POWERED BY
Institute for
Citizen-Centred
Service

Artificial Intelligence in Government: Privacy and Human Rights Implications

- Government Applications
- Privacy and Human Rights Implications
- Examples of AI Challenges
- Strategies for Responsible Use

Image Source: bizlibrary

JOINT COUNCILS' EXECUTIVE MONTHLY REPORT

Developed by the Research Committee

September 2021

1. Introduction

The adoption of Artificial Intelligence (AI) in the Canadian public sector is expanding as the application of these tools and techniques continues to evolve.[1] Governments are embracing AI technologies to support a range of activities, including contributing to public policy objectives and assisting public interactions with government. These technologies also have the potential to help government transform vital programs and services to better serve clients, while also saving time and money.[2]

Due to the growth of the internet and mobile technology, clients are providing government organizations massive amounts of personalized data. AI tools are able to analyze complex mathematical algorithms and generate meaningful and actionable insights to support government decision-making.

Despite the opportunities for efficiency and effectiveness, the role of AI in government policy and service delivery raises concerns regarding client privacy and human rights. According to Brookings, **"as artificial intelligence evolves, it magnifies the ability to use personal information in ways that can intrude on privacy interests by raising analysis of personal information to new levels of power and speed"**.[3]

The use of AI in government must address these concerns and focus on protecting privacy and human rights to build and maintain trust among clients.

[1, 2.] Artificial Intelligence Policy and Funding in Canada
[3, 5.] Protecting privacy in an AI-driven world
[4.] COVID-19 and privacy: artificial intelligence and contact tracing in combatting the pandemic

Why is this Report Important?

- The implementation of AI accelerated across the public sector during the COVID-19 pandemic ("the pandemic")[4] and Governments are leveraging AI in a variety of ways. For example, identifying and tracking the spread of the virus, and implementing chatbots (such as virtual assistants) to provide information to the public.
- The pandemic increased client reliance on technology to engage with government. As a result, there is growing public concern around personal privacy and the lack of control over how data is used. Governments will need to get ahead of these concerns in order to realize the full potential of AI technologies.[5]
- In early 2019, the Joint Council's Research Committee published a report titled, *Artificial Intelligence in the Public Sector.* The report explored the different types of AI and how government will use the technology in the future. The focus of this report will be to highlight the privacy and human rights implications of AI use in government.

What is Covered in this Executive Report?

This report includes the following:

- Introduction
- Government Applications of AI
- Privacy and Human Rights Implications
- Examples of AI Challenges
- Strategies to Ensure the Responsible Use of AI in Government

2. Government Applications of AI

According to the Organisation for Economic Co-operation and Development (OECD), the potential benefits of government's use of AI includes:[6]

1. Reducing organizational costs
2. Improving operational efficiency and decision-making
3. Enhancing communication and engagement with clients
4. Improving the speed and quality of public services

Applications of AI in government are broad and growing. The following are some examples of how AI is currently used in the public sector:

Examples of AI Applications in the Public Sector

Ontario

The Ontario government (in partnership with various organizations) uses AI to detect the number of vehicles driving in high occupancy toll lanes on provincial roads.[7] In March 2021, Ontario published the draft *Artificial Intelligence (AI) Guidance Framework*. This Framework outlines how Ontario plans to "facilitate clear, transparent and ethical use of AI". The document also outlines the communication and management of the risks and benefits of using data-enhanced technologies in government processes, programs and services.

Government of Canada

Employment and Social Development Canada (ESDC) developed a prototype for the Passport Chatbot.[8] The prototype is currently being tested on Canada.ca. The Passport Chatbot aims to support Canadian Citizens with passport services by answering frequently asked questions regarding (only domestic) passport services.

British Columbia

The City of Surrey uses AI to support the delivery of municipal services to residents. The City launched a pilot program of AI research assistants on the MySurrey mobile app to help residents navigate through municipal infrastructure.[9] Residents using this app are now able to type out or say question(s) related to municipal services, and the app will immediately search through thousands of webpages to provide the correct answer.

United States

Since the start of the COVID-19 pandemic, many individuals experienced a decline in their mental wellness. This led to a dramatic increase in the use of telehealth services. In the US, some government organizations have turned to AI to broaden access to and availability of mental health services. AI-powered mental health chatbots and virtual assistants are now offered on smartphone apps (i.e. Woebot and Moodkits). These apps aim to help clients with mental health concerns (i.e. stress and anxiety).[10]

[6] Hello, World: Artificial intelligence and its use in the public sector
[7] IPC Comments on the Ontario Government's Consultation on Ontario's Trustworthy Artificial Intelligence (AI) Framework
[8] Terms of Use for Passport Chatbot
[9] Surrey uses AI to deliver city services to residents
[10] What Role Could Artificial Intelligence Play in Mental Healthcare?

3. Privacy Implications

As investments of AI in government continues to evolve and reshape operations, data privacy concerns are also rising. The adoption of AI accelerated during the COVID-19 pandemic, however many leaders are concerned that AI deployments are moving too fast, according to a KPMG survey – *Thriving in an AI World*.[11] The following highlights some of the key considerations prompted by AI in relation to data privacy.

Personal Information

- As the amount of available data increases, AI technologies are improving how data is processed and analyzed.
- There is an increasing concern from clients regarding the collection of personal information. Specifically, if an individual's identity can be ascertained from that information.[12]

Collection, Purpose and Use

- Clients may be unaware of how some organizations are collecting and processing a vast amount of user data in their AI-based systems.
- There is growing concern regarding how personal data will be used, or if it will be sold without knowledge or consent.[13]

Transparency and Consent

- Data privacy rests on the ability for clients to exercise choice regarding the data organizations have about them and what is done with it. However, the complexity around AI is that processes and use may be unclear to clients. This makes truly informed and meaningful consent challenging.[14]
- For example, deep learning techniques can pose challenges to transparency. Providing an explanation about how conclusions are drawn may be difficult, even for those developing the algorithms. As a result, organizations may struggle to be transparent in their AI practices, or to obtain consent, if they cannot communicate the processes to clients.

Accountability and Governance

- Governance and oversight in data privacy laws ensures appropriate structures are in place to prevent a power imbalance between clients and government. This relies on regulators ensuring personal data is handled appropriately.
- AI technology is not confined to one jurisdiction, this poses challenges to create and maintain good privacy practices and governance across borders.
- Determining who owns the data, where it is stored and who has responsibility for it is a complex task for regulators.[15]

[11] Thriving in an AI World

[12] Privacy Issues of AI

[13, 14] Artificial intelligence (AI) and the great privacy challenge

[15] ARTIFICIAL INTELLIGENCE AND PRIVACY – ISSUES AND CHALLENGES

4. Human Rights Implications

The impact of AI on human rights is one of the most crucial factors driving the debate around government's use of this evolving technology. The benefits of improving government decision-making based on mathematical calculations generated by AI capabilities can be valuable across sectors. However, human rights experts advise that relying too heavily on AI, without addressing human rights concerns, can negatively impact clients by increasing the risk of perpetrating injustices and restricting the rights of clients.[16] The harms related to the use of AI often disproportionately impact marginalized populations. The following highlights some of the key considerations of AI in relation to human rights.

Privacy and Data Protection

○ Privacy is a fundamental right that is essential to human dignity. Data collection using AI systems may interfere with rights to privacy and data protection. The data analyzed may reveal private information about individuals (i.e. age, gender, occupation, marital status, and location).

○ If the AI systems used to process data are not transparent or accountable, key elements of the right to data protection and privacy are violated.[17]

Discrimination

○ AI systems are designed to sort and filter (i.e. rank search results or categorize people into buckets). This discrimination can interfere with human rights when it treats different groups of people differently.

○ Discrimination often results in bias decision-making. The use of AI in some systems can perpetuate historical injustice in key areas such as prison sentencing, loan applications, and service delivery.[18]

Unemployment

○ Automation has resulted in job loss in various sectors, and it is predicted that AI will accelerate this trend. The role of AI in the automation of jobs may prevent some individuals from accessing the labor market and finding employment.[19]

○ Job automation may result in a range of challenges that governments will have to address to ensure an adequate standard of living.

Surveillance

○ Concerns regarding the potential use of AI for surveillance purposes is increasing. AI systems have the capability to combine data from satellite imagery, facial recognition-powered cameras, and cellphone location information. AI can provide a detailed picture of an individual's movements, as well as predict future location(s).[20]

○ Concerns are also rising around the use of AI to enforce social control during the current pandemic.

16. Safeguarding human rights in the era of artificial intelligence
17. Updating Canada's Privacy Act for Artificial Intelligence
18. HUMAN RIGHTS IN THE AGE OF ARTIFICIAL INTELLIGENCE
19. The Social Impact of Artificial Intelligence and Data Privacy Issues
20. Protecting privacy in an AI-driven world

5. Recent Examples of AI Challenges

The following are some examples of AI challenges that emerge as a result of unaddressed privacy and human rights considerations:

Sidewalk Toronto

- Sidewalk Toronto was an innovative experiment conducted by Sidewalk Labs (part of Alphabet—the parent company of Google) and Waterside Toronto to create an urban smart district that was "climate positive, affordable and inclusive for residents, created jobs, and operated as an innovation hub for smart city experiments".[21]
- In 2020 the project was shutdown due to concerns raised by data privacy and security experts regarding the privacy, ownership and governance of the smart city project.
- Dr. Ann Cavoukian was on of the privacy experts that cautioned against the project and stated, "concerns for privacy is at an all-time high, trust is at an all-time low". Cavoukian highlighted the need to address this lack of trust through the Privacy by Design (PbD) methodology. PbD focuses on proactively ensuring all necessary measures for privacy and security is embedded into all aspects of a product or design before it is released.[22]

Facial Recognition Technology

- In 2020, an investigation by the Federal, Alberta and BC Privacy Commissioners found that Cadillac Fairview - one of North America's largest commercial real estate companies - broke Canadian privacy laws.[23]
- According to the investigation, the company installed facial recognition technology inside a dozen malls and analyzed visitors' images without obtaining proper consent.
- Facial recognition software was used to generate personal information about individual shoppers, including estimated age and gender.
- While the images were deleted, investigators found that the sensitive biometric information generated from the images was being stored in a centralized database by a third party.
- Cadillac Fairview stated that it was unaware that the database of biometric information existed. This compounded the risk of potential use by unauthorized parties or by malicious actors in the event of a data breach.

Population Control and Movement

- Freedom of movement derives from many international declarations and has been recognized as a fundamental right by many countries. The ability of AI systems to limit this right is related to its use for surveillance purposes.
- A report from the Carnegie Endowment for International Peace highlighted that roughly 75 out of 176 countries globally are actively using AI for security purposes (such as border management).[24]
- Privacy and human rights concerns are increasing regarding the disparate impact of surveillance on marginalized populations that are already discriminated by police (such as refugees and irregular migrants). AI-powered predictive policing tools raises the risk of creating inaccurate, skewed, or systemically biased data.

[21] The Sidewalk Toronto project

[22] The 7 Foundational Principles of Privacy by Design

[23] Cadillac Fairview collected 5 million shoppers' images

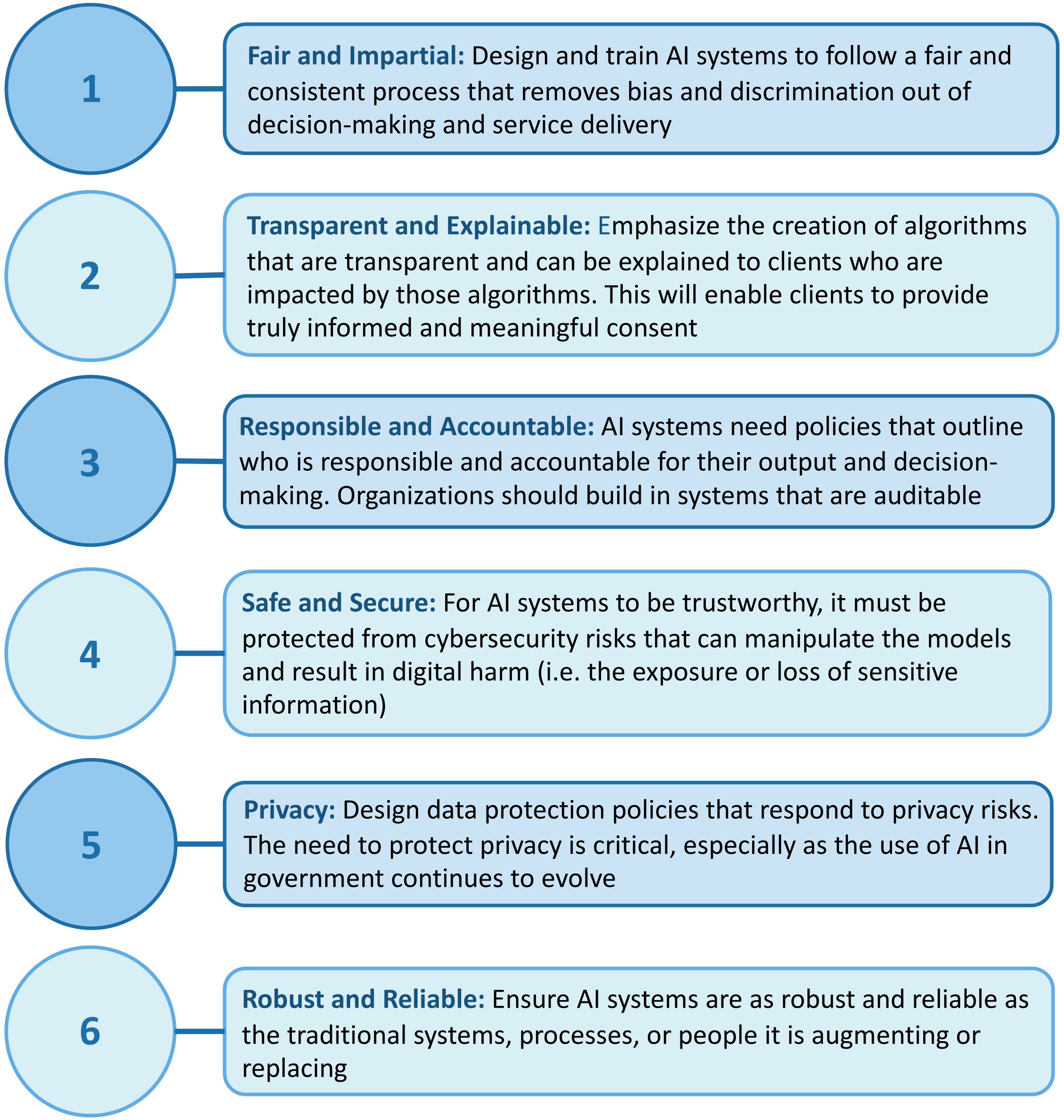
[24] The Global Expansion of AI Surveillance

5. Strategies to Ensure the Ethical Use of AI in Government

AI technology has the potential to revolutionize how government delivers services to clients.[25] The earlier sections highlighted important privacy and human considerations that emerge as a result of AI use. However, as AI technologies continue to evolve, future implications are yet to be determined.

To help address the current (and future) privacy and human rights implications of AI, organizations must develop and implement safeguards to mitigate potential risks. Building principles into the development of AI systems will ensure it functions in a trustworthy, equitable and ethical manner. This will help build and maintain public trust.[26] The following are some strategies organizations should consider to ensure the ethical use of AI:

Strategies for the Ethical Use of AI [27]



1 **Fair and Impartial:** Design and train AI systems to follow a fair and consistent process that removes bias and discrimination out of decision-making and service delivery

2 **Transparent and Explainable:** Emphasize the creation of algorithms that are transparent and can be explained to clients who are impacted by those algorithms. This will enable clients to provide truly informed and meaningful consent

3 **Responsible and Accountable:** AI systems need policies that outline who is responsible and accountable for their output and decision-making. Organizations should build in systems that are auditable

4 **Safe and Secure:** For AI systems to be trustworthy, it must be protected from cybersecurity risks that can manipulate the models and result in digital harm (i.e. the exposure or loss of sensitive information)

5 **Privacy:** Design data protection policies that respond to privacy risks. The need to protect privacy is critical, especially as the use of AI in government continues to evolve

6 **Robust and Reliable:** Ensure AI systems are as robust and reliable as the traditional systems, processes, or people it is augmenting or replacing

[25] Evolving Use of Artificial Intelligence in Government
[26] How do we ensure the responsible use of AI by Governments?
[27] Trusted AI, trusted government: Developing and deploying trustworthy AI in government

For Further Reading

- UN urges moratorium on use of artificial intelligence technology that imperils human rights
- We Need to Get Smart About How Governments Use AI
- Social Service Agencies Turn to the Cloud and AI to Serve Families in Crisis
- German Federal Cabinet adopts strategy for cybersecurity 2021
- Right to contest automated AI decision under review as part of UK government data protection consultation
- Using AI and machine learning to reduce government fraud

Other noteworthy articles:

IBM Canada Survey: Cybercrime and security risks at government level have more than 9 in 10 tech leaders concerned

Three steps to heaven: Delivering genuine value through public services technology

Study finds growing government use of sensitive data to ‘nudge’ behaviour

CX: Voice Of The Customer: Are You Listening?

Research Repository

Access the Citizen First Research Repository.

Recent entries on the research repository:

A Highlight of the Citizens First 2020 Study - Joint Council’s Executive Report August 2021

The report highlights the following areas: An Overview of the Report, Key Insights, and Recommendations.

Trends in the Daily Newsletter

According to a recent article, the COVID-era emergency legislation supporting e-signatures could become permanent in Australia. The government has announced plans to provide the first nationally consistent way of digitally signing legally binding documents. Supported by enthusiastic business and legal industry feedback, the Morrison government has positioned electronic document signing as a key part of its Deregulation Agenda, releasing the new issues paper to drive a consensus about how e-signatures can best be harnessed in the future.

Data privacy is set to become the defining issue that impacts how clients choose to interact with government and big business, according to ITProPortal. Client concerns are rising as the pandemic increases digitization across sectors. Although legislation like Europe's General Data Protection Regulation (GDPR) represents a valiant first attempt to hold government bodies and private companies accountable regarding how personal data is handled, many clients are concerned with the growing lack of data privacy and control.

The National Post recently published an article that examined what Canadian provinces and territories have announced about the implementation of proof-of-vaccination programs, or lack thereof. The article highlights public information available as of September 2021.

We would love to hear from you!

Do you know someone who may be interested in the Joint Councils Executive Report? Please share a copy of this report. If you are not already a subscriber, you can now subscribe to receive the Executive Report by signing up. Send your questions to info@iccs-isac.org.

Follow: