public agency may not develop, procure, or use an automated decision system that discriminates against an individual, or treats an individual less favorably than another, in whole or in part, on the basis of one or more [enumerated] factors…*
>
> *A public agency may not develop, procure, or use an automated final decision system to make a decision impacting the constitutional or legal rights, duties, or privileges of any Washington resident...*[161]

This legislation would further require agencies proposing to use ADM systems to publicly disclose

> *…a description of any potential impacts of the [ADM] system on the civil rights and liberties and potential disparate impacts on marginalized communities, and a mitigation plan…*[162]

Interestingly, the federal Directive does not appear to *explicitly* require AI or ADM systems to comply with the *Charter* or Canadian human rights legislation. Rather, the federal Directive states that its objective is to:

> *…ensure that Automated Decision Systems are deployed in a manner that reduces risks to Canadians and federal institutions, and leads to more efficient, accurate, consistent, and interpretable decisions made pursuant to Canadian Law.*[163]

By way of contrast, the federal Directive is explicit about the requirement to comply with "administrative law principles."[164] The Directive further states that its expected results are that

> *Decisions made by federal government departments are data-driven, responsible, and complies with procedural fairness and due process requirements.*[165]

The federal Directive also explicitly requires the developers of all federal AI systems to consult with government legal services to ensure the use of the ADM comply with "applicable" laws.[166]

The LCO believes the federal Directive should be commended for its explicit commitment to administrative law principles and "applicable laws". Nonetheless, the LCO further believes that the federal Directive would be strengthened considerably if it added an explicit commitment that the federal government will ensure that AI and ADM systems comply with the *Charter* and appropriate human rights legislation. These provisions, although potentially technically unnecessary, would provide greater legal certainty and accountability and promote public trust in the face of widespread concerns about "racist" or discriminatory AI and ADM systems. The federal government's assessment of a system's *Charter* or human rights compliance should also be included in a system's impact assessment, as discussed above. These requirements should also be included in any equivalent legislative or regulatory instrument governing AI and ADM systems used by provincial governments, municipalities and other public institutions.

The LCO will discuss AI systems and compliance with *Charter* and human rights provisions further in our third Issue Paper, *AI, ADM and Government Decision-making*.

Data Disclosure Requirements

Many of the proposals and options promoting greater disclosure of AI and ADM systems are designed to reducing bias and discrimination.

"Data discrimination" issues are discussed at length in the LCO's *Criminal AI Issue Paper*. Perhaps more than any other issue, "data discrimination" and data validity issues are at the heart of most public controversies about AI and ADM. Accordingly, many of the proposals for addressing bias and discrimination require comprehensive disclosure of the data and variables used to train, calibrate and operate AI and ADM systems.

Once again, the Washington State legislation is a good example of a thoughtful approach. In this regime, the developers of all ADM systems must produce an algorithmic accountability report that includes, among other things,

> *…clear and understandable statements of…the type or types of data inputs that the technology uses; how that data is generated, collected, and processed; and the type or types of data the system is reasonably likely to generate.*[167]

The LCO discussed data disclosure requirements earlier in this paper, where we suggested that these requirements could mandate disclosure of information regarding a system's source and use of data, including:

- Training data.
- Description of design and testing policies and criteria.
- List of factors that tools use and how they are weighted.
- Thresholds and data used to determine labels for scoring.
- Outcome data used to validate tools.
- Definitions of what the instrument forecasts and for what time period.
- Evaluation and validation criteria and results.

Best Practices and Ethical AI Guidelines

In addition to the proposals discussed above, there are many emerging best practices for addressing bias and discrimination in AI and ADM systems. The LCO's *Criminal AI Issue Paper* provides several examples of best practices (data practices, public participation, evaluation of AI and ADM systems) designed to reduce or mitigate biased AI and ADM systems.[168] The HLEG's Assessment List, described above, is a detailed example of a best practice to address "data discrimination." Key excerpts include:

> *In order to achieve Trustworthy AI, we must enable inclusion and diversity throughout the entire AI system's life cycle. AI systems (both for training and operation) may suffer from the inclusion of inadvertent historic bias, incompleteness, and bad governance models…*
>
> **Avoidance of Unfair Bias**
>
> - *Did you establish a strategy or a set of procedures to avoid creating or reinforcing unfair bias in the AI system, both regarding the use of input data as well as for the algorithm design?*
> - *Did you consider diversity and representativeness of end-users and/or subjects in the data?*
>   - *Did you test for specific target groups or problematic use cases?*
>   - *Did you research and use publicly available technical tools, that are state-of-the-art, to improve your understanding of the data, model and performance?*
>   - *Did you assess and put in place processes to test and monitor for potential biases during the entire lifecycle of the AI system (e.g., biases due to possible*

  - *limitations stemming from the composition of the used data sets (lack of diversity, non-representativeness)?*
  - *Where relevant, did you consider diversity and representativeness of end-users and or subjects in the data?*

- *Did you put in place educational and awareness initiatives to help AI designers and AI developers be more aware of the possible bias they can inject in designing and developing the AI system?*
- *Did you ensure a mechanism that allows for the flagging of issues related to bias, discrimination or poor performance of the AI system?*
  - *Did you establish clear steps and ways of communicating on how and to whom such issues can be raised?*
  - *Did you identify the subjects that could potentially be (in)directly affected by the AI system, in addition to the (end-)users and/or subjects?*
- *Is your definition of fairness commonly used and implemented in any phase of the process of setting up the AI system?*
  - *Did you consider other definitions of fairness before choosing this one?*
  - *Did you consult with the impacted communities about the correct definition of fairness, i.e., representatives of elderly persons or persons with disabilities?*
  - *Did you ensure a quantitative analysis or metrics to measure and test the applied definition of fairness?*
  - *Did you establish mechanisms to ensure fairness in your AI system?*[169]

The LCO believes best practices of this sort should be used to supplement, not replace, stronger anti-bias and discrimination regulatory protections.

Explanation Requirements and Interpretable Models

Both Washington State House Bill 1655 and the Government of Canada's Directive on Service and Digital contain important but perhaps underappreciated provisions linking requirements for explanations and interpretable models with bias reduction. For example, the federal Directive on Service and Digital states:

> *Having an easily interpretable model can also greatly simplify testing and monitoring of [an ADM] system, including assessing bias.*[170]

Research, Testing and Evaluation Requirements

Another important initiative to reduce the potential for bias and discrimination is a requirement for regular research, testing and evaluations of AI and ADM systems. Accordingly, governments should establish mandatory regulatory requirements that AI and ADM be audited and evaluated for accuracy, effectiveness, efficiency, and bias.

There are many examples of statutory research, evaluation and/or auditing requirements. Washington State House Bill 1655 explicitly acknowledges the importance of "independent third-party testing, auditing, [and] research" in order to verify accuracy and mitigate the potential for bias and discrimination. [171]

Similarly, the American *FUTURE of Artificial Intelligence Act of 2017* would direct the Department of Commerce "to establish a Federal Advisory Committee…[to study how]…bias can be identified and eliminated in the development of artificial intelligence and in the algorithms that support them," including with respect to the following:

> (i) The selection and processing of data used to train artificial intelligence.
> (ii) Diversity in the development of artificial intelligence.
> (iii) The ways and places the systems are deployed and the potential harmful outcomes.[172]

Another American proposal, *SIL20719—A Bill to provide for data accountability and transparency,* is a more nuanced approach.[173] This Bill would require data aggregators that use automated decision systems to perform "continuous and automated testing for bias on the basis of a protected class" and for "disparate impacts on the basis of a protected class."[174] However, this Bill does not completely prohibit the use of biased AI systems (or those that produce biased results), stating:

> *[i]f the use of personal data causes a disparate impact on the basis of a protected class... the data aggregator has the burden of demonstrating that such use of personal data–*
>
> *(1) is not intentionally discriminatory.*
>
> *(2) is strictly necessary to achieve one or more substantial, legitimate, nondiscriminatory interests; and*
>
> *(3) there is no reasonable alternative policy or practice that could serve the interest described in paragraph (2) with a less discriminatory effect.*[175]

The federal Directive requires testing for unintended biases before the system goes into production. Data used by the system must also be "routinely tested to ensure that it is still relevant, accurate, and up-to-date."[176] Finally, the Directive also requires peer review of all systems classified at Level II or higher. Peer review for Level IV systems appears robust, requiring the review of at least two qualified experts from listed organizations, including the National Research Council of Canada, relevant non-governmental organizations, or a contracted third-party vendor with a relevant specialization.[177]

The issue of bias and AI and ADM systems will be discussed further in the LCO's third Issue Paper, *AI, ADM and Government Decision-Making.*

2. Procedural Fairness/Due Process

This section considers whether or how governments can enshrine or ensure procedural fairness or due process protections in AI or ADM systems.

The pioneering work in this area was undertaken by Professor Danielle Keats Citron is a seminal 2008 article titled "Technological Due Process."[178] Professor Citron argued that AI and algorithms require deeper analysis of due process and regulatory issues than traditional legal models would suggest. She stated that

> *The twenty-first century's automated decision-making systems bring radical change to the administrative state that last century's procedural structures cannot manage.*[179]

Many of the proposals to ensure AI and algorithmic accountability discussed in this report are based on "technological due process" principles and priorities. The key elements of technological due process are transparency, accuracy, accountability, participation, and fairness.

The LCO's research reveals a general lack of procedural fairness and due process protections in most AI and ADM regulatory models and best practices. Access Now, for example, notes that due process "is a consistent gap in the AI strategies."[180] Many of the ethical AI guidelines addressed in this paper include general references to human rights or explainability rather than detailed due process protections.

The federal Directive is a notable exception. The Directive explicitly states that an objective of the Directive is that "[d]ecisions made by federal government departments are data-driven, responsible, and compl[y] with procedural fairness and due process requirements."[181] Professor Scassa notes that "…[the Directive] and AIA are, in fact, built upon norms for administrative decision-making that have their roots in common law principles of procedural fairness."[182] For example, the Directive states that a government department using an ADM system must

- Provide "notice on relevant websites that the decision rendered will be undertaken made in whole or in part by an Automated Decision System."[183]
- Provide "a meaningful explanation to affected individuals of how and why the decision was made."[184]
- Provide "clients with any applicable recourse options that are available to them to challenge the administrative decision."[185]

The Directive further states that

> *Procedural fairness is a guiding principle of government and quasi-government decision-making. The degree of procedural fairness that the law requires for any given decision-making process increases or decreases with the significance of that decision and its impact on rights and interests.*[186]

The administrative law-orientation of the Directive is confirmed in the AIA, which includes questions such as

- Will the audit trail identify the authority or delegated authority identified in legislation?
- Will the system provide an audit trail that records all the recommendations or decisions made by a system?
- Will the audit trail show who the authorized decision maker is?
- Will the system be able to produce reasons for its decisions or recommendations when required?
- Will there be a recourse process planned or established for clients that wish to challenge the system?
- Will the system enable human override of system decisions?[187]

Professors Scassa and Raso have both analyzed the Directive against Canadian administrative law principles and requirements, including the requirements for fairness, notice, disclosure, hearings and reasons. Professor Scassa writes, for example, that "the [Directive] is an intriguing example of "procedural fairness by design" and that

> *A major contribution of the [Directive] and the AIA tool is their attempt to embed principles of fairness, transparency and accountability up front in system design – rather than relying upon judicial review to correct the problems with specific outcomes."*[188]

Both scholars conclude that Canadian administrative law and the Directive itself leave many unanswered questions that may have to be addressed through judicial review or amendments.[189] Outstanding questions include:

- Are the notice and disclosure provisions of the Directive sufficient to meet administrative law requirements?[190]
- If a "hearing" requires a decision-maker to "hear" and consider both sides to a dispute, "…what does this standard mean when human officials *plus* algorithmic tools evaluate some [of the] evidence?"[191]
- What does the Directive's requirement for a "meaningful explanation" mean?[192]
- What is the standard of review of decisions made or assisted by ADM systems?[193]

These and other questions about the Directive will no doubt be addressed by tribunals, courts, academics, litigants and policymakers over the course of time.

These and related issues will be discussed further in the LCO's third Issue Paper, *AI, ADM and Government Decision-Making*. For the purpose of this report, however, the LCO wants to bring attention to several recurring issues and themes concerning procedural fairness and due process in AI and ADM systems.

Scope and Exclusions

As noted earlier in this report, the federal Directive has several important limits on its application and scope, including explicit exemptions (e.g. national security) and the Directive's limitation to "administrative decisions" and ADM systems that provide external services." Absent amendments to the Directive or judicial interpretation, ADM systems beyond these parameters will lack the procedural fairness protections enacted in the Directive.

Criminal Justice Applications

Significantly, the Directive does not appear to apply to AI, ADM or algorithmic tools that may be used in the criminal justice system, including predictive policing, algorithmic risk assessments, and/or facial recognition technology. These are probably the most common and highest impact AI, ADM or algorithmic systems used by governments today.

Once again, experience in the United States demonstrates the harms and controversies that can (and likely will) arise if and when these tools are introduced in Canada without proper due process protections in place prior to implementation.

In this regard, it is worth noting that American policymakers, community organizations, academics and governments have identified a wide range of proposals, laws, rules and best practices to ensure:

- An appropriate role and tools for courts overseeing AI and ADM systems; and,
- An effective right to challenge the operation or use of an AI or ADM tool in individual cases.[194]

Jurisdictional Gaps

The federal Directive regulates AI and ADM in the federal government and federal agencies. As discussed, there is no equivalent regulatory framework in Ontario or any other Canadian province. As a result, there are no dedicated procedural fairness or due process protections governing potential uses of AI and ADM by provinces, municipalities, police services, child welfare agencies and/or many other important public institutions.

The Mixed Model/Shared Mandate

Finally, the LCO notes that governments will have to determine which procedural fairness/due process protections can or should be enshrined in "framework" or "horizontal" regulation as opposed to "vertical" instruments.

Experience suggests that comprehensive protections for procedural fairness and due process will very much depend on explicit and dedicated statutes, regulations, directives and rules of practice governing specific areas of government activity or ministries.

XIII. OVERSIGHT AND REMEDIES

1. Independent Oversight

Governments will need to consider whether and how to establish independent oversight of both individual AI and ADM systems and government use of this technology generally. These are two separate issues, both of which can make significant contributions to AI and ADM transparency, accountability and effectiveness.

Oversight of Individual Systems

There is an international consensus that AI and ADM systems should be subject to regular oversight and evaluations by external experts. For example, the Partnership on AI's "ten minimum requirements for the responsible deployment of criminal risk assessment tools" include two specifically dedicated to open research and evaluations:

> ***Requirement 8:*** *Tool designs, architectures, and training data must be open to research, review and criticism*
>
> *Risk assessment tools embody important public policy decisions made by governments, and must be as open and transparent as any law, regulation, or rule of court…In particular, the training datasets, architectures, algorithms, and models of all tools under consideration for deployment must be made broadly available to all interested research communities—such as those from statistics, computer science, social science, public policy, law, and criminology, so that they are able to evaluate them before and after deployment.*
>
> ***Requirement 10:*** *Jurisdictions must take responsibility for the post-deployment evaluation, monitoring, and auditing of these tools*
>
> *Jurisdictions must periodically publish an independent review, algorithmic impact assessment, or audit of all risk assessment tools they use…Subsequent audits will need to examine the outcomes and operation of the system on a regular basis.*
>
> *To ensure transparency and accountability, an independent outside body (such as a review board) must be responsible for overseeing the audit…To mitigate privacy risks, published versions of these audits should be redacted and sufficiently blinded to prevent de-anonymization.*[195]

The federal Directive fulfills some, but not all, of these requirements. The Directive permits external, independent review, but does not require it. The extent of the peer review depends upon the identified risk of the system. An ADM system with a "moderate" impact (Level II) must be peer reviewed by at least one expert. Systems with a potentially "very high impact" (Level IV) must include at least two experts. Independent review is possible, but not guaranteed, as the Directive states that experts can include specialists internal to government, academics, representatives from an NGO, a "third-party vendor", or an expert from an advisory board established by the federal Treasury Board.

In the LCO's view, the Directive and any equivalent instruments at the provincial, municipal or agency level should mandate independent reviews consistent with the PAI standards. These requirements should explicitly specify that independent evaluations must include representatives from a broad cross-section of experts and stakeholders, including data scientists, legal representatives, and members of the communities most affected by the AI or ADM system.

Oversight of Government AI and ADM Systems Generally

Many proposals recommend that governments establish an independent oversight body or coordination office to oversee systemic AI and ADM development, deployment and evaluation.The rationale for this approach has been summarized by the New Zealand Law Foundation as follows:

> *[w]hile important, …, regulatory models that rely on affected individuals enforcing legal rights are unlikely to be adequate in addressing the concerns around increasing use of algorithms. One, affected individuals will lack the knowledge or the means effectively to hold these tools and processes to account. They are also likely to lack the 'wide-angle' perspective necessary to evaluate their effective populations.*[196]

The New Zealand Law Foundation's report, *Government Use of Artificial Intelligence in New Zealand,* includes a very comprehensive review of various oversight models, including regulatory agencies and self-regulatory models.[197]

Some jurisdictions, such as Manitoba, have established bodies to advise governments on "the ethical, social and emerging technologies"[198] including AI systems.

CIFAR (formerly the Canadian Institute for Advance Research) has recommended the establishment of a Department of Digital Policy and an Office of the Chief Algorithmic Intelligence Auditor, who would be responsible for managing government responses to AI systems, developing regulations with respect to transparency and accountability for AI system-informed decisions, and ensuring that AI systems are designed to align with human rights regulations.[199]

There are many American examples of coordinated or independent oversight of AI and ADM systems. For example, an Executive Order adopted by the City of New York Office of the Mayor establishes an "Algorithms Management and Policy Officer" who will be responsible for matters

> *…relating to the fair and responsible use of algorithmic tools and other emerging technologies in city agency decision-making, coordinate efforts to create and strengthen related best practices citywide, and support agencies in implementing such practices."*[200]

A recent bill introduced in the US Senate, *A Bill to Provide for Data Accountability and Transparency,* would establish an independent body responsible for overseeing government use of AI.[201] Washington State House Bill 1655 assigns responsibilities to the Washington's Chief Privacy Officer to adopt rules "regarding the development, procurement, and use of automated decision systems by a public agency" which must include "the minimum standards and procedures" established by the Bill. [202]

The LCO supports the principle of independent oversight and intergovernmental coordination of AI and ADM systems. The LCO is less certain about the institutional design or placement of these functions. Governments will have to give considerable thought to the best way to achieve independent oversight, especially in light of the mandates of existing government agencies, such as Privacy Commissioners or Human Rights Commissions.

2. Remedies

Access to meaningful remedies is a key principle of access to justice. The LCO's research reveals comparatively few examples of statutes, regulations or guidelines that set out explicit remedial provisions.

The federal Directive is a partial exception to this finding. The federal Directive states that the Assistant Deputy Minister responsible for a program using an ADM system is responsible for:

> *6.4.1 Providing clients with any applicable recourse options that are available to them to challenge the administrative decision.*[203]

This commitment, while explicit, is not very specific. More importantly, while the federal Directive may acknowledge the need for remedies, the Directive does not actually *create* a legal right to a remedy. Professor Scassa notes that

> *While directives are important policy documents within the federal government, and while there are accountability frameworks to ensure compliance, the requirements to comply with directives are internal to government, as are the sanctions. Directives do not create actionable rights for individuals or organizations.*[204]

This is a significant limitation on the effectiveness and potential accountability of the Directive.

The federal Directive may be contrast with Washington State House Bill 1655. That proposed statute creates rights of appeal for individuals about whom decisions are made by, or with the assistance of, ADM systems. The Bill would also require agencies to be able to explain the bases for such decisions. Section 4(1)(c) of that Bill states:

> *A public agency that develops, procures, or uses an automated decision system must…*
>
> *(c) Ensure that any decision made or informed by the automated decision system is subject to appeal, immediate suspension if a legal right, duty, or privilege is impacted by the decision, and potential reversal by a human decision maker through a timely process clearly described and accessible to an individual impacted by the decision.*[205]

Finally, the Bill would give any person injured by a "material violation" of the Act (which may include denial of any government benefit) a statutory right to institute proceedings against an agency and the right to seek injunctive relief, restoration of the government benefit in question, declaratory relief, or a "writ of mandate."[206]

The lack of a statutory remedies regime obviously does not mean that government decisions made or aided by AI and ADM cannot or will not be challenged. There are many potential grounds and routes for legal challenges, particularly if it is alleged that the decision or system was discriminatory in some fashion.

The LCO's *Criminal AI Issue Paper* discussed the limits of "regulation by litigation" as a strategy for challenging ADM decisions in the criminal justice system at length.[207] Unfortunately, the LCO concluded that

> *Litigation obviously has an important role in regulating AI and algorithms in the criminal justice system. Many issues will always be best addressed in open court with the benefit of an evidential record and high-quality and experienced counsel…*
>
> *Litigation, while obviously necessary to address specific cases, is insufficient to address the systemic statistical, technical, policy and legal issues that have been addressed in this report so far.*[208]

In that paper, the LCO emphasized the enormous practical burden placed on individual defendants wishing to challenge decisions based on automated risk assessment tools:

> *Consider just some of the complex statistical, technical and policy issues that could (or should) have been litigated in Loomis or equivalent cases:*
>
> - *Is the historic data used to train the COMPAS tool biased, accurate, reliable and valid?*
> - *Are COMPAS risk factors and scores weighed and calculated appropriately?*
> - *Which communities bear the burden of statistical errors?*
> - *Are the confidence estimates for COMPAS predictions appropriate?*
> - *Are COMPAS predictions validated appropriately?*
> - *Does COMPAS use factors such as education or employment as impermissible statistical proxies for race or gender?*
>
> *Loomis was a comparatively simple, State-court criminal proceeding in which Loomis had already plead guilty. The COMPAS issue arose at sentencing. It is inconceivable that Loomis or any other criminal defendant (particularly one represented by a public defender/legal aid or self-represented) would be in a position to mount an effective challenge to the complex statistical, technical and legal issues raised by COMPAS.*[209]

The LCO ultimately concluded that access to justice in criminal proceedings depended on both regulation of ADM *systems* and a dedicated remedial regime that allowed criminal defendants to effectively challenge *individual* ADM-based decisions. The LCO also warned that failure to adopt such measures could add significant barriers for low-income, Indigenous and racialized communities, thus compounding the over-representation of these communities in the criminal justice system.

Outside of the criminal context, most challenges to government AI or ADM decisions will likely be based in civil litigation, administrative law principles or perhaps the Canadian or Ontario Human Rights Code. The LCO's third Issue Paper, *AI, ADM and Government Decision-Making,* will consider these issues in detail.

XIV. CONCLUSION

This paper has identified a series of important legal and policy issues that Canadian policymakers should consider when contemplating regulatory framework(s) for AI and ADM systems that aid government decision-making.

The LCO has concluded that law reform is needed to ensure AI and ADM meet high legal standards regarding disclosure, legal accountability, equality, procedural fairness/due process and access to remedies. Law reform is also needed to support better public services; economic development; AI innovation and trustworthiness; and fair and legitimate government and justice-system decision-making.

Proactive law reform will help Ontario and other Canadian jurisdictions maximize AI and ADM's potential benefits, while minimizing potential harm.

A key finding in this report is that there is an extraordinary regulatory gap in Canada. The federal Directive is a significant initiative to regulate AI and ADM in Canada. Unfortunately, there is no equivalent regulatory framework in Ontario or any other Canadian province. As a result, some of the most consequential potential uses of AI and ADM by provinces, municipalities, police services, child welfare agencies and/or many other important public institutions are under- or unregulated.

Fortunately, the key elements of a comprehensive regulatory regime can be identified, including

- Baseline requirements for all government AI and ADM systems, irrespective of risk.
- Strong protections for AI and ADM transparency, including disclosure of both the existence of a system and a broad range of data, tools and processes used by the system.
- Mandatory "AI Registers."
- Mandatory, detailed and transparent AI or algorithmic impact assessments.
- Explicit compliance with the Charter and appropriate human rights legislation.
- Data standards.
- Access to meaningful remedies.
- Mandatory auditing and evaluation requirements.
- Independent oversight of both individual systems and government use of AI and ADM generally.

Finally, the LCO believes there must be broad participation in the design, development and deployment of these systems. Unequal access to information and participation in AI and algorithmic decision-making can significantly worsen existing biases and inequality. Broad participation must include technologists, policymakers, legal professionals and the communities who are likely to be most affected by this technology.

XV. HOW TO GET INVOLVED

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

- Learn about the project on the LCO website (***www.lco-cdo.org***);
- Contact us to ask about the project; or,
- Provide written submissions or comments on this report.

The LCO can be contacted at:

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

Email:	LawCommission@lco-cdo.org
Web:	www.lco-cdo.org
Twitter:	@LCO_CDO
Tel:	(416) 650-8406
Toll-free:	1 (866) 950-8406

[1] Canada, *Directive on Automated Decision-Making*, (2019) [Canada Federal Directive], online: **https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592#appA**.

[2] See generally, Law Commission of Ontario, *The Rise and Fall of Algorithms in American Criminal Justice: Lessons for Canada*, (October 2020) [LCO Criminal AI Issue Paper], online: **https://www.lco-cdo.org/wp-content/uploads/2020/10/Criminal-AI-Paper-Final-Oct-28-2020.pdf** at 20-40.

[3] Canada, *Algorithmic Impact Assessment*, (2019) [Canada Algorithmic Impact Assessment], online: **https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html**.

[4] Access Now, *Europe's Approach to Artificial Intelligence: How AI Strategy Is Evolving*, (2020) [Access Now AI Strategy], online: **https://www.accessnow.org/eu-trustworthy-ai-strategy-report/** at 8.

[5] Canada Federal Directive, ss. 1.1 and 1.2.

[6] LCO Criminal AI Issue Paper.

[7] Law Commission of Ontario, *AI, ADM and Government Decision-Making,* (Forthcoming) [LCO Civil AI Issue Paper].

[8] This paper is being written for the LCO by Jill Presser, a Toronto-based criminal lawyer and principle of Presser Barristers, and Kate Robertson, an associate at Markson Law and Research Fellow at The Citizen Lab (Munk School of Global Affairs and Public Policy, University of Toronto). Law Commission of Ontario, *Probabilistic Genotyping DNA Tools in Canadian Criminal Courts* (Forthcoming) [LCO Genotyping Issue Paper].

[9] For more information on the LCO's AI, ADM and the Justice System project see **https://www.lco-cdo.org/en/our-current-projects/ai-adm-and-the-justice-system/**.

[10] This is a multidisciplinary workshop organized by the LCO and the Ontario Digital Service, a branch of the provincial government's Treasury Board Secretariat. Law Commission of Ontario, *Legal Issues and Government AI Development: Workshop Repor*t, (March 2021) [LCO Government AI Workshop], online: **https://www.lco-cdo.org/wp-content/uploads/2021/03/LCO-Govt-AI-Workshop-Report-%E2%80%94-March-2021.pdf**.

[11] LCO Criminal AI Issue Paper.

[12] In December 2019, the LCO organized Canada's first multidisciplinary forum considering the use of AI and algorithms in regulatory investigations, government benefit determinations, and to support decision-making in the civil and administrative justice systems. This event brought together almost 40 policy makers, lawyers, jurists, technologists, academics, and community organizers to share experiences, discuss issues and consider law reform options in civil and administrative law applications. Read about this event **here**.

[13] In March 2019, the LCO organized Canada's first multidisciplinary forum on AI in Canada's criminal justice system. The event brought together more than 50 policymakers, Crown Attorneys, defence counsel, jurists, technologists, academics and community organizers to discuss predictive policing, algorithmic risk assessments, how to "litigate algorithms" and related human rights and due process issues. Material for this event is available **here**.

[14] LCO Government AI Workshop.

[15] See, for example, the discussion in the LCO's Criminal AI Issue Paper at 31-35.

[16] Treasury Board of Canada, "Responsible Artificial Intelligence in the Government Canada: Digital Disruption White Paper Series (10 April 2018), [Treasury Board White Paper], online: < **https://docs.google.com/document/d/1Sn-qBZUXEUG4dVk909eSg5qvfbpNlRhzIefWPtBwbxY/edit**> at 5-6.

[17] *Ibid.* ("…enthusiasm for AI in government has been high" at 23.)

[18] Engstrom, David Freeman and Ho, Daniel E. and Sharkey, Catherine M. and Cuéllar, Mariano-Florentino, Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies (February 1, 2020) [US Federal Administrative Agencies], online: **https://ssrn.com/abstract=3551505** at 6.

[19] *Ibid*.

[20] See, for example, "How AI Can be a Force For Good in Government", Feb 28, 2019, George Atalla, EY Consulting **https://www.ey.com/en_gl/consulting/how-ai-can-be-a-force-for-good-in-government**; "Ten Ways Data can Make Government Better", Harvard Kennedy School Ash Center **https://datasmart.ash.harvard.edu/news/article/ten-great-ways-data-can-make-government-better-1041**.

21 See, for example, *Transparency and Algorithmic Governance*, Administrative Law Review, Vol. 71, P. 1, 2019, Cary Coglianese and David Lehr and Sandra Gabriel Mayson, *Bias In, Bias Out* (September 28, 2018), 128 Yale Law Journal 2218 (2019), University of Georgia School of Law Legal Studies Research Paper No. 2018-35 [Mayson] at 2280, online: **https://ssrn.com/abstract=3257004**.

22 Sarah Picard-Fritshe et al, *Beyond the Algorithm: Pretrial Reform, Risk Assessment, and Racial Fairness*, Center on Court Innovation, (July 2019) [Pitcard-Fritshe], online: **https://www.courtinnovation.org/sites/default/files/media/document/2019/Beyond_The_Algorithm.pdf** at 3.

23 Australian Human Rights Commission, *Human Rights and Technology Discussion Paper,* (December 2019) [Australian Human Rights and Technology], online: **https://tech.humanrights.gov.au/sites/default/files/2019-12/TechRights_2019_DiscussionPaper.pdf** at 23.

24 This term comes from the title of a book by Cathy O'Neil, a former Wall Street data scientist and mathematician. Her 2016 book, *Weapons of Math Destruction*, popularized the idea that AI, algorithms and big data reinforce and worsen bias and discrimination in public and private sector decision-making.

25 Human Rights Watch, *Not In It For Justice,* (April 2017) [Human Rights Watch], online: **https://www.hrw.org/report/2017/04/11/not-it-justice/how-californias-pretrial-detention-and-bail-system-unfairly** at 8.

26 LCO Criminal AI Issue Paper at 20-23.

27 *Ibid* at 23-24.

28 *Ibid* at 24-26.

29 *Ibid* at 29-30.

30 *Ibid* at 31-35.

31 These examples will be discussed in detail in the LCO's third Issue Paper, *AI, ADM and Government Decision-Making*, which will be released in the spring of 2020.

32 US Federal Administrative Agencies at 6.

33 This table is compiled from several international surveys of government use of AI and ADM by governments, including AINow Institute, *Algorithmic Accountability Policy Toolkit*, (October 2018) [AINow Accountability Toolkit], online: **https://ainowinstitute.org/aap-toolkit.pdf**; US Federal Administrative Agencies; Michele Gilman, *Poverty Algorithms: A Poverty Lawyer's Guide to Fighting Automated Decision-Making Harms in Low-Income Communities,* Data and Society (September 2020), online: **https://datasociety.net/wp-content/uploads/2020/09/Poverty-Lawgorithms-20200915.pdf**; Australian Human Rights and Technology; and *Government Use of Artificial Intelligence in New Zealand: Final Report on Phase 1 of the NZ Law Foundation's AI and Law in NZ Project*, (Wellington, 2019) [NZ AI and Law], online: **https://www.cs.otago.ac.nz/research/ai/AI-Law/NZLF%20report.pdf**.

34 US Federal Administrative Agencies at 16.

35 *Ibid* at 17.

36 Jennifer Raso, "AI and Administrative Law" in *Artificial Intelligence and the Law in Canada,* eds. Teressa Scassa and Florian Martin-Bariteau, (Lexis-Nexis Canada) (2021).

37 See the current use surveys identified in note 33 above.

38 AINow Accountability Toolkit at 9.

39 LCO Criminal AI Issue Paper.

40 Kate Robertson, Cynthia Khoo and Yolanda Song, *To Surveil and Predict, A Human Rights Analysis of Algorithmic Policing in Canada*, Citizen Lab and International Human Rights Program, University of Toronto Faculty of Law, (September 2020) [Citizen Lab], online: **https://citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf**.

41 Petra Molnar and Lex Gill, *Bots at the Gate: A Human Rights Analysis of Automated Decision-making in Canada's Immigration and Refugee System,* (2018), online: **https://citizenlab.ca/2018/09/bots-at-the-gate-human-rights-analysis-automated-decision-making-in-canadas-immigration-refugee-system/**.

42 LCO Government AI Workshop.

43 Canada Federal Directive, ss. 1.1 and 1.2.

44 For an introduction to the range of AI definitions, history and the operation of AI and algorithmic predictive systems see NZ AI and Law at 5-19.

45 LCO Criminal AI Issue Paper at 29-30, 33.

46 Automated Decisions Systems Task Force, *Automated Decision Systems Task Force Report*, New York City, (November 2019) [NYC AI Task Force], online; **https://www1.nyc.gov/assets/adstaskforce/downloads/pdf/ADS-Report-11192019.pdf**.

47 Rashida Richardson, ed., *Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force*, AI Now Institute, December 4, 2019 [AINow Shadow Report], online: https:// ainowinstitute.org/ads-shadowreport-2019.html.

48 See Wendy Gillis, "Critics of new carding policy: "Destroy the data," *Toronto Star* November 17, 2016), online: **https://www.thestar.com/news/gta/2016/11/17/critics-of-new-carding-policy-destroy-the-data.html**.

49 See Donovan Vincent, "Sidewalk Labs' urban data trust is "problematic," says Ontario privacy commissioner," *Toronto Star,* (September 26, 2019), online: **https://www.thestar.com/news/gta/2019/09/26/sidewalk-labs-urban-data-trust-is-problematic-says-ontario-privacy-commissioner.html**.

50 US, Office of the President: *Executive Order on Maintaining American Leadership in Artificial Intelligence*, February 11, 2019, online: <**https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence**>.

51 *Ibid.*

52 US Office of Budget and Management, Acting Director in Coordination with the Directors of the Office of Science and Technology, the Domestic Policy Council, and the National Economic Council, "Memorandum for the Heads of Executive Departments and Agencies" (2020), online: < **https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf**>.

53 *Ibid* at 2.

54 US, Bill SIL20719, *A Bill to Provide for Data Accountability and Transparency,* 16th Cong, 2019-2020. Online: **https://www.banking.senate.gov/imo/media/doc/Brown%20-%20DATA%202020%20Discussion%20Draft.pdf**.

55 US, Bill HR 2231, Algorithmic Accountability Act of 2019, 116th Cong, 2019-2020.

56 Cory Booker, "Booker, Wyden, Clarke Introduce Bill Requiring Companies To Target Bias in Corporate Algorithms" (10 April 2019), online: **www.booker.senate.gov/news/press/booker-wyden-clarke-introduce-bill-requiring-companies-to-target-bias-in-corporate-algorithms#:~:text=The%20Algorithmic%20Accountability%20Act%20would,to%20new%20and%20existing%20systems**.

57 *Ibid,* ss. 3(b)(1) and 6.

58 *Ibid,* s 3(b)(1)(B).

59 *Ibid,* s 3(b)(1)(C).

60 *Ibid,* s 3(b)(1)(D).

61 *Ibid,* s 3(b)(2).

62 European High-Level Expert Group on Artificial Intelligence, "Ethics Guidelines for Trustworthy AI" (2019) [HLEG Guidelines], online: **https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top**.

63 *Ibid* at 2.

64 Note that this quote is on the Canada Federal Directive's webpage but does not appear to be included in the Directive itself. Online: **https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592#appC**.

65 NYC AI Task Force.

66 *Ibid* at 26. ("Some members [of the Taskforce] believed it was better that the definition continue to be broadly inclusive of possible tools and systems, and that limiting the scope of the definition could exclude tools or systems that might be considered relevant for additional agency assessment. Other members believed that including such a wide array of tools or systems could divert… attention from the specific types of technical tools and systems that the law was intended to address, and also that too expansive a definition would render the recommendations infeasible to implement.")

67 *Ibid.*

68 European High-Level Expert Group on Artificial Intelligence, "A Definition of AI: Main Capabilities and Disciplines" (2019), online: **https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=56341**.

69 See, for example, US, Bill S.847, *Commercial Facial Recognition Privacy Act of 2019*, 116th Cong, 2019-2020; *Transparency Guidelines for Data-Driven Technology in Government*, 2020, online: *Github* <**https://github.com/ongov/Transparency-Guidelines/tree/84557ccd16ba4c8615648532ac255254ba1e58ff**>, *Alpha Principles for the Ethical Use of AI and Data Driven Technologies in Ontario,* 2020, online: *Github* <**https://github.com/ongov/AI-Principles**>.; *Ontario's Open Data Directive, 2019,* March 16, 2020, online: *Government of Ontario*: <**https://www.ontario.ca/page/ontarios-open-data-directive**>; *Simpler, Faster, Better Services Act, 2019*, SO 2019, c 7, Sched 56, online: ontario.ca <**https://www.ontario.ca/laws/statute/19s07**>; and EU, OJ L 119, *General Data Protection Regulation,* 25 May 2018, online: gdpr-info.eu <**https://gdpr-info.eu/**>.

70 NYC AI Task Force at 19.

71 Canada Federal Directive, s.5.2.

72 See, generally, NZ AI and Law at 5-19.

73 Teresa Scassa, *Administrative Law and the Governance of Automated Decision-Making: A Critical Look at Canada's Directive on Automated Decision-Making* (October 30, 2020). Forthcoming, (2021) 54:1 University of British Columbia Law Review [Scassa], online: **https://ssrn.com/abstract=3722192** at 6-7.

74 Algorithmic Accountability Act, Preamble.

75 *Ibid,* s. 1(c).

76 Canada Federal Directive, s. 5.2.

77 Note, however, that the Directive could apply to certain aspects of policing done by the RCMP, and to certain decisions made by the Correctional Services Canada and the Parole Board of Canada.

78 Canada Federal Directive, s. 5.4.

79 *Ibid*, s 9.1.1.

80 *Ibid,* s 9.2

81 *Ibid*, s. 5.1.

82 *Ibid,* s. 5.3.

83 Council of Europe Ad Hoc Committee on Artificial Intelligence (CAHAI), "Feasibility Study" (17 December 2020), online: **http://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da** [CAHAI Feasibility Study].

84 Citizen Lab at 62-63.

85 See Citizen Lab and Canadian Civil Liberties Association, Facial Recognition (updated February 3, 2021), online: **https://ccla.org/facial-recognition/**.

86 *Ibid*.

87 San Francisco, Administrative Code – Acquisition of Surveillance Technology, File No. 190110, online: **https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A**.

88 Boston City Council, Report of Committee Chair (24 June 2020), online: **www.documentcloud.org/documents/6956465-Boston-City-Council-face-surveillance-ban.html**.

89 US, AB-1215, "Law Enforcement: facial recognition and other biometric surveillance" (10 September 2019), online: **https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB1215**.

90 US, *The Facial Recognition and Biometric Technology Moratorium Act,* 116th Cong., 2nd Sess, online: **https://drive.google.com/file/d/1gkTcjFtieMQdsQ01dmDa49B6HY9ZyKr8/view**.

91 Access Now AI Strategy at 26.

92 Algorithm Watch, AI Ethics Guidelines Global Inventory, online at: **https://inventory.algorithmwatch.org/about**. The Canadian Guidelines listed include three documents from the Government of Canada (including the Directive on Automated Decision-Making), the Montreal Declaration, an advisory statement from the National Research Council and a White Paper from the Centre for International Governance Innovation.

93 HLEG Guidelines.

94 *Ibid* at 5.

95 *Ibid* at 3-4.

96 *Ibid* at 3.

97 CAHAI Feasibility Study.

98 Information Technology Industry Council, "AI Policy Principles: Executive Summary", online: **https://www.itic.org/public-policy/ITIAIPolicyPrinciplesFINAL.pdf** at 5.

99 *Ibid* at 1.

100 Access Now, *Mapping Regulatory Proposals for Artificial Intelligence in Europe,* (2018) [Access Now Mapping Report], online: **https://www.accessnow.org/mapping-artificial-intelligence-strategies-in-europe/** at 32.

101 See generally, Thomas Metzinger, "Ethics Washing Made in Europe" (Aug. 4, 2019), online at: **https://www.tagesspiegel.de/politik/eu-guidelines-ethics-washing-made-in-europe/24195496.html**.

102 H.B. 1655, S.B. 5527, *Establishing guidelines for government procurement and use of automated decision systems in order to protect consumers, improve transparency, and create more market predictability*, (Washington 2019) [Washington State 1655], online: **https://app.leg.wa.gov/billsummary?BillNumber=1655&Chamber=House&Year=2019**.

103 *Ibid.*

104 Scassa at 11.

105 Statement by UN High Commissioner for Human Rights Michelle Bachelet, "Smart mix of measures needed to regulate new technologies" (April 24, 2019) online: **https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24509**.

106 Government of Canada, Directive on Service and Digital, online: **https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32601**.

107 UK, *Guidelines for AI Procurement* (8 June 2020), online: gov.uk <**https://www.gov.uk/government/publications/guidelines-for-ai-procurement**>.

108 Institute of Electrical and Electronics Engineers, *Ethically Aligned Design* (1st Edition, 2019) [IEEE], online: **https://standards.ieee.org/industry-connections/ec/autonomous-systems.html**.

109 See generally, LCO Criminal AI Issue Paper at 31-35.

110 The federal Directive anticipates many of these issues. For example, sections 6.3.1 and 6.3.3 require testing for intended biases and to ensure data is relevant, accurate, up to date and collected in accordance with privacy legislation. Canada Federal Directive, ss. 6.3.1 and 6.3.3.

111 LCO Criminal AI Issue Paper at 40.

112 *Ibid.*

113 European Commission, *White Paper on Artificial Intelligence – A European Approach to Excellence and Trust,* 2020) [European Commission White Paper], online: **https://ec.europa.eu/futurium/en/node/8438**.

114 *Ibid* at 22-23.

115 Cited in Access Now AI Strategy at 23.

116 *Ibid.*

117 *Ibid* at 34.

118 Washington State 1655, s. 3.

119 *Ibid*, s. 6.

120 Canada Algorithmic Impact Assessment.

121 Canada Federal Directive, ss. 6.1.1 and 6.1.2.

122 Scassa.

123 Jennifer Raso, "AI and Administrative Law" in *Artificial Intelligence and the Law in Canada,* eds. Teressa Scassa and Florian Martin-Bariteau, (Lexis-Nexis Canada) (2021).

124 Canada Federal Directive*, s. 6.*

125 *Ibid*, s. 6.3.1.

126 *Ibid*, s. 6.3.2.

127 *Ibid*, s. 6.4.

128 Access Now Mapping Report at 13.

129 Deven Desai and Joshua Kroll, *Trust But Verify: A Guide to Algorithms and the Law* (April 27, 2017). Harvard Journal of Law & Technology, Georgia Tech Scheller College of Business Research Paper No. 17-19, online: **https://ssrn.com/abstract=2959472** at 8.

130 **https://data.ontario.ca/group/ about/artificial-intelligence-and-algorithms**.

131 See generally, Khari Johnson, "Amsterdam and Helsinki launch algorithm registries to bring

transparency to public deployments of AI." (September 28, 2020); online: **https://ai.hel.fi/en/get-to-know-ai-register/**.

132 **https://ai.hel.fi/en/get-to-know-ai-register/**.

133 **https://data.ontario.ca/group/artificial-intelligence-and-algorithms**.

134 Canada Federal Directive, s 6.2.1.

135 *Ibid,* s 6.2.2.

136 *Ibid*, s 6.2.3.

137 *Ibid*, Appendix C — Notice.

138 Government of Ontario, *Open Data Directive, 2019*. Online: **https://www.ontario.ca/page/ontarios-open-data-directive#section-4**.

139 **https://data.ontario.ca/**.

140 LCO Criminal AI Issue Paper at 32.

141 Algorithmic Accountability Act, s. 2(7).

142 Dillon Reisman, Jason Schultz, Kate Crawford and Meredith Whittaker, *Algorithmic Impact Assessments: A Practical Framework for Public Agency Accountability,* AI Now Institute (April 2018) [AI Now Impact Assessment], online: **https://ainowinstitute.org/aiareport2018.pdf**.

143 HLEG Assessment List at 26-31.

144 Canada Federal Directive, s. 6.1.

145 Canada Algorithmic Impact Assessment.

146 Washington State 1655, ss. 2(3) and 5(2).

147 Washington State House Bill 1655 Substitute Bill, [Washington House Substitute 1655], online: **http://lawfilesext.leg.wa.gov/Biennium/2019-20/Htm/Bills/House%20Bills/1655-S.htm**, s. 3.

148 *Ibid.*

149 See generally, Taylor R. Moore, *Trade Secrets and Algorithms as Barriers to Social Justice*, Center for Democracy and Technology (August 2017), online: **https://cdt.org/wp-content/uploads/2017/08/2017-07-31-Trade-Secret-Algorithms-as-Barriers-to-Social-Justice.pdf**.

150 *State v. Loomis,* 881 N.W.2d 749 (Wisc. 2016).

151 For a good discussion of *State v. Loomis*, see Berkman Klein Early Lessons.

152 UK, *Guidelines for AI Procurement* (8 June 2020), online: gov.uk <**https://www.gov.uk/government/publications/guidelines-for-ai-procurement**>.

153 Canada Federal Directive, ss. 6.2.6 and 6.2.7.

154 Alice Xiang and Daniel Ho, Partnership on AI, *From Affirmative Action to Affirmative Algorithms: The Legal Challenges Threatening Algorithmic Fairness,* (November 9, 2020), online: **https://www.partnershiponai.org/affirmativealgorithms/**.

155 Human Rights Watch at 8.

156 See generally, LCO Criminal AI Issue Paper at 20-26. Note, however, the importance of understanding the differences and distinctions between how lawyers and technologists understand bias. See generally, Alice Xiang, Reconciling Legal and Technical Approaches to Algorithmic Bias (July 13, 2020). Tennessee Law Review, Vol. 88, No. 3, 2021,online: **https://ssrn.com/abstract=3650635**.

157 Ontario, *Promoting Public Trust and Confidence in Ontario's Data Economy* (n.d.), online: engage.ontario.ca <**https://engage.ontario.ca/sites/default/files/discussion_paper1_eng_final.pdf**> 2019.

158 *Ibid*.

159 *Ibid* at 6.

160 *Ibid* at 6-7.

161 Washington State 1655, s. 4(1).

162 *Ibid,* s. 5(2)(g).

163 Canada Federal Directive, s. 4.1

164 See note 64.

165 Canada Federal Directive, s. 4.2.1.

166 *Ibid*, s. 6.3.8.

167 Washington State 1655, s.5(2)(b).

168 LCO Criminal AI Issue Paper at 27-35.

169 HLEG Assessment List at 16-17.

170 Canada Directive on Service and Digital, s. 4.5.3.

171 Washington State 1655, s. 4(3)(b).

172 US, Bill S.2177, *FUTURE of Artificial Intelligence Act of 2017*, 2017-2018, Reg Sess, 115th Cong, online: < https://www.congress.gov/bill/115th-congress/senate-bill/2217>.

173 US, Bill SIL20719, *A Bill to Provide for Data Accountability and Transparency,* 16th Cong, 2019-2020, s 206.

174 *Ibid*, s. 105(a).

175 *Ibid* s. 104(a).

176 Canada Federal Directive, Appendix C, Impact Level Requirements, "Testing".

177 *Ibid,* Impact Level Requirements, "Peer Review".

178 Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008) [Citron], online: **https://openscholarship.wustl.edu/law_lawreview/vol85/iss6/2**. See also, Danielle K. Citron & Ryan Calo, *The Automated Administrative State: A Crisis of Legitimacy*, (2020), online: **https://scholarship.law.bu.edu/faculty_scholarship/838**.

179 Citron at 1252.

180 Access Now Mapping at 42.

181 *Ibid*, s. 4.2.1.

182 Scassa at 2.

183 Directive. 6.2.1.

184 *Ibid,* s. 6.2.3.

185 *Ibid,* s. 6.4.1.

186 *Ibid,* Appendix A – Definitions.

187 Canada Algorithmic Impact Assessment.

188 Scassa at 28.

189 See generally Scassa at 17-27 and Raso at 7-14. Professor Raso writes, for example, that with exception of Directive, "…Canadian administrative law – common law, statutes, soft law and beyond – largely overlooks algorithmically-assisted decision-making" and that "…administrative law is more gap than law when it comes to algorithmically-driven decision-making." Raso at 6 and 16.

190 According to Professor Raso. "[t]hus far, this degree of transparency is only partially provided in the federal Directive." Raso at 8.

191 *Ibid* at 9.

192 Scassa at 24-26.

193 *Ibid* at 27.

194 LCO Criminal AI Paper at 33-34.

195 Partnership on AI (PAI), *Report on Algorithmic Risk Assessment Tools in the U.S. Criminal Justice System*, (April 2019) [PAI] at 7, online: **https://www.partnershiponai.org/report-on-machine-learning-in-risk-assessment-tools-in-the-u-s-criminal-justice-system/** at 29, 31.

196 NA AI and the Law at 62.

197 *Ibid* at 62-73.

198 Bill 237, *The Technology Advisory Council Act* 4th Sess, 41st Legislature, Manitoba, 2018-2019, s 3(1).

199 CIFAR, *Rebooting Regulation: Exploring the Future of AI Policy in Canada* (May 2019), at 8, online: **https://www.cifar.ca/docs/default-source/ai-reports/rebooting-regulation-exploring-the-future-of-ai-policy-in-canada.pdf?sfvrsn=616c04f3_8**.

200 The City of New York Office of the Mayor, *Executive Order No 50, Establishing an Algorithms Management and Policy Officer*, 2019, online: < **https://www1.nyc.gov/assets/home/downloads/pdf/executive-orders/2019/eo-50.pdf?mc_cid=f74d21dc3f&mc_eid=c06bcd901c** > at 1.

201 US, Bill SIL20719, *A Bill to Provide for Data Accountability and Transparency,* 16th Cong, 2019-2020.

202 Washington State 1655, s.3.

203 Canada Federal Directive, s.6.4.1.

204 Scassa at 11.

205 Washington State 1655, s. 4(1)(c).

206 *Ibid,* s.(6).

207 LCO Criminal AI Issue Paper at 35-37.

208 Ibid at 36-37. Footnotes omitted.

209 *Ibid*.