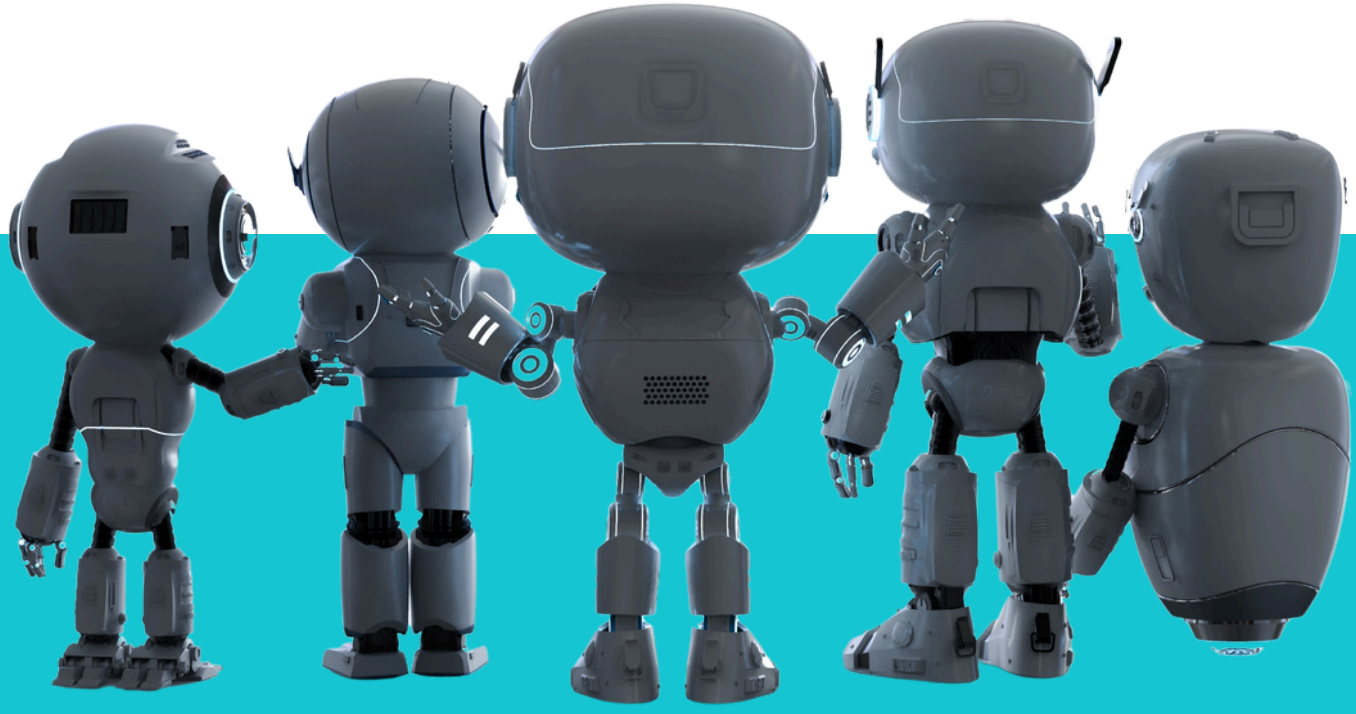
Engage.

AI IN MOTION

Chapter 1: What's up with AI Policy?



Written By

Justin Nakao

Edited & Designed by:

Dael Vasquez, Anjelica Ramsewack, Anastasia Podlesnykh

@engagefdn

general@engagefdn.com

https://www.engagefdn.com/

INTRODUCTION

America has long been the policy leader for nations across the world. With the advent of artificial intelligence (AI), the United States aims to continue its legacy of pioneering breakthrough policies for other countries to adopt. Executive Order (EO) 14110, also called the **"Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence"**, was signed on the 30th of October 2023 by United States President Joe Biden is a key step for AI policy and adoption.

Outlining the policy's purpose, section 2 of the EO "Policy and Principles" lays out the following broad, specifically:

1. AI must be safe and secure
2. AI must promote responsible innovation, competition, and collaboration;
3. The responsible development and use of AI require a commitment to supporting American workers;
4. AI policies must be consistent with the Biden administration's dedication to advancing equity and civil rights;
5. The interests of americans who increasingly use, interact with, or purchase AI and AI-enabled products in their daily lives must be protected;
6. Americans' privacy and civil liberties must be protected as AI continues advancing;
7. Manage the risks from the Federal Government's own use of AI and increase its internal capacity to regulate, govern, and support responsible use of AI;
8. The Federal Government should lead the way to global societal, economic, and technological progress.

In addition to the insights we can gather from section 2 of the EO, the document offers additional details into the key policy impacted by AI's influence, such as:

- geopolitics including national security, defence and global leadership;
- civil rights such as privacy and equality;
- economic competition, protection, and promoting innovation;
- human capital including immigration and labour;
- and Government integration.

As an American policy, Canadians may be wondering why the EO deserves any attention. In response, we contend that the policy's influence will have far reaching effects on Canada in this report. However, to provide a holistic perspective on the EO and its effects, we delve into the policy's major needs for improvement in a complementary publication.

Given the far reaching impacts of AI, this report will explain the ways in which artificial intelligence will affect the five policy sectors listed above and outline the actions being taken to address related challenges and opportunities. In doing so, the report provides high level key policy insights on the EO, grounding readers in the policy's major implications.

POLICY INSIGHTS

Geopolitics and AI

The EO highlights the potential risks and benefits that AI presents to a state's national security and defence. The first set of risks are raised in sections 4.1 and 4.4. They include the potential capabilities of AI to cause harm in the following domains: chemical, biological, radiological, nuclear (CBRN), cyber, critical infrastructure, and energy-security threats or hazards. Further risks include synthetic content highlighted under section 4.5, referring to "information, such as images, videos, audio clips, and text, that has been significantly modified or generated by algorithms, including by AI". The risk being the spread of misinformation and the inability to distinguish between organic and synthetic content.

Policies aimed at preventing and mitigating these threats include creating tools to evaluate an AI model's potential for danger and the safe use and control of dual-use foundation models; dual-use referring to:

"an AI model that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters."

The regulation of dual-use models is further elaborated upon in section 4.2 with the establishment of a reporting structure for companies developing these models. Reporting would require ongoing disclosures to the U.S. federal government on the acquisition, development, or possession of potentially large-scale computing clusters along with reporting the existence, location, and total computing power available for these clusters. Infrastructure as a Service providers must also report the identity of any foreign cluster buyer, including those buying from resellers, for verification. With regards to synthetic content risk, this can be mitigated through digital content authentication and synthetic content detection measures.

Section 4.7 aims to ensure that federal data is not used maliciously by AI, especially against CBRN threats by developing guidelines for performing security reviews to identify and manage the potential security risks of releasing Federal data for AI training.

Section 4.8 seeks to create the national security policy paradigm related to AI by addressing AI as a component in various national security systems or for military and intelligence purposes. The section also responds to the potential use of AI systems by adversaries and other foreign actors.

With regards to the policy's benefits, U.S. AI policy recognizes the value of integrating AI into the national security framework. EO section 4.3 highlights the value of AI in protecting critical infrastructure and to improve U.S. cyber defences while also identifying the threat AI may pose to vulnerabilities.

Under section 11, the U.S. outlines its plan to strengthen its role as policy/regulatory power on the international stage in regards to AI. This includes taking leadership outside of the military and intelligence spaces, expanding engagements with international allies and partners to bolster their understanding of existing and planned AI-related guidance and policies of the United States. This also involves leading the way to establish a strong international framework for managing the risks and harnessing the benefits of AI through "encouraging international allies and partners to support voluntary commitments similar to those that United States companies have made". This will be done through coordination with key partners and allies by achieving consensus around AI-related standards.

Civil Rights, Equality and Privacy and AI

Section 7 of the EO "Advancing Equity and Civil Rights" has 3 subsections that pertain towards civil rights, with section 8 and 9 including privacy rights. Section 7.1 covers the role of AI in the criminal justice system - aimed at addressing unlawful discrimination and other harms that may be exacerbated by AI - and increasing the number of relevant experts among law enforcement offices.

The role of AI in the criminal justice system involves:

- sentencing;
- parole, supervised release, and probation;
- bail, pretrial release, and pretrial detention;
- risk assessments, including pretrial, earned time, and early release or transfer to home-confinement determinations;
- police surveillance;
- crime forecasting and predictive policing, including the ingestion of historical crime data into AI systems to predict high-density "hot spots";
- prison-management tools; and
- forensic analysis;

Targeting these areas ensures law enforcement and criminal justice can bolster efficiency and accuracy, while also protecting privacy, civil rights, and civil liberties. Consequently, section 7.1 calls for the implementation and enforcement of existing Federal laws to address AI violations including algorithmic discrimination as vehicles to meet civil rights objectives.

Section 7.2 focuses on AI in relation to government benefits and programs that promote the equitable administration of public benefits. The policy is intended to prevent unlawful discrimination and other harms that result from uses of AI in federal programs. This is also applied to sub-federal governments which aim to adopt automated or algorithmic systems, as they are required to ensure equitable outcomes by prompting the:

"assessment of access to benefits by qualified recipients; notice to recipients about the presence of such systems; regular evaluation to detect unjust denials; processes to retain appropriate levels of discretion of expert agency staff; processes to appeal denials to human reviewers."

Section 7.3 focuses on ensuring civil rights protection in economic processes including hiring, housing market access, retail financial markets, and protecting people with disabilities from risks "including unequal treatment from the use of biometric data like gaze direction, eye tracking, gait analysis, and hand motions". To ensure the civil rights of citizens in hiring, the EO offers guidance to federal contractors against discrimination when implementing AI enabled hiring tools. With regards to housing, the EO authorises the Director of the Federal Housing Finance Agency and the Director of the Consumer Financial Protection Bureau to ensure that AI tools within their areas of jurisdiction comply with federal law.

This is done by ensuring that models avoid bias against protected groups and evaluating automated collateral-valuation and appraisal processes for bias. AI housing policy also sees that tenant screening systems are evaluated for violations of the Fair Housing Act and other laws by ensuring that data or records do not lead to discriminatory outcomes. People with disabilities will be protected by evaluating the "risks and benefits of AI in using biometric data as an input; and to provide people with disabilities access to information and communication technology and transportation services".

Lastly, privacy is governed under sections 8 and section 9. Section 8 addresses AI-related privacy risks in relation to American consumer privacy. The EO aims to clarify existing regulations and guidance that apply to third party AI, including the transparency of AI models. Section 9 aims to "mitigate privacy risks potentially exacerbated by AI - including by AI's facilitation of the collection or use of information about individuals, or the making of inferences about individuals".

This is done in 3 steps:

01 Identifying Commercially Available Information (CAI) procured by agencies, particularly personally identifiable information (PII);

02 Evaluating risk posed by existing policies on CAI and PII breaches;

03 Creating guidelines that limit the improper access of CAI and PII.

Economic Competition, Protection, and Innovation and AI

AI represents a massive shift in the economy and section 5 of the EO reflects this by focusing on the promotion and innovation of competition across industries. Section 8 focuses on consumer protections and users such as patients, passengers, and students.

Section 5.2 sets out the policy designs for promoting innovation. First it sets out to launch a pilot program that will develop the infrastructure, governance mechanisms, and user interfaces to initialise the integration of distributed computational, data, model, and training resources to support AI-related R&D. Secondly it requires the publishing of guidance to "patent examiners and applicants addressing inventorship and the use of AI, including the scope of protection for works produced using AI and the treatment of copyrighted works in AI training". This is relevant for protecting intellectual property (IP) and mitigating AI-enabled IP theft. Third, the section promotes AI innovation in the area of healthcare to improve the welfare of patients and workers in the industry.

Section 5.3 focuses on promoting competition through 3 measures. First, competition will be protected through antitrust measures: "addressing risks arising from concentrated control of key inputs, taking steps to stop unlawful collusion and prevent dominant firms from disadvantaging competitors, and working to provide new opportunities for small businesses and entrepreneurs". Second, ensuring that AI technologies remain available to competing entities and promoting competition and innovation in the semiconductor industry. Third, supporting small businesses, innovating, and commercialising AI by providing "support, technical assistance, and other resources to...innovate, commercialize, scale, or otherwise advance the development of AI", while also supporting entities that educate and train AI human capital alongside subsidising expenses of small businesses related to the adoption of AI.

Protections extended by section 8 include requiring regulatory agencies to use their authority to protect American consumers from fraud, discrimination, and threats to privacy and other risks that may arise from the use of AI. Specifically, by emphasising or clarifying where existing regulations and guidance apply to AI.

With regards to telecommunications, 3 objectives stand out:

01 Recognizing the potential for AI to increase the efficiency of and operations with federal and non-federal spectrums (radio and signals) and expanding opportunities for sharing the non-Federal spectrum;

02 Improving network security, resilience, and interoperability using next-generation technologies that incorporate AI;

03 Increasing efforts through both legislation and technology to combat unwanted robot calls and texts that may be worsened by AI, and to deploy AI technologies that better serve consumers by blocking these communications.

Lastly, across the health, transportation, and education sectors, the EO calls for the development of "a strategic plan that includes policies and frameworks — possibly including regulatory action, as appropriate — on responsible deployment and use of AI and AI-enabled technologies".

Human Capital and AI

AI represents a challenge but also an opportunity for many people in the workforce. The EO has policy objectives to ensure protections for workers, this section also covers the AI related opportunities for prospective immigrants.

Section 5.1 aims to attract and retain AI talent in the United States. It aims to attract talent by streamlining processing times of visa petitions and applications for noncitizens who wish to work in AI and related technologies. The policy also considers "initiating a rulemaking to establish new criteria to designate countries and skills on the Department of State's Exchange Visitor Skills List", allowing a 2-year residency to foreigners with skills critical to AI projects. Additionally, the section considers creating a program to identify and attract top talent in AI and related technologies from universities, research institutions, and private sector overseas. Under section 5.2, the U.S. aims to train 500 new researchers by 2025 capable of meeting the rising demand for AI talent through a new pilot program. Another domestic human capital initiative is the hosting of two 3-month nationwide AI Tech Sprint competitions that provide "participants access to technical assistance, mentorship opportunities, individualised expert feedback on products under development, potential contract opportunities, and other programming and resources".

Section 6 aims to identify the effects of AI on the labour market and assess which federal programs can best assist displaced workers. The section also aims to strengthen and expand education and training opportunities related to AI. Additionally, it stands to develop and publish principles and best practices for employers to mitigate the AI related harm against employees while also maximising the integration of AI into their operations. Lastly, as it relates to domestic human capital, the EO "prioritise[s] available resources to support AI-related education and AI-related workforce development through existing programs, and shall use appropriate fellowship programs and awards for these purposes".

Within the Federal government itself, section 10.2 aims to attract AI talent to the government while identifying priority mission areas for AI talent recruitment. This involves identifying and spreading the best practices for agencies to hire, retain, and train AI talent. This AI talent surge in the Federal government requires the increasing capacity for AI related talent such as data scientists alongside those hiring personnel needed to formulate the AI hiring strategy and get them to critical priority areas. This initiative will be launched alongside programs aimed at "increas[ing] the availability and use of AI training and familiarisation programs for employees, managers, and leadership in technology as well as relevant policy, managerial, procurement, regulatory, ethical, governance, and legal fields".

Government Intergration and AI

Section 10 outlines the U.S. federal government's plans to coordinate the use of AI across the public service. First, the government seeks to create an "interagency council to coordinate the development and use of AI in agencies' programs and operations". Second, the government will develop a method of tracking and accessing the progress and ability of agencies to integrate and use AI, that manages risk and complies with federal policy and law. Third, the government plans to limit access to "specific generative AI services based on specific risk assessments", while also establishing guidelines on the use of generative AI. This is aimed at allowing the use of AI for experimentation and routine tasks that carry a low risk of impacting Americans' rights, while also providing government workers access to secure and reliable generative AI.

Lastly, the government aims to acquire specific types of AI services and products "such as through the creation of a resource guide or other tools to assist the acquisition workforce. Specified types of AI capabilities shall include generative AI and specialised computing infrastructure." This also involves bolstering the Federal government's human capital across its institutions and workforce including addressing gaps in AI talent for national defence.

Conclusion

In conclusion, Executive Order 14110, heralds a pivotal moment in U.S. AI policy. The EO, titled "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," charts a comprehensive roadmap across critical sectors.

In geopolitics, the EO addresses national security concerns, outlining measures to mitigate risks associated with AI, such as dual-use foundation models and synthetic content. Simultaneously, it acknowledges the potential benefits of integrating AI into national security frameworks, affirming the U.S.'s commitment to global leadership in AI standards.

Civil rights feature prominently, with the EO targeting algorithmic discrimination in the criminal justice system and ensuring equitable access to government benefits. Privacy protections are underscored, emphasising transparency in AI models to safeguard individual rights.

Economic competition and innovation are central, with the EO promoting competition, protecting consumers, and fostering innovation. Antitrust actions and measures to ensure accessibility to AI technologies are highlighted, alongside support for small businesses in AI innovation.

Human capital initiatives aim to attract and retain AI talent, streamlining visa processes and investing in domestic education and training programs. The EO also addresses labor market impacts, supporting displaced workers and integrating AI-related education into existing programs.

Government integration is a priority, with plans to coordinate AI development across federal agencies. The establishment of an interagency council, progress monitoring, and access regulation for generative AI services are key features.

Overall, the EO presents a comprehensive strategy, balancing the opportunities and challenges of AI while reaffirming U.S. leadership in setting global AI standards. It signals a proactive stance towards AI policy, reflecting a nuanced understanding of AI's multifaceted impact across diverse sectors.