Global Affairs Canada | Affaires mondiales Canada

UNCLASSIFIED

MEMORANDUM FOR ACTION

TO:	**The Minister of Foreign Affairs**
CC:	**The Digital Inclusion Lab, Office of Human Rights Freedoms and Inclusion**
SUBJECT:	Artificial Intelligence and Privacy Harms

SUMMARY:
This memorandum presents options to mitigate the risk posed to privacy from the advent of Artificial Intelligence (AI) based technologies. AI, with current and potential capabilities to increase surveillance presents a serious threat to individual liberty and autonomy. Manipulative uses of AI has and will have the effect of chilling of speech and self determination in society.

Given that AI is a data intensive technology, any comprehensive AI policy will also need to address data collection and the current statutory regime that addresses data collection – *PIPEDA* (*the Personal Information Protection and Electronic Documents Act)*.

RECOMMENDATION(S):

- That you approve the creation of an AI Accountability Office to regulate AI powered machines and their implications. Similar to sector specific acts, like the *Bank Act*, an Act covering the AI industry should be created with input from various stakeholders.
    - The accountability office should have commissioners dedicated to specific sectors of the economy. One such commissioner would be the AI privacy commissioner with powers to enforce privacy regulations, fine violators and ensure remedies to the public are available for privacy violations.
    - The accountability office under its purview would enact the mandatory use of Algorithmic Impact Assessments (AIAs) for algorithms used in public agencies. AIAs would offer a pragmatic framework to assess the risks posed by automated decision-making systems used for resource allocation or predicative policing.
    - The accountably office should also be given audit powers, similar to CRA, to audit algorithms in the private sector.
- That you assign a task force to address the question of ownership of data inferences. Such inferences can be violative and misleading with serious consequences for the liberty of citizens.
- That you put forth legislation to update current privacy legislation considering the implications of biometrics, robots and drones.
    - Legislation should address meaningful consent, the changing of privacy considerations from strictly an informational sphere to spatial and physical as well.

[Kiran Kingra]
[Faculty of Law, University of Windsor]

☐ I wish to discuss
☐ I concur ☐ I do not concur

Minister

Canada

BACKGROUND:

1. AI's explosion resulting from machine learning using "big data" has brought autonomous vehicles, facial recognition technology and autonomous weapons to life. Machine learning, the process by which computers train themselves without explicit programming, requires large data sets to train. Machine learning improves with the size of data thus making AI dependant on the big data revolution. Data becomes the raw material that powers AI and monitoring of the collection of this raw material is critical.

2. AI powered technologies such as drones, robots and 'internet of things' (IoT) have capabilities to collect audio, visual, sensory and olfactory data. All these technologies coupled with social media allow for incessant and copious amounts of data collection facilitating constant and direct surveillance. Data collected through AI technologies and then used with AI machines can have severe consequences that can impact individual autonomy and liberty, perpetuate existing biases in society and raises *Charter* and ethical issues. Recent headlines have pointed out these threats as well.

3. Third party firms obtained data from millions of Facebook users, including Canadians, and used AI to create a 'psychological warfare tool' to influence the 2016 American elections. The firm used voters' internet footprints and real-time data from social media to build unique psychographic profiles to influence their decision making disrupting the notion of free elections.

4. AI systems will also be electronic gatekeepers that will be answering subjective open-ended questions impacting race and human rights in Canada as they decide how to allocate resources; which candidate gets the job or what news feed to show a user. Machine bias, the erroneous assumption in machine learning processes, can perpetuate existing prejudices into automated systems if the data used to train the system are from non-representation data sets. Systemic racism in Canada's justice system has been acknowledged by academics and politicians. The use of data that is already prejudice will only perpetuate biases and inequality in Canada when AI is used to assist and replace human decision making.

5. AI's sheer power to make inference through predicative analysis also raises *Charter* and ethical issues. The inference itself may be very sensitive and not intended to be revealed to the public at large by the subject or the inference may be completely wrong as result of machine bias.

CONSIDERATIONS:

6. Technological innovation is surpassing innovation in governance. Stakeholders from all sides need to be brought together to address social, ethical, commercial and moral issues so a comprehensive AI strategy can be rolled out within the next 18 months or less. The longer Canada lags in a comprehensive AI strategy, the longer it will take to catch up in governance. The damage that could be done through use of AI by the time we catch up will erode citizens' trust in the effectiveness of their government.

7. Privacy has been recognized as a fundamental human right. In Canada, privacy rights are recognized in statutes at both federal and provincial levels, as well as, in common law. Respect for individual autonomy was the background in *PIPEDA*, Canada's private sector privacy legislation, and consent as the foundational principle. Autonomy underpins the democratic system and using AI to exploit and manipulate user through data they shared is violation of privacy and the fundamental human right that privacy provides citizens. Moreover,

constant surveillance interferes with the chilling of speech and self-determination weakening citizens and imposing social control on them. Law enforcement through warrants can have access to user data and harnessing the power of machine learning may make inferences that could jeopardize individual liberties and erode the trust that exists between state and citizen.

8. AI can be a powerful tool for economic and social growth giving Canada a further leadership edge if Canada chooses be at the forefront of encouraging policies that promote and protect privacy rights of citizens, bring transparency and responsibility to the use of AI, and advocate for educating all stakeholders of AI's implications.

9. The introduction of regulations for AI will most definitely be met with cries of government stifling innovation. Commercial interests will also push the notion that consumers are making rational choices when using services and protectionist measures are not required. This is a fallacy, consumers are encouraged to give up data because they are told that there are benefits to the trade-off for personal information. This trade-off has long been used to give policymakers false justification for allowing the collection of all kinds of consumer data even when the public finds the data collection objectionable.[1] Yet research has shown that consumers aren't making rational decisions when it comes to giving up their data bur are "*resigned to the inevitability of surveillance"* rather than having done an actual cost benefit analysis.

10. History has also proven wrong the argument that regulation will stifle innovation. A few decades ago those wanting environment friendly products were regarded as Birkenstock wearing hippies, however, today the green consumer carries immense economic power and she rewards corporations following environment friendly policies and compliance with environment standards.[2] Environmental certification is a source of pride to be lauded in annual reports and advertising, such is now the power of the green consumer from her organic honey growing days. Messaging on Privacy and AI should be similar to messaging on environmental protection measures. It should be framed as being desirable and important to human rights while not always being economically justifiable.

COMMUNICATIONS IMPLICATIONS/ACTIONS:

11. The negative media coverage surrounding issues raised shows that the public has concerns that necessitate address and introduction of a regulations or even government's call to action on AI regulation would feed a positive news cycle.

12. Canadian government's commitment of $125 million dollars of to fund AI is currently regarded as a positive step towards economic and social growth. However, without any governance attached, the first misstep by AI technologies will generate negative press coverage and indicate ineffectiveness on the part of government. This coupled with legislators inaction on issues already identified will also make legislators look weak. We don't have the liberty to endure lessons learned the hard way on AI.

---

[1] Joseph Turow, Michael Hennessy & Nora Draper "The Tradeoff Fallacy*"* June 2016*,* A Report from the Annenberg School for Communication University of Pennsylvania online: <https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

[2] Becky Engel "The Evolution of the Green Consumer" (30 November 2012) blog online: <https://gradybritton.com/brand-development/the-evolution-of-the-green-consumer/>.