Achyut Prasad Adhhikari
Public Policy and Public Administration, McGill University, Canada. (email: achyutrajadk@gmail.com)

Submitted: 7 August 2025, Revised: 2 September 2025, Accepted: 3 September 2025

Achyut Prasad Adhhikari did his first master's degree in public administration from the Public Administration Campus Tribhuvan University and got another master's degree in business studies from Shankar Dev Campus of the same university, in Nepal. As Mr. Adhhikari is a lifelong learner, he pursued his studies even abroad to acquire another master's degree in public administration and governance from McGill University, Canada where he is also serving as an assistant professor. Besides, Mr. Adhhikari is a full-time healthcare manager at CIUSSS West-Central Montreal (A publicly funded group of hospitals) in Canada. He is desperate in healthcare and environmental governance, public policy, project management, and political economics. Alongside the profession, he is passionate about reading, writing, traveling, and networking.

Policy & Governance Review
ISSN 2580-4820
Vol. 9, Issue 3, pp. 334-349
DOI: https://doi.org/10.30589/pgr.v9i3.1275

Artificial Intelligence in Governance: The State of Facial Recognition Technology in Canada

Abstract

Innovation in public service delivery can help the rapid transformation of society into a post-COVID era. In addition to minimizing administrative hassles, efficiently using Artificial Intelligence (AI) can protect citizens from unwanted behaviors. AI broadly denotes the efficiency of computers in replicating human intelligence, such as identifying different patterns and making predictions and decisions. AI encompasses numerous techniques, and machine learning is one of the most widely used. Machine learning is a method of deploying large datasets to make predictions that improve over time with more data. By 2030, Canada aims to have one of the most robust national AI ecosystems in the world, founded upon scientific excellence, high-quality training, deep talent pools, public-private collaboration, and their strong value of advancing AI technologies to bring positive social, economic, and environmental benefits for people and the planet. This study intended to assess the overall situation of AI in governance and policy compliance. I found that the country relies on patchwork and faces numerous legal and practical issues owing to the absence of an umbrella policy and organization. This research also proposes ideas to enhance governance to improve biometric data protection, legal frameworks, and quality standards for collecting biometric data based on the FRT. This study is based on focus group discussions, policy papers of the government of Canada, and many other literature and research articles.

Keywords:
innovation; artificial intelligence; machine learning; face recognition; governance; public policy

Introduction

Artificial intelligence (AI) has been a part of the lives of individuals and the government to serve citizens with prompt intervention effectively and efficiently. As AI exists in every human activity, the government should regulate this behavior with the required legal provisions to serve the public and protect its citizens from fraud and numerous social evils. According to a recent study on the use of technology in public administration in Canada, robots are on doorstep (Molnar and Gill, 2018), raising images of robotic savages preparing to cause havoc in jobs in the public arena. Government officials use AI to distribute benefits, determine status, revoke licenses, and perform various other duties. The Canadian government has long believed that using technology in public administration improves life in Canada by enabling public policy thinkers to develop a long-term vision, helping them analyze large amounts of data, and responding to the exponential growth of computing power to assist the public more efficiently and effectively. According to a recent fascinating contribution by Lepage-Richer and McKelvey, two Canadian prime ministers, Pierre Elliott Trudeau and his son Justin, tried to embrace technology because they believed it might be advantageous to further the common good (Digital Disruption White Paper Series 2018:3; Lepage-Richer and McKelvey 2022).

On the one hand, technological advances are pushing Canadians into an outdated state and have replaced friendly bureaucrats with useless machines. On the other hand, using technology allows us to confidently advance to utopian, less expensive, and efficient decision-making processes (Boyd and Crawford, 2012, pp. 663).

Utilizing AI to put citizens under surveillance, scrutinize their activities, and monitor their financial transactions to ensure better tax compliance; therefore, extracting more revenue from the government is a disturbing trend (Daly, 2023). A less prevalent and more desirable trend is to use AI to augment citizen services. Even though AI can significantly increase efficiency and fairness in these processes, it is frequently forgotten that file disposal and decision-making are the most crucial duties for any department of the federal or local government (Wirtz et al., 2019).

Methods

This study broadly focuses on the administrative and governance notions of Artificial Intelligence. Specifically, it aims to determine the deployment of Facial Recognition Technology (FRT) in Canada. This study reviews a range of proposed and pending laws and regulations that aim to reduce or address human and civil rights concerns raised by the Canadian government related to the use of FRT. My goal is to draw on the challenges and pitfalls of using FRT in Canada and to determine mitigation strategies to ensure the wide acceptance of FRT.

Two identical data sources were used in this study. The first is the public list of the Treasury Board's Directive on Automated Decision-Making (DADM) (2023). The Canadian Treasury Commission Secretariat 2023 (DADM) is the federal government’s strategy to regulate AI and algorithms, while the Algorithm Impact Assessment (AIA) tool (Government of Canada 2021) acts as an additional tool to implement DADM. The second source includes Web searches conducted in August 2023 on the websites of Canadian federal agencies, either directly or through Google.

General overview of AI and FRT

Artificial Intelligence (AI) refers to machine Intelligence that is capable of perceiving, learning, and problem-solving using human-like cognition. Created in the 1940s, AI arose from the convergence of research areas in cybernetics, information theory, and algorithm theory (Gritsenko & Zherebtsov, 2020). Regardless of the different definitions that have emerged with technological advancement, no definition has been agreed upon. UNESCO (2020) has understood AI as an algorithmic information-processing system capable of learning and performing cognitive operations, such as decision-making and forecasting autonomously.

AI is widely used in numerous sectors, such as national defense, healthcare, finance, and telecommunications, because it improves administrative efficiency and processes large amounts of data. It is highly important for public administration to streamline service delivery. Facial recognition technology (FRT), which is widely used in public infrastructure and daily life, is one of the most well-known and controversial uses of AI. FRT is widely used in schools, transportation systems, and law enforcement and can be found in phones, smart devices, and public surveillance networks (Richardson, 2023).

Law enforcement agencies in countries such as Canada, America, and even Europe use FRT for real-time surveillance and accessing public and private image stores. Because its rapid adoption has triggered unmatched privacy and ethical concerns, regulatory reactions have been inconsistent. Whereas some locations ban or limit FRT use, others have implemented sectoral guidelines, highlighting the decentralized nature of regulation (Richardson, 2023).

The increasing ubiquity of AI and FRT calls for blanket regulations that weigh innovation against the protection of human rights.

AI in Governance World Scenario

Artificial Intelligence (AI) is transforming public administration globally by bridging governments and citizens using enhanced efficiency, transparency, and responsiveness. A digitized, information-rich world enables smart public service provision provided that ethical standards and robust regulatory environments are used. AI is used extensively in governance sectors by the US, EU, China, Russia, and India, all of which are doing so within particular political, social, and regulatory contexts.

European Union: Ethical Digital Governance Focused on Privacy

The European Union is a global leader in ethical AI governance that focuses on privacy, data protection, and human rights. The General Data Protection Regulation (GDPR) remains the cornerstone of this approach, with strict rules for processing personal data such as biometric data obtained using facial recognition technologies (EU, 2016). For instance, Sweden's data protection agency fined a secondary school to pilot a facial recognition attendance system with insufficient safeguards. In the UK, the Information Commissioner's Office has explained that all processed facial images, whether or not they match, are sensitive personal data and thus subject to GDPR controls (ICO, 2019). Such steps ensure the broad regulation of AI systems, particularly those used in law enforcement and surveillance, and reinforce the EU's commitment to upholding democratic values in the digital era.

United States: Patchwork but Evolving Framework

In contrast to the EU, the U.S. has no overarching federal framework to govern AI and biometric data. Instead, states have discrete pieces of legislation, typically directed toward the private sector. In particular, Illinois has become a courtroom battleground because of its Biometric Information Privacy Act (BIPA). The defendants Motorola and Vigilant faced allegations by plaintiffs in a high-profile case of illegally extracting images from a state photo depository to develop facial recognition software for law enforcement, underscoring the knotty legal landscape of public-private partnerships utilized in AI surveillance (ACLU, 2022). With litigation on the rise, these laws unintentionally affect government use of AI by imposing liability on technology vendors, which indirectly affects public-sector use.

China: Strategic Innovation and Global Ambitions

China has rapidly established AI regulations through the mandating of regulatory compliance with generative algorithms, deepfake content, and AI recommendation systems (FMPRC, 2022). While the Chinese government welcomes AI as an enabler of national development and economic growth, its application raises concerns about monitoring, censorship, and control. New regulations impose safety checks on AI applications related to public opinion or potential mass mobilization. Moreover, AI providers should adapt to national values and avoid promoting separation. Despite these limits, China has led the world in facial recognition technology exports with 201 contracts, surpassing the U.S. (Knight, 2023). This leadership is due to China's double-edged strategy of building local AI capacity while spreading its technological influence abroad. In addition, China encourages international agreements on ethical AI governance and attempts to contribute to global norms through diplomacy and regulation models (FMPRC 2022).

Russia: Incremental Progress with Surveillance Concerns

The evolution of Russia's AI policy followed these periods. From early digital reforms like "Electronic Russia" (2002–2009) to the "Information Society" (2011–2020) and continuing developments under the "AI Strategy 2030," the government is gradually building e-governance (Zherebtsov & Gritsenko, 2020). Strategic planning documents: Presidential Decree No. 204 and the Strategy for Scientific and Technological Development prioritize AI. The implementations were uneven. Interestingly, Moscow possesses one of the world's largest facial recognition systems for surveillance and integrates over 160,000 cameras, including 3,000 that have recognition software installed. Although promoted as a law enforcement system, it fuels global protests against privacy breaches and state surveillance (Marchi, 2023).

India: Inclusion, Innovation, and Ethical Sensibility

'The trajectory of India' in the use of AI in governance has been steered by its diverse socio-culture and aspirations of digital inclusion. The government has also put in place AI systems to improve public service delivery, such as the claims management system adopted by the Defense Ministry, together with IIT-Kanpur. AI is also used to prevent fund leakage in welfare schemes, pointing to an aspiration for responsible governance (Government of India 2023). AI centers of excellence will be established, and a "Hub and Spoke" approach will be adopted to research ethical AI. However, there are concerns about algorithmic bias in nations with gender, caste, and linguistic heterogeneity. Policymakers should develop safeguards against discriminatory outcomes, and make AI transparent, interpretable, and socially responsible. If they can do so, India's demographic and linguistic advantages can propel it to become a global AI powerhouse, especially in developing large language models (Government of India 2023).

The global application of AI in public administration reflects both the hope and risk of online governance. While the EU and national governments that emphasize democratic values of the ethical deployment of AI exist, other countries, such as China and Russia, use AI to augment state power. The United States is technologically advanced but is plagued by regulatory fragmentation, whereas India wrestles with an innovation-inclusion balance and shifts in international power. Each country's political environment, societal expectations, and technological competence determine its governance model of AI. While various approaches have been utilized, international cooperation has become more vital in establishing shared norms, ethical standards, and policy frameworks for AI technologies. Achieving this balance determines whether AI remains a public good or becomes an exclusionary, surveillance, and unequal force.

AI and FRT in Canada

A joint investigation in 2021 by Canadian provincial and federal privacy commissioners found that Clearview AI collected billions of web pictures to develop facial recognition technology (FRT) sold to police forces in Canada, without individuals' complete permission (McPhail, 2021). Likewise, Cadillac Fairview used FRT in 12 shopping malls without customer knowledge (Office of the Privacy Commissioner of Canada, 2020). The FRT identifies individuals through biometric characteristics, creating serious privacy concerns, especially when applied secretly (Canadian Civil Liberties Association, 2022).

Despite the overall optimism for the advantages of AI, Canadians are apprehensive about data security, privacy, and potential abuse (Nanos Research, 2021). Current Canadian privacy laws do not adequately protect citizens' biometric information, leading to loopholes in informed consent requirements (Stevens & Brandescu, 2021). Quebec introduced provincial biometric protection legislation, but the federal and provincial regimes remain fragmented.

Canadian regulation of AI and FRT is fragmented and split between the federal administration of privacy and human rights and the provincial administration of consumer and property rights. The Clearview AI case illustrates the need for harmonized national guidelines, stronger legal frameworks, and transparent accountability mechanisms to govern the use of biometric data in AI systems.

Legislative efforts

AI has multiple uses in Canadian federal law and policy domains. By this time, the Committees of the Senate and House of Commons had studied and examined AI related to various policy areas and the specific use of technology that encompasses the following:

- The House of Commons Standing Committee on Access to Information, Ethics and Privacy, Facial Recognition Technology, and Increasing Potential, produced a report in October 2022 (House of Commons, 2022).
- Challenge Ahead: Integrating Robotics, Artificial Intelligence, and 3D Printing Technologies into Canada's Healthcare Systems, a study published in October 2017 by the Senate Standing Committee on Social Affairs, Science, and Technology (Senate of Canada, 2017).
- Driving Change: The Senate Standing Committee on Transport and Communications published Technology and the Future of Automated Vehicles in January 2018 (Senate of Canada, 2018).

AI research advancements may affect various policy domains, including

- The use of AI in national security and intelligence.
- Decisions are made automatically when processing immigration and asylum petitions.
- How can privacy concerns be balanced by the openness, sharing, and linking aspects of AI development?
- How does AI affect the environment?
- The application of AI to public health and population health decision-making, especially during pandemic management.
- The effects of AI on employment include automation of industries and professions.
- Making certain AI systems respect human rights, equity, and inclusivity; and
- AI and automated decision-making in the public sector are covered by the Treasury Board Directive on Automated Decision-Making.

Governance Approach

As previously stated, Canada lacks an effective and comprehensive governance approach concerning digital governance regarding biometric technologies, such as FRT. Our strategy calls for updating Canada's data and privacy protection laws, establishing data and algorithm quality standards that facilitate interoperability between international and provincial/territorial jurisdictions, and establishing an independent oversight body and a new AI Ethics and Responsibility Commissioner to improve the country's current digital governance (Council of Canadian Academies 2021). Finally, I outline Canada's involvement with the international community in implementing digital governance.

Legislative Reform: Data Protection and Privacy Laws

Canada's existing privacy legislation does not expressly define biometric data as personal information; however, it is often assumed to be so because it can be employed to identify an individual (Innovation, Science, and Economic Development Canada, 2019). The Canadian Digital Charter sees trust and transparency in digital government, intending to coordinate

Fragmented federal and provincial privacy legislation with key human rights protection. Its main goal is to limit the public and private sectors' use of facial recognition technology (FRT) for mass surveillance (House of Commons, 2022).

Biometric data pose an increased threat to privacy, particularly when government agencies transfer data to private contractors, as in the case of Clearview AI (McPhail, 2021). The current law allows such sharing under vaguely worded national security exceptions, with minimal transparency or public oversight. Reform is thus essential to manage private-public data exchange and close loopholes, allowing unregulated biometric use.

Informed consent is also central to the privacy law. New reforms will require "meaningful consent" in plain, easy-to-understand language, particularly for vulnerable parties such as children and cognitively disabled individuals. The reforms were based on the 2021 Chief Privacy Commissioner's request for a right-based privacy law. They encourage more open data retention policies, transparent use limitations, and the enhanced protection of sensitive biometric information.

Standardization and Quality Control

A face-recognition algorithm and a mass facial image database are the two fundamental components of facial recognition technology (FRT) (Garvie et al., 2016). However, most of these databases are not ethnically diverse or image-rich, thus decreasing the performance of the FRT for people from underrepresented groups (Balasubramaniam et al., 2021). There are over 100 commercial facial recognition algorithms; however, algorithmic bias due to training data disparities disproportionately affects marginalized groups (Buolamwini & Gebru, 2019; Buolamwini & Gebru, 2018).

To respond to this, the Standards Council of Canada (2021) emphasized the importance of improved standardization and data stewardship. The proposed governance framework suggests that FRT development maintains prominent levels of quality, in alignment with international standards and ethical data practices. This involves leveraging ethically sourced, varied, and consent-based datasets to train algorithms.

The proposal also recommends establishing a national licensing agency to regulate and certify FRTs used in Canada. Such an agency would ensure that FRT systems conform to a country's standards of quality, privacy, and ethics to ensure public trust and compatibility across countries. Such standards would prevent bias, enhance the reliability of algorithms, and respect individual rights when using AI technologies.

Oversight and Enforcement

The Personal Information and Electronic Documents Act (PIPEDA) and Privacy Act are two important federal privacy laws enforced by Canada's Office of the Privacy Commissioner (OPC) (OPC, 2023). However, the OPC currently lacks the authority to impose binding orders or fines, acting instead as an ombudsman that issues nonbinding recommendations (McSorley, 2022). To address this limitation, the proposed governance model includes the establishment of an independent oversight body led by a federal Artificial Intelligence (AI) Ethics Commissioner. This body incorporates AI experts, policymakers, representatives from diverse communities, the OPC, and the Chief Information Officer.

An oversight body should be mandated to lead public consultations on biometric technologies, handle complaints, enforce data protection laws, and apply penalties to institutions that misuse personal data. The body would also conduct human rights impact assessments, advise on privacy law reform, and represent Canada in global AI governance discussions. Strengthening oversight through this mechanism aims to enhance public trust as AI technologies such as Facial Recognition Technology (FRT) increasingly affect everyday life.

Canada’s Contributions to International Efforts Seeking to Advance AI and Data Governance Initiatives

Canada is credited with developing the world's first national AI strategy through the pan-Canadian Artificial Intelligence strategy. The Canadian Institute for Advanced Research (CIFAR) spearheaded the policy's introduction in 2017, and has since elevated the nation to a prestigious position as a global leader in AI research. In addition to its national efforts, Canada actively participates in international initiatives to advance AI, data governance, and policy development as part of the United Nations' Digital Cooperation Roadmap initiative, the OECD's Going Digital Project, and the World Economic Forum's data governance policy project. Canada is the co-creator of the International Panel on AI with France and is a founding member of the Global Partnership on AI (GPAI).

Canada's present commitment to advancing AI technology (including FRT), policy development, and data governance is arguably rooted in the broader international context as it continues to develop its own AI governance. The improved governance strategy outlined in this section seeks to establish Canada as a pioneer in digital governance, guarantee uniform global adoption of the technology, and fortify its regulatory framework in line with other countries. However, it has unintentionally had drawbacks and difficulties (Government of Canada 2021).

Challenges and Pitfalls

A patchwork of laws and regulations governs Facial Recognition Technology despite its widespread use and the privacy and civil liberties it raises (OPC, 2021). Few authorities have banned its use, whereas others have implemented more targeted interventions. However, none of the laws and regulations have been drafted to address technologies other than FRT, although they might be relevant to FRT. In this regard, a few prominent issues of FRT can be summarized as follows:

Bias and inaccurate

A study led by the US National Institute of Standards and Technology (NIST) examined 189 different algorithms on 18 million images to determine the accuracy of the models. The study found significantly higher rates of incorrect matches among Asian, African American, and indigenous populations. The study also discovered that the algorithm was more likely to misidentify women, children, and the elderly (Grother et al. 2019; Buolamwini and Gebru 2018; Melendez 2018). Because disadvantaged people are subject to excessive police surveillance, inaccurate models put them at a greater risk of being misidentified and can lead to real harm. In a recent report on the failure of this technology in the United States, a young black man was misidentified, arrested, spent 10 days in a correctional center, and fought for a year to get his charge cleared (Johnson 2022).

Fragile and human influence

However, this technology is vulnerable to adverse effects. This implies that actors could trick falsely defined models (Goodfellow et al. 2014). For example, studies have explored the significant impact of wearing accessories, such as eyeglasses, on these models (Sharif et al. 2016).

Risk of Wrong Interpretation

Facial recognition systems develop their own sets of patterns and rules by analyzing large data collections. It is difficult for researchers to define these rules and determine how they make decisions. Therefore, the creator of the model lacks clear comprehension of how to make decisions when a person is misidentified by the model (Linardatos et al., 2020).

Developing unethical models

Facial recognition technology (FRT) systems typically rely on large datasets of millions of images, some of which are gathered without informed consent (Balasubramaniam et al., 2021). Clearview AI, for instance, admitted that it has gathered images from websites, such as Google, Flickr, and Facebook. However, Canada's Office of the Privacy Commissioner (OPC) rejected the argument that publicly shared images signify a breach of privacy rights, pointing out that social media photos are not exempt from the Personal Information Protection and Electronic Documents Act (PIPEDA), and therefore require consent to collect.

There are numerous challenges to implementing a national model of governance for FRT. Harmonizing privacy standards and laws across federal and provincial authorities presents complex political deals. In turn, imposing shared standards on multinational corporations operating across legal borders presents an additional challenge. Licensing and quality requirements may discourage innovation, reduce investment, and prompt firms to move their production to more permissive jurisdictions. Small organizations can be deterred by such compliance at the cost of jobs. Furthermore, FRT's dependency on extensive datasets increases the risk of cyberattacks and brings with it further challenges in seeking

Meaningful consent from digitally excluded communities. These considerations underline the need for a robust, enforceable, equitable governance framework.

Policy issues

Canada's PIPEDA regulates how the private sector collects, uses, and discloses personal data, whereas the Privacy Act controls the government's use of personal data. Most provinces and territories have passed privacy laws that reflect PIPEDA and empower commissioners or ombudsmen to interpret and apply all the relevant laws. Under the Privacy Act, organizations can conduct privacy impact assessments for their programs or services. The privacy effect evaluations of the Passport Canada project, which uses face recognition technology to identify fraud in passport applications, have been subject to review by the Office of the Federal Privacy Commissioner since 2004. The Office of the Privacy Commissioner has offered several suggestions since 2012 regarding how the project can lessen the risks of bias and privacy associated with using facial recognition.

Mitigation Strategies

To effectively address evolving digital governance and biometric technology issues, such as Facial Recognition Technologies, the Canadian federal government is urged to step forward and enact a comprehensive Digital Governance Act. The Act should be developed through extensive consultation with crucial stakeholders, including provincial and territorial governments, private organizations, and civil society. The increased interconnectivity brought about by globalization and the rapidity of technological change require increased intergovernmental and trans-sectoral cooperation in data protection, cybersecurity, and service delivery (Leitner & Stiefmueller, 2019).

Institutional Mechanisms for Digital Oversight

It is recommended that certain public institutions be established by law to regulate cybersecurity, standardize data, and ensure the quality of digital services. These frameworks should offer strategic policy recommendations, handle complicated issues with specialized knowledge, and uphold consistent standards across the country with the help of provinces and territories. By doing so, the federal government can make harmonizing data collection practices easier, eliminate waste, and improve public service delivery across federal, provincial, territorial, and local jurisdictions. These frameworks do more than invite operational uniformity; they invite accountability and transparency, both of which are important to efficient digital governance.

Leadership Founded on Ethics and Competence

Digital transformation is a leadership framework founded on ethics and competence. According to the values and ethics codes for public services and the Canadian public service key leadership competencies (KLCs), leaders should be courteous, professional, and honest (Government of Canada 2011, 2016). These values play a critical role in building and maintaining public trust, especially in cases where intrusive technologies such as FRT harvest and analyze sensitive biometric data.

The decline in public trust brought on by the secret use of surveillance technologies is a significant problem (OPC 2021). Leaders must ensure that strong transparency measures are implemented to combat covert surveillance. These include making departmental and oversight reporting accessible, clearly communicating the policy's intention, and educating the public, especially the underprivileged groups who might harbor a history of Mistrusting Government Institutions. Such communications can be made more inclusive by applying Gender-Based Analysis Plus (GBA+) lenses (Government of Canada, 2016).

Preservation of Transparency and Public Confidence

Leadership must be transparent at all stages of the development, implementation, and monitoring of FRT policies. The Parliament ensures legislation transparency, but extraordinary efforts must be made to enlighten the public on technical parameters and decisions by oversight bodies for emerging technologies. Specialized communication techniques must be used to convey information to the general public because FRT is a highly technical field.

In addition, transparency calls for more than just releasing information. It also calls for accountability processes that enable the public to examine government operations. Public trust is not only based on transparency, but also on the belief that authorities make responsible and ethical choices regarding the utilization of FRT and other AI technologies (Leitner & Stiefmueller, 2019).

Long-Term Vision and Strategic Foresight

Another essential leadership function is the use of foresight and long-term strategic thinking. This revolutionary, fast-paced nature of biometric technologies calls for leaders to project future socio-political and economic developments and accordingly create adaptive governance policies. Stiefmueller (2019) underscores the necessity of foresight to enable policymakers to respond proactively earlier than technological developments and craft resilient policy methods.

Evaluating biometric data governance from the perspective of the government's threefold role as a technology promoter, regulator, and consumer will also be part of strategic thinking. Leaders must strike a balance between these responsibilities carefully when drafting laws, putting oversight plans into place, and establishing performance standards that can adapt to new developments.

Stakeholder Engagement and Shared Ownership

Stakeholder involvement is a critical component of good governance. Implementing structured communication processes with industry stakeholders, citizens, experts, and special interest groups is necessary for leadership. This participatory process enhances policy ownership and reduces the tensions associated with the implementation of FRT.

The KLC views stakeholder partnership as fundamental. Public hearings, town meetings, and opinion surveys as means of engagement must be integrated to gather feedback and muster support for the governance strategy. At a more elevated level, stakeholder engagement should be managed through robust project management practices to consolidate feedback from diverse sources and translate it into actionable policy (Government of Canada, 2016).

Adapting to Change through Change Management

Owing to the constantly changing nature of digital technologies, governance systems must be agile. Leaders must consider change management as a cyclical process of implementation, evaluation, and adjustment. As technologies develop, undesirable outcomes may arise that require swift policy refinements.

Leitner and Stiefmueller (2019) emphasize that policymaking in tech governance is an iterative process and requires leaders to formulate instruments to monitor gaps between governance goals, and what happens. Muhammad (2014) also adds that effective change management comes from leaders' capability to recognize when policy changes are needed, and why, and alter strategy accordingly.

To detect early indicators of distress, leaders must establish autonomous monitoring systems and feedback loops (Leitner and Stiefmueller 2019). Proactiveness and engaging leadership competencies are vital in gap analysis and in closing gaps between the governance framework constructed and the ever-changing realities of technology uptake.

For Canadian digital governance, especially in FRT, there needs to be an adoption of synergy among legislative creativity, ethical leadership, and cooperative governance. The creation of a Digital Governance Act, underpinned by a strong institutional and regulatory structure, has a huge potential to provide stability, transparency, and responsible use of data across the country. With the KLCs of the Canadian Public Service at the forefront and made possible by an open stakeholder consultation mechanism, political leaders are expected to be visionary, innovative, and participative to effectively address the complex challenges of new technologies and continue to be trusted by the public in digital governance.

Discussions

Methods to increase the accuracy of facial recognition technology include improving neural network architecture and deep learning models through continuous training on new datasets, which are often larger and more complex, with the best quality. There is always the possibility of misidentification. When such a case occurs, it could lead to false accusations of theft or fraud. Unlike many other types of data, faces cannot be encrypted because they are more difficult to change than passwords or credit card numbers. A data breach involving facial recognition raises the risk of identity theft, harassment, etc.

One of the main challenges in face detection and recognition is the diversity of human faces in terms of their shape, size, posture, expression, light intensity and direction, and makeup.

"Diagnostic Automation." However, the technology's usage remains unclear, and some researchers have questioned its accuracy. The researchers discovered that middle-aged white males were less likely than people of color, transgender individuals, and women to be incorrectly identified by technology.

Not 100% accurate. Changes in the skin texture alter the highlights of the face. While the best algorithms achieve impressive results even as the subject ages, changes such as wrinkles and changes in face shape can make it harder for a person to be recognized by the recognition algorithm, especially the elderly.

Hackers can use social network photos to unlock their phones. Scammers can obtain pictures of almost anyone in the social media age and use them to evade facial recognition. Therefore, scammers can use social media images to compromise devices and accounts if facial biometric technology is unable to recognize specific aspects of an image. A snapshot can now be used to open multiple Android phones.

Lean a little if you want to beat facial recognition. While these looks are fun, there are easier ways to beat facial recognition: looking down. Most cameras were mounted near the top of the wall and looked downward. Looking down will only show the top of your head to the camera, not your face or anything like it.

Thus, FRT and AI may not work properly. More than 99% of the black male, white male, black female, and selected white female demographics could identify the top 150 algorithms, according to data from the most recent review, which was conducted on June 28. The highest performing demographic group's accuracy for the top 20 algorithms ranged from 99.7% to 99.8% compared to the lowest group. The accuracy was lowest among middle-aged individuals (M=85.3%, SD=6.6%), and the elderly (M=77.9%, SD=9.7%). age (M = 90.4%, SD = 6.0%).

Conclusion

The rapid advancement of facial recognition technology (FRT) presents both opportunities and challenges for governance, particularly in Canada where the absence of a comprehensive regulatory framework has led to fragmented policies and ethical dilemmas. This study sought to address the central research question: *How can Canada improve its FRT governance to balance technological innovation with privacy, equity, and human rights protection?* Through an analysis of legal, technical, and societal dimensions, this study highlights critical gaps in Canada's approach to FRT, and proposes actionable solutions to mitigate risks while harnessing its potential benefits.

One of the most pressing issues is the lack of a unified governance framework. Currently, Canada's FRT regulationis dispersed across federal and provincial jurisdictions, resulting in inconsistent standards and enforcement. For instance, while Quebec has introduced biometric data protection, other provinces lag behind, creating loopholes that companies such as Clearview AI have exploited. This patchwork system undermines public trust and makes citizens vulnerable to unchecked surveillance. Moreover, existing privacy laws such as PIPEDA and the Privacy Act fail to explicitly address biometric data, relying instead on broad interpretations of personal information. This ambiguity allows misuse, particularly when sensitive facial recognition data are shared between government agencies and private contractors without robust consent mechanisms.

Another major concern is the inherent bias in FRT algorithms, which disproportionately misidentifies racial minorities, women, and older individuals. Studies, including those conducted in the U.S. The National Institute of Standards and Technology (NIST) has demonstrated that these inaccuracies are not marginal, but systemic, leading to wrongful arrests and reinforced discrimination. In Canada, where diversity is a cornerstone of society, such biases pose significant risks to civil liberty. The ethical implications are further compounded by the technology's "black box" nature: many FRT systems operate without transparency, making it difficult to scrutinize their decision-making processes. Without accountability, marginalized communities face heightened surveillance and unjust treatment, exacerbating existing social inequalities.

To address these challenges, this study proposed a multifaceted governance strategy. First, legislative reform is urgently required to close regulatory gaps. The *Digital Governance Act* could harmonize federal and provincial laws, explicitly define biometric data protection, and impose strict transparency requirements on FRT deployment. Second, bias mitigation must be prioritized through standardized, diverse training datasets and mandatory third-party audits of the FRT systems. This ensures algorithmic fairness and reduces discriminatory outcomes. Third, oversight mechanisms should be strengthened by establishing an independent **AI Ethics Commissioner** with authority to investigate complaints, enforce penalties, and conduct human rights impact assessments. Such a body would bridge the current enforcement gap, where agencies such as the Office of the Privacy Commissioner can only issue nonbinding recommendations.

Beyond policy change, fostering public trust is essential. This requires meaningful stakeholder engagement, particularly in communities most affected by FRT, such as racial minorities and indigenous populations. Transparency initiatives, such as public reporting on FRT use cases, accuracy rates, and data retention policies, can demystify technology and empower citizens to hold institutions accountable. Additionally, Canada should align its FRT governance with international best practices such as the EU's GDPR to ensure interoperability and uphold global human rights standards.

This study contributes to the broader discourse on AI governance by underscoring the intersection between technology, law, and social justice. It not only maps Canada's regulatory shortcomings, but also offers a forward-looking blueprint for ethical FRT deployment. Future research should explore the real-world efficacy of the proposed governance models, particularly their impact on marginalized groups. Comparative studies of FRT regulations in other jurisdictions could also yield valuable insights for refining Canada's approach. Additionally, the socioeconomic ramifications of FRT, such as its effects on employment, policing, and public services, warrant deeper investigation to ensure that policies remain adaptive to emerging challenges.

In conclusion, while the FRT holds promise for enhancing security and administrative efficiency, its unchecked use threatens fundamental rights and democratic values. Canada stands at a crossroads: it can either perpetuate a fragmented, reactive approach or lead the way in developing a rights-based governance framework that balances innovation with accountability. By adopting comprehensive legislation, enforcing rigorous oversight, and centering equity in technological deployment, Canada can set a global precedent for responsible AI governance. The path forward demands collaboration among policymakers, technologists, and civil society—a collective effort to ensure that FRT serves the public good without compromising the freedoms it is meant to protect.

References

Balasubramaniam, L., Cooper-Simpson, C., Morello, J. & Pietrusiak, P. (2021). *Interim Report: Facial Recognition Technology in Canada*. Retrieved September 3, 2023 from https://ccla.org/wp-content/uploads/2021/07/Interim-Report-CompiledBM.pdf

Browne S. (2015). *Dark matters: On the surveillance of blackness*. Duke University Press.

Buolamwini, J., & Gebru, T. (2018). *Gender Shades: Intersectional Accuracy Disparities in commercial gender classification.* Retrieved September 3, 2023 from https://proceedings.mlr.press/v81/buolamwini18a.html

Buolamwini, J. (2019). *Response: Racial and Gender Bias in Amazon Recognition — Commercial AI System for Analyzing Faces*: Medium, 2019, Retrieved September 3, 2023 from https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced

Burke, L. (2020). *Facial Recognition Surveillance on Campus.* Inside Higher Ed, 2020.

Canadian Civil Liberties Association (2022). *Facial Recognition - CCLA. Canadian Civil Liberties Association*. Retrieved September 3, 2023 from https://ccla.org/our-work/privacy/surveillance-technology/facial-recognition/

CII (2023). *Artificial Intelligence in Governance*, Confederation of Indian Industry, 17 May 2023, Retrieved August 30, 2023 from https://ciiblog.in/artificial-intelligence-in-governance/

Council of the Canadian Academy. (2021). *Leaders in the Digital Economy: The Governance of artificial intelligence in Canada*. Council of the Canadian Academy.

Crumpler, W, & Lewis, J A (2021). How Does Facial Recognition Work?: A Primer", Center for Strategic and International Studies (CSIS). Retrieved September 3, 2023 from https://www.jstor.org/stable/resrep32894

Daly, P. (2023). *Mapping Artificial Intelligence Use in the Government of (2023)*. SSRN. Retrieved September 3, 2023 from https://ssrn.com/abstract=4459314.

Facial personality analytics, Faception, (n.d.), Retrieved September 3, 2023 from https://www.faception.com/

FMPRC. (2022). "*Position Paper of the People's Republic of China on Strengthening Ethical Governance of Artificial Intelligence (AI)*", Ministry of Foreign Affairs of the People's Republic of China, Retrieved August 31, 2023 from https://www.fmprc.gov.cn/eng/zy/wjzc/202405/t20240531_11367525.html

Forbes. (2023). *How Does China's Approach To AI Regulation Differ From The US And EU*?", 18 July 2023, Retrieved August 31, 2023 from https://www.forbes.com/sites/forbeseq/2023/07/18/how-does-chinas-approach-to-ai-regulation-differ-from-August 31,d-eu/?sh=1f38971f351c

Forbes. (2012). Data Protection Act and General Data Protection Regulation: Big data, artificial intelligence, machine learning and data protection. UK Information Commissioner's Office.

Gartner Inc. (n.d.), Gartner Hype Cycle Research Methodology, Gartner. Retrieved September 3, 2023 from https://www.gartner.com/en/research/methodologies/gartner-hype-cycle

Garvie, C. (2019). *Garbage In, Garbage Out: Face Recognition on Flawed Data*.

Georgetown Law Center on Privacy and Technology. 2019.

Goodfellow, I. J., Shlens, J, & Szegedy, C. (2014). *Explaining and Harnessing Adversarial Examples*. Retrieved September 3, 2023 from https://arxiv.org/abs/1412.6572

Government of Canada. (2011). *Values and Ethics Code for the Public Sector*, Treasury Board of Canada Secretariat. Retrieved September 3, 2023 from https://www.tbs-sct.canada.ca/pol-cont/25049-eng.pdf

Government of Canada. (2016). *Key Leadership Competency profile and examples of effective and ineffective behaviors*, Government of Canada. Retrieved September 3, 2023 from https://www.canada.ca/en/treasury-board-secretariat/services/professional-development/key-leadership-competency-profile/examples-effective-ineffective-behaviours.html

Government of India. (2023). *AI can be the backbone of India's Governance through Tech*, Government of India, Retrieved August 30, 2023 fromhttps://blog.mygov.in/editorial/ai-can-be-the- backbone-of-indias-governance-through-tech/

Gritsenko, D. & Zherebtsov, M. (2021). *E-Government in Russia: Plans, Reality, and Future Outlook*. The Palgrave Handbook of Digital Russia Studies, pp. 33-51, Retrieved September 3, 2023 from https://link.springer.com/chapter/10.1007/978-3-030-42855-6_3

Grother, P., Ngan, M., & Hanaoka, K. (2019). NISTIR 8280: *Face recognition vendor test part 3: Demographic effects*, National Institute of Standards and Technology. Retrieved September 3, 2023 from https://doi.org/10.6028/NIST.IR.8280

Hao, K. (2019). A US Government Study Confirms Most Face Recognition Systems are Racist. *MIT Technology Review.*

Innovation, Science, and Economic Development Canada (2019). *Canada's Digital Charter in Action: A Canadians Plan for Canadians. Government of Canada*. Retrieved September 3, 2023 from https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00109.html

Israel, T. (2020). Facial Recognition at a Crossroads: Transformation at our Borders & Beyond. Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic, 2020.

Johnson, K. (2022). How wrongful arrests based on AI derailed 3 men's lives. Wired. Retrieved September 3, 2023 from https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/.

Kamolov, S., Molchanovskaya, I., & Kaunov, E. (2021). Artificial intelligence is a strategic instrument for the economic development of Russia and the improvement of its public administration. *E3S Web Conference*, *291*. https://doi.org/10.1051/e3sconf/202129104002.

Knight, W. (2023). China Is the World's largest face recognition dealer. Wired, January 24, 2023. Retrieved September 2, 2023 from https://www.wired.com/story/china-is-the-worlds-biggest-Face recognition dealer/.

Kroll, J. A. (2022). ACM TechBrief: Facial Recognition Technology. ACM. Retrieved September 3, 2023 from https://dl.acm.org/doi/pdf/10.1145/3520137 p.2.

Law, K. (2021). Students Share Concerns about Facial Recognition on Campus Security Cameras. Daily Bruin.

Leitner, C., & Stiefmueller, C. M. (2019). Disruptive Technologies and the Public Sector: The Changing Dynamics of Governance. In Public Service Excellence in the 21st Century (pp. 237-274). Springer Nature, Singapore. Retrieved September 3, 2023 form https://doi-org.proxy3.library.mcgill.ca/10.1007/978-981-13-3215-9_8.

Linardatos, P., Papastefanopoulos, V., & Kotsiantis, S. (2020). Explainable AI: A Review of Machine Learning Interpretability Methods. *Entropy, 23*(1), 18. https://doi.org/10.3390/e23010018.

Marsi, L. (2023). Facial recognition helps Putin curb dissent with the aid of U.S. technology. Rwetters, March 28, 2023. Retrieved September 2, 2023 from https://www.reuters.com/investigates/special-report/ukraine-crisis-russia- detentions/.

McPhail, B. (2021). Clearview AI Engaged in "Mass Surveillance Canadian Civil Liberties Association. Retrieved September 3, 2023 from https://ccla.org/privacy/surveillance-technology/clearview-ai-engaged-in-mass-surveillance/.

McSorley, T. (2022). Standing committee on access to information, privacy and ethics [Presentation to the House of Commons]. Retrieved September 3, 2023 from https://

www.ourcommons.ca/DocumentViewer/en/44-1/ETHI/meeting- 12/evidence

Melendez, S. (2018). Uber Driver Troubles Raise Concerns About Transgender Face Recognition. Fast Company.

Muhammad, F. (2014). Leadership, Governance, and Public Policy Implementation Competencies in the Broader Public Sector. European Journal of Business and Management *6*(36), 66-73. Retrieved September 3, 2023 from https://www.iiste.org/Journals/index.php/EJBM/article/view/17352.

Nanos Research. (2021). Canadians' Views on Artificial Intelligence. Innovation, Science, and Economic Development Canada. Retrieved September 3, 2023. https://publications.gc.ca/collections/collection_2021/isde-ised/Iu4-396-2021-eng.pdf

Office of the Privacy Commissioner in Canada. (2020). Cadillac Fairview collected 5 million shoppers. Retrieved September 3, 2023, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/nr-c_201029/.

Office of the Privacy Commissioner in Canada. (2021). Police use of facial recognition technology in Canada and the way forward: Special report to Parliament on the OPC's investigation into the RCMP's use of Clearview AI and draft joint guidance for law enforcement agencies considering the use of facial recognition technology. Retrieved on September 3, 2023 from https://epe.lacbac.gc.ca/100/201/301/weekly_acquisitions_list-ef/2021/2150/publications.gc.ca/collections/collection_2021/cpvp-opc/IP54-110- 2021-eng.pdf p.15-16.

Paul, K. (2020). Ban This Technology': Students Protest US Universities' Use of Facial Recognition. The Guardian, 2020.

Peterson, J. C., Uddenberg, S., Griffiths, T. L., Todorov, A., & Suchow, J. W. (2022). Deep models of superficial face judgments. Proceedings of the National Academy of Sciences, 119(17), e2115228119. Retrieved September 3, 2023 from https://doi.org/10.1073/pnas.2115228119

Raji, I.D., Gebru, T., Mitchell, M., Buolamwini, J., Lee, J., & Denton, E. (2018). Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing. Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, 2020, pp. 145-151; Melendez, S. Uber Driver Troubles Raise Concerns About Transgender Face Recognition. Fast Company, 2018.

Richardson, R. (2023). Facial Recognition in the Public Sector: The Policy Landscape. February 3, 2021. Retrieved August 30, 2023 https://www.gmfus.org/news/facial-recognition-public sector policy landscape

Robertson, K., Khoo, C., & Song, Y. (2020). To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada. Citizen Lab and International Human Rights Program, 2020. 25.

Rogers, E. M., & Marshall, L. R. (2003). Diffusion of innovations. Free Press.

Sharif, M., Bhagavatula, S., Bauer, L., & Reiter, M. K. (2016). Accessorizing a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition. Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 1528– 1540. Retrieved September 3, 2023 from https://doi.org/10.1145/2976749.2978392

Standard Council of Canada. (2021). Canadian Data Governance Standardization Roadmap. Retrieved September 3, 2023 from https://www.scc.ca/en/system/files/publications/SCC_Data_Gov_Roadmap_EN.pdf.

Stark, L. (2019). Facial Recognition is the Plutonium of AI. XRDS: Crossroads. *The ACM Magazine for Students, 25*(3), 50-55.

Stark, L. & Hutson, J. (2021). Physiognomic Artificial Intelligence. *SSRN Electronic Journal.* https://doi.org/10.2139/

ssrn.3927300

Stevens, Y., & Brandescu, A. (2021). Weak privacy, weak procurement: The state of facial recognition in Canada — Center for Media, Technology, and Democracy. Centre for Media, Technology and Democracy. Retrieved September 3, 2023 from https://www.mediatechdemocracy.com/work/weak-privacy-weak-procurement-state-of-facial-recognition-in-canada.

Wirtz, B. W., Weyerer, J. C., & Geyer, C. (2019). Artificial intelligence and the public sector: Applications and challenges. *International Journal of Public Administration, 42*(7), 596–615.