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:	Identifying and Removing Extremist Content Online

SUMMARY:

This memorandum presents options to address the current and potential future threat posed to Canadian public safety by online extremist content and radicalization of vulnerable individuals. The Internet allows domestic, foreign, and state sponsored extremists to widen their reach to Canadian citizens. However, online spaces are only one contributing factor to a person's decision to turn to violent extremism. AI is a tool for combating online extremism and reducing such content rather than eliminating it altogether. Government has a key role to play in promoting national sovereignty and protecting the rights of citizens.

RECOMMENDATION(S):

That you approve three Government of Canada policy priorities for AI as a tool to address online extremist content:

- Government must be proactive and collaborate with private sector companies to invest in technology to counter violent extremism.
- The tools created with government support must be fully transparent in providing the public information on the purpose, scope, and results of these tools.
- Government should enact policy that protects citizens' data and digital rights while allowing private enterprise to innovate and flourish.

[Rebecca Herbener, Sebastian Lacey, Matthew Markudis]
[Global Governance, Balsillie School of International Affairs]

☒ I wish to discuss
☒ I concur ☒ I do not concur

_____
Minister

BACKGROUND:

1. The Internet plays a key role in violent extremism by connecting people who previously would not otherwise have been able to engage with each other. In many cases this allows for a non-violent expression of discontent and sharing of ideas. However, frustrated moderates also have been pushed to radicalism through online connections.

2. The Internet helps support extremist groups through financial flows, recruitment, arms trade, and logistics planning. Radical groups, governments, and individuals have exploited online media platforms. Facebook has been used to spread propaganda, Twitter has helped connect moderate Western Muslims with Islamist militants in the Middle East, and YouTube has been used as a tool to spread messages of white supremacy. This has serious security implications for the Federal Government and agencies concerned with protecting Canadians. At the center of this is the balance between citizens' rights to privacy and security with national priorities of ensuring public security and safety.

3. Though most common on large online platforms, violent extremism has also spread to small and medium sized enterprises (SMEs) that conduct their business online, which often lack sufficient human, financial or technological resources to invest in AI for countering violent extremism.

4. AI for countering extremist content is essential, but without sufficiently comprehensive datasets or safeguard mechanisms there will be issues of misidentified content. Currently, there is little in terms of AI capacity that has the same capability as knowledgeable human analysts to sort through data. Therefore, AI is most effective when used in conjunction with human experts who can review information and pinpoint potential or imminent threats.

5. Canadians are deeply concerned with how and by whom their digital data is collected, stored, and used. Recently disclosed data breaches and misuse by private transnational companies mean Canadians increasingly distrust AI and private enterprises handling their data.

6. Many forms of AI may be chosen by private companies to combat online violent extremism, including multiple algorithm-based applications; data collection to compile big data on violent extremism in Canada; reverse engineered algorithms to track the process leading to radicalization of known individuals; and a two-step collection process involving established human analysts to sort through the noise.

CONSIDERATIONS:

7. Legal remedies against Canadians who upload or host content in violation of their Charter right to freedom of expression currently exist. However, Canadian legal jurisdiction does not extend to foreign or state sponsored propagators of extremist content. Recognizing that Canadian values of freedom of expression are not universal, firms that engage in AI monitoring for online extremism can be incentivized to limit the access to Canadian users by geographically blocking content, rather than having it removed. While some users would be able to get around this, the added difficulty to access extremist content provides a substantial barrier.

8. Outright removal of content can have the positive effect of shifting it to areas where fewer users access it. However, it can also be perceived as limiting Canadian citizens' freedom of expression as well as decreasing non-violent avenues to voice socio-political grievances. This may drive moderates and radicals alike to more insulated and encrypted parts of the Internet, which can increase the likelihood of radicals turning to violence. As well, perceived

singling out of specific communities such as white conservatives or Muslims, risks creating a surveillance mentality that may increase a sense of being an outsider and target.

9. There is a large gap between the capacities and incentives of dominant technology firms and digital SMEs. The majority of extremist content is accessed through the platforms of large technology corporations, but extremist content is projected to increase in the short to medium term on SMEs. While SMEs do not currently have the resources to develop AI for combating extremism on their platforms, trends indicate that within the next decade the reduction in the cost of AI will result in its widespread accessibility.

10. Because of potential profit loss, dominant technology firms have demonstrated their willingness to engage in risk-adverse behaviour that can lead to an over-policing of controversial but not extremist speech on their platforms. This has pushed censored users towards other forums more willing to tolerate their discourse without punishment.

11. Government subsidies for AI development to monitor extremist content both addresses the issues of competitiveness and lack of resources for SMEs. However, subsidies for dominant technology firms might face issues of insufficient incentives due to diminishing marginal returns.

12. Regulation on uploading or hosting extremist content would also address issue of SMEs competitiveness disincentive by providing a level playing field for firms to operate within. Punitive regulations would ensure that dominant firms are sufficiently motivated to address the issue of extremism. However, without sufficient subsidies, regulations would disproportionally effect SMEs business viability in Canada. Unless specifically addressed, a regulatory floor will not prohibit firms from engaging in over-policing and can instead motivate them to engage in this risk-adverse behaviour by interpreting the law broadly to avoid reprisal.

13. A parallel governmental mechanism, such as expanding the purview of the Canadian Human Rights Commission (CHRC), would be required to address grievances caused by AI monitoring. In the case of a subsidy regime, if sufficient evidence is collected that a firm is using the Canadian Government's policy on countering online extremism as a mandate to unreasonably censor individuals freedom of expression, future funding could be suspended pending credible assurances that the firm's conduct will better align with the policy. While in the case of a regulation, fines could be imposed.

COMMUNICATIONS IMPLICATIONS/ACTIONS:

14. Media coverage and scrutiny should be expected in the current climate. Tensions between rights to digital privacy and state securities are rife and relatively new. Media outlets on all sides of the political spectrum are looking to see what different state agencies and organizations propose. The public will also be on high alert to see what their government will do to protect their physical and digital security.

15. It is unlikely any form of compromise will go without criticism. Those in favour of a completely free online space will argue against any perceived form of government regulation and surveillance. Proponents of government regulation will oppose private enterprise being allowed to execute independence from government oversight.

16. Clear and open communication with the public is of the utmost importance. Digital data and government access to it is often shrouded in mystery. Government communication through media briefings and news releases must clearly communicate actions taken by the government and why it is doing so.