— A Justice Centre Report —

May 5, 2026

The danger of government-controlled Artificial Intelligence

How state-controlled AI threatens our privacy, autonomy, and free expression – and how Bill C-22 paves the way

Author: Nigel Hannaford

Justice Centre
for Constitutional Freedoms

We Defend
Freedom
in Canada

Abstract

This report examines the current state of public policy in Canada in relation to artificial intelligence (AI), including recent calls to regulate or even nationalize AI. Such proposals come in the wake of the February 2026 Tumbler Ridge mass shooting and the perceived failure of OpenAI (owner of ChatGPT) to disclose the shooter's ChatGPT interactions to police. While framed as necessary for public safety, these proposals risk drawing Canadians' private AI interactions under state surveillance and control. This report argues that such measures – alongside Bill C-22's ambition to expand state access to personal data – threaten *Charter*-protected rights to privacy, freedom of expression, and autonomy by normalizing government access to sensitive personal information without adequate judicial oversight. It concludes that public safety must be pursued through narrowly tailored, warrant-based safeguards that preserve Canadians' fundamental freedoms.

Acknowledgements

We thank the thousands of Canadians who continue to support the Justice Centre with their donations. Their generosity empowers the Justice Centre to defend freedom in Canada and to shape public policy that respects *Charter* rights and freedoms.

Updates to this report

This is Version 1.1 of this report, which may be updated periodically.

About the author

This report was written by veteran journalist and public policy analyst Nigel Hannaford.

Disclaimer: This report discusses ChatGPT, a product of OpenAI. It is an independent publication and is not affiliated with or endorsed by OpenAI.

Table of Contents

Abstract **2**

Executive Summary **5**

Introduction **7**

Tumbler Ridge, OpenAI, and the public reaction **7**

Nationalizing AI? **8**

Increased regulation of AI? **9**

Is nationalization or regulation of AI even effective? **11**

Constitutional implications of AI nationalization and regulation **11**

1. Government bias and "influence" **11**

2. Erosion of privacy **12**

Canadians Courts on privacy protections 13

Restricting autonomy: thought, intellectual exploration, and expression 14

Privacy invasion and self-censorship – A case study 14

Bill C-22 and AI **15**

Conclusion **17**

Bibliography **19**

Executive Summary

February's mass shooting in Tumbler Ridge, British Columbia, was the deadliest mass shooting in Canada since 1989. In June 2025, eight months before the attack, OpenAI (the AI company that owns ChatGPT) suspended gunman Jesse Van Rootselaar's ChatGPT account after internal reviews flagged chats describing gun violence scenarios. OpenAI employees determined that the contents, however, did not meet its threshold of "imminent danger" or "credible risk of serious physical harm" and did not, therefore, report the chats to police. Only after the shooting did OpenAI disclose the chats.

Public and government discourse quickly pivoted from gun control to OpenAI's perceived failure and to the accountability of privately-owned artificial intelligence (AI) companies in general. The federal government signalled it may introduce new legislation addressing private AI companies. Policy analysts have called for a nationalized – or government-controlled – AI, arguing that only government-controlled systems can ensure accountability, democratic oversight, and public safety.

Government control (nationalization or regulation) of private AI companies would come at a very high cost: it could easily facilitate routine state surveillance of private conversations. State surveillance threatens privacy, erodes freedom of expression, and introduces political bias into content moderation. Among its many uses, AI is a tool for private exploration – testing ideas, drafting arguments, and exploring doubts. Nationalization and regulation would afford the federal government broad authority to influence Canadians' use of AI, much like the *Canadian Radio and Telecommunications Commission* (CRTC) inappropriately influences what content Canadians discover through broadcasted and streamed media. Further, such responses to Tumbler Ridge may violate Canadians' right to protection from unreasonable search and seizure.

Bill C-22, the *Lawful Access Act* (introduced in Parliament in March 2026), already lowers the threshold for law enforcement to access what Canadians say and do online. The Bill lowers the legal threshold for lawful access to subscriber information from "reasonable grounds to believe" to "reasonable grounds to suspect" – making it easier for police to obtain sensitive subscriber information. Under this Bill, the federal government may also require "electronic service providers" to retain metadata (definition in footnote[1]) and to create built-in capacity for possible disclosure to law enforcement. Critics highlight mandatory metadata retention as one of the most privacy-invasive tools available, creating

[1] Metadata (or "data about data") is information that, when aggregated, can reveal the detailed patterns of behaviour, associations, and personal interests of an individual. This includes subscriber information such as name, physical address, billing information, and when you opened the account, when and where you access the service, location and physical movements, who you communicated with, the time and duration of calls, and the IP addresses used; etc. (See this Government of Canada website with a detailed list of data included under metadata: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2014/md_201410/)

backdoor surveillance capabilities extending beyond stated anti-crime goals.[2] Given Bill C-22's extremely broad definition[3] of "electronic service providers,"[4] AI platforms like OpenAI will likely also be captured by this legislation, paving the way for an unprecedented degree of state surveillance.

While public safety is a legitimate goal, it must be achieved without expanding state access to AI interactions that would normalize surveillance, erode anonymity, chill intellectual exploration, and lead to ongoing self-censorship. A society where citizens must think twice before asking a question is not a free society.

Governments must pursue their legitimate objectives while respecting the *Charter* rights and freedoms of Canadians, including the right to privacy and freedom from state surveillance. The Justice Centre concludes that Parliament should:

- Resist calls to nationalize or centrally control AI systems
- Reject Bill C-22 and its metadata retention and compelled-access provisions
- Maintain robust warrant requirements for all state access to personal data, limiting such access to circumstances involving serious, imminent, and credible threats

With these measures, Canada can address legitimate safety concerns without sacrificing the fundamental freedoms that underpin a free and democratic society.

[2] Michael Geist, among others.
[3] Bill C-22 defines "electronic service provider" so broad that it essentially captures all services on the internet and more: "electronic service provider means a person that, individually or as part of a group, provides an electronic service, including for the purpose of enabling communications, and that (a) provides the service to persons in Canada; or (b) carries on all or part of its business activities in Canada."
[4] Bill C-22 is directed at electronic or telecommunications service providers generally, not just Internet Service Providers. That broader scope is deliberate and reflects modern communications law, where many entities – not only ISPs – hold subscriber data and metadata relevant to lawful access regimes.

Introduction

As of February 2026, OpenAI's (a leading AI company) ChatGPT attracts approximately 900 million users per week for work, study, and personal purposes.[5] People around the world use the technology for tasks as complex as software development, engineering, and financial modelling, for matters as mundane as planning a garden or fitness regimen, and even for matters as personal as counselling. Increasingly, AI is the world's engineer, data analyst, search engine, problem solver, and, in some cases, confidant.

This report addresses the calls for government surveillance of AI that emerged in the wake of the February 2026 Tumbler Ridge school shooting in British Columbia. OpenAI is the focal point of public reaction. Some call for the nationalization of AI, or legislation that would compel privately-owned AI companies to report concerning AI conversations to law enforcement. This report addresses the constitutional implications of both a state-owned AI model and the regulation of privately-owned AI companies.

While nationalization and regulation are framed in terms of public safety, security, and sovereignty, they would normalize routine government access to private communications without judicial authorization. Technological progress should not require surrendering fundamental freedoms.

This report also examines Bill C-22, the *Lawful Access Act*. If passed into law, this will likely turn OpenAI (and other AI companies) into "electronic service providers," given its broad definition of the term, which would give the federal government and law enforcement much greater powers to access users' information.

Tumbler Ridge, OpenAI, and the public reaction

On February 10, 2026, Jesse Van Rootselaar of Tumbler Ridge, British Columbia, shot and killed his mother and younger half-brother in their home. Then, at the nearby secondary school, Van Rootselaar murdered six students and school staff. Van Rootselaar injured another 27 before dying of a self-inflicted wound. This was the deadliest school shooting in Canada since 1989.

The national conversation did not fixate long on the perennial political question of gun violence. Instead, public scrutiny turned to both the lack of mental health supports in remote communities such as Tumbler Ridge but also to the role that OpenAI played – or, as some would have it, "failed" to play – in the shooting.

[5] Malik, Aisha. "ChatGPT reaches 900M weekly active users" TechCrunch. February 27, 2026. https://techcrunch.com/2026/02/27/chatgpt-reaches-900m-weekly-active-users/

Eight months earlier, in June 2025, OpenAI had suspended Van Rootselaar's ChatGPT account after it had been flagged internally for chats describing gun violence scenarios. After multiple OpenAI employees had reviewed and discussed the chats internally, OpenAI determined that Van Rootselaar should be banned from the platform for "misuse of [its] models in furtherance of violent activities."[6] OpenAI did not escalate the matter to law enforcement, however, after determining that the content of the chats did not constitute an imminent danger or a credible risk of serious physical harm. After the mass shooting, OpenAI disclosed Van Rootselaar's chat history to police.

Nationalizing AI?

On March 1, 2026, Nathan E. Sanders and Bruce Shneier argued in the *Globe and Mail* that "OpenAI has shown it cannot be trusted. Canada needs nationalized, public AI"[7] in response to OpenAI's connection – however loose – to the Tumbler Ridge mass shooting. They argue that privately-owned AI platforms are guided by commercial values that conflict with safety, transparency, and the public good. AI platforms, they argued, are concentrated in foreign jurisdictions and operate with limited transparency and democratic oversight.

This *Globe and Mail* column argued further that AI today functions like critical public infrastructure – such as public broadcasting, power grids, and highways – and that it is time for the federal government to create a nationalized, government-controlled AI. In practice, this could mean the creation of government-funded AI models overseen by public institutions or federal agencies. AI would be to information technology what the *CBC* is to broadcasting.

For Sanders and Schneier, AI is too powerful for its use across broad spectrums of society to be left to a free market. "By contrast," they concluded, "public AI developed by transparent, accountable agencies would allow democratic processes and political oversight to govern how these powerful systems function," which is an unsubstantiated assumption that governments are more transparent and accountable than private corporations.

This *Globe and Mail* column is not mere wishful thinking. In a September 2025 news release,[8] the federal government announced the launch of an *AI Strategy Task Force* and a

---

[6] Winter, Jesse. "Tumbler Ridge shooter's ChatGPT messages were flagged months before attack." The Globe and Mail. February 20, 2026. Malik, Aisha. "ChatGPT reaches 900M weekly active users" TechCrunch. February 27, 2026. https://techcrunch.com/2026/02/27/chatgpt-reaches-900m-weekly-active-users/?utm_source=chatgpt.com. Accessed April 22, 2026.

[7] Sanders, Nathan E., and Bruce Schneier. "OpenAI Has Shown It Cannot Be Trusted. Canada Needs Nationalized, Public AI." Schneier on Security. March 01, 2026. https://www.schneier.com/essays/archives/2026/03/openai-has-shown-it-cannot-be-trusted-canada-needs-nationalized-public-ai.html

[8] Government of Canada. Innovation, Science and Economic Development Canada. "Government of Canada Launches AI Strategy Task Force and Public Engagement on the Development of the Next AI Strategy."

"30-day national sprint that will help shape Canada's approach to AI" – an approach framed not merely as routine technological innovation but as a step toward securing "digital sovereignty" amidst "profound geopolitical shifts."[9]

Ottawa's ambition is not only to support investment in the development of privately-owned AI technology in Canada, however. In an April 15, 2026 news release, the federal government announced a national effort to "build one of the most advanced artificial Intelligence (AI) supercomputing systems."[10] Importantly, this infrastructure will be Canadian-owned, i.e., government-owned. Meanwhile, as part of its *Sovereign AI Compute Strategy*, the federal government is spending $700 million in developing AI computational infrastructure and capacity for Canadian users.

What the federal government is doing right now appears to check all the boxes for Sanders and Schneier: a state-owned AI model or models, developed and supported within Canada, and subject to Canadian laws and regulations.

Increased regulation of AI?

The family of child victim Maya Gebala of the Tumbler Ridge mass shooting has filed a lawsuit in the Supreme Court of British Columbia against OpenAI, alleging that OpenAI acted negligently by not reporting Van Rootselaar's chat history to law enforcement. In their *Notice of Civil Claim*, the family (plaintiffs) characterized ChatGPT as a "trusted confidante, collaborator, ally, and friend" and alleged that Van Rootselaar "relied on ChatGPT for mental health and counselling, treating ChatGPT as a mental health counsellor, advisor, and/or pseudo therapist."[11]

The plaintiffs argue, therefore, that OpenAI had a "duty of care to report instances of clear and imminent risks of serious bodily harm or death posed to individuals identified with reasonable specificity..."[12] The lawsuit effectively asks the court to expand duty of care obligations to an AI platform and even frames ChatGPT as an active participant in or facilitator of the mass shooting.

Shortly after the mass shooting, federal AI Minister Evan Solomon summoned OpenAI's top safety representatives to Ottawa to explain its escalation policies for flagged AI chats. "They will come here, and we will have a sit-down meeting to have an explanation of their safety protocols and when they escalate and their thresholds of escalation to police, so we

---

September 2025. https://www.canada.ca/en/innovation-science-economic-development/news/2025/09/government-of-canada-launches-ai-strategy-task-force-and-public-engagement-on-the-development-of-the-next-ai-strategy.html.

[9] Ibid

[10] Ibid.

[11] Van Rootselaar's family. Notice of Civil Claim. Supreme Court of British Columbia. https://www.courthousenews.com/wp-content/uploads/2026/03/tumbler-ridge-openAI.pdf, at page 8.

[12] Ibid.

have a better understanding of what's happening and what they do," Minister Solomon told reporters.[13]

Minister Solomon expressed disappointment with that meeting. OpenAI safety representatives had informed him that the company's policy is to escalate conversations to law enforcement only when they indicate "an imminent and credible risk of serious physical harm to others."[14]

In response to OpenAI's alleged negligence, the federal government has contemplated three solutions: banning ChatGPT in Canada,[15] forcing OpenAI to modify its escalation policies (which OpenAI has since done),[16] or introducing federal legislation to regulate all AI companies operating in Canada (which Minister Solomon and Justice Minister Sean Fraser have threatened).[17]

Later, on March 4, 2026, Minister Solomon informed OpenAI CEO Sam Altman that "Canadian experts need to assess ChatGPT conversations that have been flagged for signs that users intend to cause imminent harm whether to alert law enforcement...."[18] British Columbia Premier David Eby has called for the federal government to legislate a minimum threshold of reporting "to make sure that the protection of the community, the protection of children, comes before the interests of shareholders"[19] – an argument similar to the one proposed by Sanders and Shneier.

Both nationalization and regulation point in the same direction: bringing Canadians' use of AI within the sphere of federal government surveillance and/or control.

---

[13] Cecco, Leyland. "Canada seeks answers from OpenAI for failing to alert police after suspending school shooter's account." The Guardian. February 23, 2026. https://www.theguardian.com/world/2026/feb/23/openai-tumber-ridge-shooter-account-suspended

[14] Singh, Divyadeep. "ChatGPT's parent company, OpenAI, banned Tumbler Ridge, B.C., school shooter's account, mulled alerting Canadian police, but held back over this reason." The Economic Times. February 21, 2026. https://economictimes.indiatimes.com/news/international/canada/chatgpts-parent-company-openai-banned-tumbler-ridge-b-c-school-shooters-account-mulled-alerting-canadian-police-but-held-back-over-this-reason/articleshow/128636101.cms

[15] Woolf, Marie. February 25, 2026. "Ottawa warns of legislation if OpenAI doesn't make changes after chat history raised red flags." The Globe and Mail. February 25, 2026. https://www.theglobeandmail.com/politics/article-openai-justice-minister-legislation-tumbler-ridge-shooter-chat-history/

[16] Hunter, Justine and Joe Castaldo. "OpenAI says recent policy changes would have flagged Tumbler Ridge shooter's messages to police." The Globe and Mail. February 26, 2026. https://www.theglobeandmail.com/canada/article-openai-chatgpt-tumbler-ridge-shooter-reporting-policies-changes/. Accessed April 10, 2026.

[17] Tumilty, Ryan. "Canada's AI minister says OpenAI to change ChatGPT after Tumbler Ridge shooting." The Star. March 06, 2026. https://www.thestar.com/politics/federal/canada-s-ai-minister-says-openai-to-change-chatgpt-after-tumbler-ridge-shooting/article_0c5daccf-e6dd-4bfd-b657-6e154a5caf23.html. Accessed April 10, 2026.

[18] Castaldo, Joe. "AI Minister tells OpenAI Canadian experts must assess flagged ChatGPT conversations." The Globe and Mail. March 04, 2026. https://www.theglobeandmail.com/business/article-ai-minister-tells-altman-canadian-experts-must-assess-flagged-chatgpt/ Accessed April 10, 2026.

[19] Ibid.

Is nationalization or regulation of AI even effective?

The events at Tumbler Ridge call into question whether legislative measures of nationalizing or regulating AI would have been effective at preventing the tragedy in the first place. A full eight months separated the attack from Van Rootselaar's use of ChatGPT. Simultaneously, Van Rootselaar had prior contact with law enforcement, who had removed firearms from the home in 2024 but then returned them less than one month before the shooting.[20] Would a state-controlled or heavily regulated AI sector have made a difference in this case?

Further, assuming – as Sanders and Schneier do in the *Globe and Mail* article – that bringing AI under government control would ensure greater transparency and accountability is to assume that governments are inherently more transparent, more accountable, and more competent stewards of such powerful digital systems as AI than private corporations. While we are not suggesting that private corporations always have clean hands, this assumption is not self-evident and is contradicted by recent federal legislative developments such as C-2, C-8, and C-22. These Bills would expand government powers to demand access to user data, while allowing them to keep such demands secret from users affected.

What nationalization or heavy regulation of AI would achieve, however, is several serious negative constitutional implications for Canadians' rights and freedoms.

Constitutional implications of AI nationalization and regulation

Canadians care deeply about the preservation of public safety and good order, especially in the wake of a mass shooting. If legislative or policy responses to Tumbler Ridge ought to be pursued, such measures must and can respect the *Charter* rights and freedoms of Canadians. But a state-owned or heavily regulated AI sector would achieve the opposite.

1. Government bias and "influence"

If history and precedent are any guide, a nationalized or heavily regulated AI platform is likely to be subject to the biases and ambitions of the government controlling it.

For example, in its regulation of the privately owned broadcasting industry, the federal government requires that broadcasters and online streaming services air mandatory levels of so-called "Canadian" content. What constitutes "Canadian" content, however, is determined by the federal government. With the passage of the *Online Streaming Act*[21] in 2023, all streaming services (e.g., Netflix, YouTube, and Spotify) now fall under the

---

[20] Pruden, Jana G, Matthew Scace, and Alanna Smith. "United in grief: Tight-knit Tumbler Ridge community pulls together in face of 'unimaginable' tragedy." Published February 13, 2026. Accessed April 28, 2026. https://www.theglobeandmail.com/canada/article-tumbler-ridge-community-tragedy-school-shooting/

[21] Parliament of Canada. *Bill C-11: The Online Streaming Act.* 44th Parliament, 1st session. Accessed April 10, 2026. https://www.parl.ca/legisinfo/en/bill/44-1/c-11

regulatory authority of the CRTC, allowing it to influence algorithms and the "discoverability" of content, regardless of consumer taste, thereby affecting what consumers are more likely to see.

Further, thanks to the 2023 *Online News Act*, [22] Meta no longer allows Canadians to post links to news stories on Facebook and Instagram – disrupting how millions of Canadians access information about the world. Despite public pressure and even international threats of retaliation,[23] the federal government has not repealed or amended the legislation.

These powers to interfere with Canadians' online experience may not long be limited to broadcasted content or online news.

A federal government controlling a nationalized AI model will have the authority to program how that model is used by researchers, innovators, and ordinary Canadians. And this is precisely the kind of programmability called for by Sanders and Schneier: if privately owned AI companies cannot be trusted to report users' alarming chats to law enforcement, then simply develop a state-controlled AI platform that cannot "fall asleep at its post." But government influence or control for nefarious purposes is not beyond the pale. Only four years ago, the perfectly legal activity of donating to a peaceful protest was subject to financial surveillance and resulted in the freezing of bank accounts, demonstrating that the government is not always a force for good.

Whether state interference arises through a state-owned AI model or through increasing regulation of privately-owned AI companies, the state would be able to intervene upon or "guide" users' AI interactions precisely because those interactions would be occurring within the scope of the state's authority, however private those interactions may feel to users.

2. Erosion of privacy

When the state owns and controls AI platforms, the line between private use and state oversight disappears. Canadians are already familiar with environments where their behaviour feels private but is not.

Employees understand that employers have the right (as well as the technical capacity) to monitor all activity occurring on company-issued hardware and software, despite how private those communications may *feel* to the employee. Citizens who enjoy public libraries understand that these state-owned institutions often maintain records of every borrowed book, magazine, and film and could, therefore, inferentially construct a profile of the citizens' interests, education level, and political leanings over time. In the same way, Canadians using a state-owned AI model would understand that the state would have both

[22] Parliament of Canada. *Bill C-18: The Online News Act.* 44th Parliament, 1st session. Accessed April 10, 2026. https://www.parl.ca/legisinfo/en/bill/44-1/c-18

[23] Boynton, Sean. "Republican bill takes aim at Online Streaming Act and threatens retaliation." Global News. Posted March 19, 2025. Accessed April 10, 2026. https://globalnews.ca/news/11738344/cusma-online-streaming-act-us-bill-tariffs/

the right and technical capacity – even if not exercised – to monitor and set constraints upon all uses of the AI model. Whether users enjoyed privacy would depend entirely on the government choosing voluntarily to refrain from seeing which Canadians are accessing AI, as well as the contents of those interactions. This is a fragile safeguard.

The regulation of privately-owned AI companies generates the same privacy concern, though to a lesser extent. Private AI companies that are regulated by government would be one degree removed from the state. However, the state could still dictate to AI companies what counts as "user inputs to be reviewed by law enforcement" and order these regulated corporations to turn over private communications to law enforcement. Out of an abundance of caution, to avoid being accused of failing to comply, regulated AI companies may opt to surrender to law enforcement any user inputs that raise even the remotest suspicion. It would be rational for any AI company operating in Canada to use this "better safe than sorry" approach, with the unfortunate and predictable consequence of non-criminal private information being disclosed to law enforcement. In this scenario, AI companies would proactively disclose to law enforcement concerning user inputs *before* police involvement and *outside* the traditional warrant process. In essence, AI companies would be deputized as intermediaries in an expanding program of state surveillance.

Canadian courts on privacy protections

Section 8 of the *Canadian Charter of Rights and Freedoms* protects Canadians against unreasonable search and seizure.[24] This constitutional protection underpins personal autonomy, dignity, privacy, control over our personal information, and freedom from state surveillance.

The Supreme Court of Canada has repeatedly affirmed that section 8 of the *Charter* protects a broad and meaningful right to privacy in the digital age. In *R v. Spencer (2014)*,[25] the Court held that privacy includes the right to control the dissemination of personal information and emphasized that anonymity is a central component of that protection. The Court has further recognized that individuals maintain a reasonable expectation of privacy in their electronic communications, even when those communications are stored or transmitted through third-party systems (*R v. Marakah 2017*;[26] *R v. Reeves 2018*).[27]

Most importantly, the Court has cautioned that the state cannot circumvent constitutional protections by relying on intermediaries to obtain information it could not lawfully access directly (*R v. Duarte, 1990*).[28]

Applied to AI, these principles carry significant implications. AI interactions often reveal the "biographical core" of personal information: users' thoughts, questions, and

---

[24] Government of Canada. *The Canadian Charter of Rights and Freedoms*. Justice Centre for Constitutional Freedoms. https://www.jccf.ca/the-canadian-charter-of-rights-and-freedoms/
[25] R. v. Spencer, 2014 SCC 43, [2014] 2 S.C.R. 212. Para. 49
[26] R. v. Marakah, 2017 SCC 59, [2017] 2 S.C.R. 608. Para. 10
[27] R. v. Reeves, 2018 SCC 56, [2018] 3 S.C.R. 531. Para. 17-22
[28] R. v. Duarte, [1990] 1 S.C.R. 30.

developing ideas. When these interactions are directly monitored by the state, or when private companies are effectively compelled to disclose them, this undermines the very protections that *Charter* section 8 is designed to guarantee. Whether privacy is violated by the state or by private companies that hand data over to the state, the result is the same: access to deeply personal information without meaningful judicial oversight, contrary to the constitutional requirement that state intrusion be carefully limited, authorized, and justified.

Restricting autonomy: thought, intellectual exploration, and expression

Limitations of the *Charter* section 8 protections against unreasonable search and seizure undermine Canadians' capacity to fully enjoy freedom of expression, personal autonomy, and freedom from unjustified state interference – the overarching ambition of the *Charter*.

Freedom of expression depends on a prior freedom – the freedom to explore ideas privately before presenting them publicly. Writers, researchers, students, and ordinary citizens must be able to experiment with unfamiliar or unsettling ideas without fear that their preliminary thoughts will be recorded, analyzed, or judged. If AI users come to believe that their interactions are monitored, self-censorship becomes a rational and prevalent behaviour. Individuals will avoid speculative questions, controversial topics, or imaginative scenarios that may be misconstrued as criminal intent. Innovation slows when people hesitate to test unconventional lines of inquiry. Democratic debate weakens when citizens refrain from developing arguments in private before expressing them in public.

Indeed, AI users often engage with difficult or even disturbing subject matter for a wide range of lawful purposes: academic research, creative writing,[29] professional analysis, or personal reflection. A regulatory framework that encourages or requires the reporting of "concerning" user inputs risks collapsing these distinctions. In practice, government regulation of AI may treat exploratory or expressive activity as suspicious, particularly where context is incomplete or misunderstood. The result is not only the potential for over-reporting, but the erosion of a space in which individuals can think, question, and create without fear of misinterpretation. At issue is the inability of AI systems – and those who regulate them – to reliably distinguish between harmful intent and legitimate exploration. And, where citizens' right to privacy is concerned, *reliability matters*.

Privacy invasion and self-censorship – A case study

After it was discovered in 2013 that the National Security Agency (NSA) had been conducting mass surveillance operations on millions of American phones, email accounts, chat forums, and online behaviours and transactions, many writers reported self-censoring in order to avoid state scrutiny. According to a 2013 survey of American writers

[29] According to an Authors Guild survey of professional novelists, 67 percent of writers are using AI writing tools.

by Pen America and the FDR Group,[30] 85 percent of survey participants (all of them writers) stated that they were concerned with government surveillance. Sixty-six percent stated that they disapproved of the government collecting internet and telecommunications data as part of their war on terrorism.[31]

The survey revealed that 16 percent of writers avoided writing or speaking about certain topics in order to avoid negative repercussions.[32] This expressive reluctance was particularly pronounced among writers and researchers inclined to criticize the government or address sensitive topics, including foreign policy, national security, and criticisms of government.

Such self-censorship reflects the risk inherent in expanding state oversight of AI interactions.

Bill C-22 and AI

Bill C-22, the *Lawful Access Act*,[33] is the federal government's latest attempt at "lawful access" legislation – a longstanding ambition of the federal governments, starting with Bill C-74, the *Modernization of Investigative Techniques Act*,[34] in 2005. If passed, the Bill could introduce state surveillance of AI by lowering the threshold for law enforcement to access user data.

Bill C-22 was introduced on March 12, 2026, as a successor to the strongly criticized *Strong Borders Act* (Bill C-2), which introduced broad surveillance powers and warrantless access provisions. Presented as "keeping Canadians safe" legislation, Bill C-22 is (at the time of writing) before the Standing Committee on Public Safety and National Security.

Bill C-22 expands police and intelligence access to Canadians' digital data, including user interactions with AI. It requires "electronic service providers" to assist police and intelligence in acquiring that data. The Bill defines "electronic service" very broadly as involving the "creation, recording, storage, processing, transmission, reception, emission or making available of information in electronic, digital or any other intangible form…"[35] This covers practically all communications between people and between people and digital systems all of the time, except for hard-copy letters, newspapers, flyers, posters and billboards. The Bill defines "electronic service provider" very broadly as including

---

[30] The FDR Group. "Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor." November 12, 2013. https://pen.org/report/chilling-effects/

[31] Ibid.

[32] Ibid.

[33] Parliament of Canada. *Bill C-22: An Act Respecting Lawful Access.* 45th Parliament, 1st Session. First Reading. Accessed April 10, 2026. https://www.parl.ca/legisinfo/en/bill/45-1/c-22.

[34] Parliament of Canada. Bill C-74: Modernization of Investigative Techniques Act. 38th Parliament, 1st Session. Accessed April 10, 2026. https://www.parl.ca/DocumentViewer/en/38-1/bill/C-74/first-reading

[35] Parliament of Canada. *Bill C-22: An Act Respecting Lawful Access.* 45th Parliament, 1st Session. First Reading. Accessed April 10, 2026. https://www.parl.ca/legisinfo/en/bill/45-1/c-22. Part Two, 2(1).

individuals as well as corporations like internet service providers, phone carriers, email providers, social media platforms, messaging apps, and potentially *any entity offering online services to the Canadian public*.[36, 37]

In short, Bill C-22 applies to essentially all non-paper communications between all Canadians at all times, and to every individual and organization that makes information available in an electronic, digital, or any other intangible form.

If Bill C-22 passes, the federal government will have the authority to order electronic service providers to develop capacity for organizing and extracting data for law enforcement review,[38] to install devices facilitating the transfer of information to law enforcement,[39] and to retain users' metadata for up to one year.[40]

Importantly, Bill C-22 lowers the legal threshold for lawful access to users' subscriber information and metadata from "reasonable grounds to *believe*" to "reasonable grounds to *suspect*" – making it easier for police to obtain sensitive subscriber information. Judges will be able to issue search warrants based on the *possibility* of a crime occurring rather than the *probability* that a crime will occur.

As for metadata retention requirements, University of Ottawa law professor and Canada Research Chair Michael Geist stated,

> *"Buried in the second half of Bill C-22 is a provision granting the government the power to require "core providers" to retain categories of metadata, including transmission data, for up to one year. This is mandatory metadata retention that would require telecom and electronic service providers to store information about the communications of all their users, regardless of whether those users are suspected of anything. It is one of the most privacy invasive tools a government can deploy, and the international experience suggests that there are major privacy risks."*[41]

While metadata, or "data about data," does not capture the *content* of communication, it does capture the *context* of communication – users' IP addresses, time of access, services used, whom you communicated with, frequency and duration of use, etcetera. As inputs in sophisticated computational models, this data is often sufficient to reveal to law enforcement patterns of behaviour, relationships, associations, interests, and habits. Over time, law enforcement can construct an incomplete but nonetheless revealing portrait of

---

[36] Ibid.
[37] Bill C-22 defines "electronic service provider" as "a person that, individually or as part of a group, provides an electronic service, including for the purpose of enabling communications, and that (a) provides the service to persons in Canada; or (b) carries on all or part of its business activities in Canada." Part Two, 2(1).
[38] Parliament of Canada. *Bill C-22: An Act Respecting Lawful Access.* Part Two, 5(2)(a)
[39] Parliament of Canada. *Bill C-22: An Act Respecting Lawful Access.* Part Two, 5(2)(a)
[40] Parliament of Canada. *Bill C-22: An Act Respecting Lawful Access.* Part Two, 5(3)(c)
[41] Geist, Michael. "The Lawful Access Privacy Risks: Unpacking Bill C-22's Expansive Metadata Retention Requirements." *Michael Geist Blog*. March 17, 2026. https://www.michaelgeist.ca/2026/03/the-lawful-access-privacy-risks-unpacking-bill-c-22s-expansive-metadata-retention-requirements/

the *biographical core* of a person. While law enforcement would still require judicial authorization to demand such data, with a lowered legal threshold to do so, this puts all Canadians at greater risk of unprecedented government surveillance of the digital services they use.

While Bill C-22 has not been framed as a solution to preventing mass shootings or other specific crimes, the lowered legal threshold to obtain subscriber information and users' metadata that this legislation introduces, would nonetheless grant government and law enforcement much broader powers to extract user information from electronic service providers. And this would likely include AI companies like OpenAI.

Conclusion

Prime Minister Mark Carney, during his visit to Tumbler Ridge in February, stated, "Obviously, anything that anyone could have done to prevent that tragedy or future tragedies must be done" – an understandable and appropriately human reaction to any mass shooting. Canadians face the challenging but familiar question: how to achieve the highest level of public safety while respecting the fundamental freedoms and privacy rights of citizens. Ottawa's response to a devastating, though isolated, mass shooting cannot be disproportionate, especially where the civil liberties of all Canadians are concerned. It should not use a human tragedy as the pretext for passing laws that bring Canada closer to becoming a surveillance state.

Policy responses now under consideration – nationalizing artificial intelligence, expanding regulatory mandates over private AI companies, and advancing sweeping lawful access powers through Bill C-22 – will draw Canadians' private interactions with AI chatbots under state surveillance and control. While prompted by a tragic event, these proposals would normalize government access to personal information and private thought in ways that violate the *Charter's* protections of privacy, expression, and autonomy.

All government access to private user data must be subject to robust warrant requirements and confined to circumstances where such access is necessary to address serious, imminent, and credible threats. Rather than lowering the threshold for obtaining warrants, as Bill C-22 proposes, Parliament should maintain a high standard while ensuring that the warrant process operates with sufficient speed and efficiency.

At the same time, this report does not suggest that AI companies have clean hands. Today's AI systems can infer sensitive information about users beyond what users themselves disclose, generating highly accurate profiles and insights that users neither anticipate nor fully control. This raises legitimate privacy concerns that may justify carefully tailored government regulation.

Canadians are therefore caught between competing pressures: government expansion of surveillance capacities in the name of public safety, and private AI corporations harvesting personal data in the name of innovation and consumer experience. How to navigate

between these pressures – without eroding fundamental freedoms – will be one of the defining policy challenges of our time.

A principled path forward is possible. Parliament should:

- Resist calls to nationalize or centrally control AI systems
- Reject Bill C-22 and its metadata retention and compelled-access provisions
- Maintain robust warrant requirements for all state access to personal data, limiting such access to circumstances involving serious, imminent, and credible threats

Canadians need a legal and regulatory framework that preserves spaces to think, explore, and communicate freely – secure in the knowledge that their *Charter* rights remain intact.

Bibliography

Bélisle-Pipon, Jean-Christophe. “Danger Was Flagged but Not Reported: What the Tumbler Ridge Tragedy Reveals About Canada’s AI Governance Vacuum.” *The Conversation*. February 25, 2026. https://theconversation.com/danger-was-flagged-but-not-reported-what-the-tumbler-ridge-tragedy-reveals-about-canadas-ai-governance-vacuum-276718.

Betke, Carl. “The Origins and Development of Social Insurance in Canada.” *Journal of Canadian Studies*. Accessed April 10, 2026. https://www.semanticscholar.org/paper/The-Origins-and-Development-of-Social-Insurance-in-Betke/3db31eb84da64e7ea68d3c8de04de868cf0c5306.

Boynton, Sean. “Republican bill takes aim at Online Streaming Act and threatens retaliation.” Global News. Posted March 19, 2025. Accessed April 10, 2026. https://globalnews.ca/news/11738344/cusma-online-streaming-act-us-bill-tariffs/

Castaldo, Joe. “AI Minister tells OpenAI Canadian experts must assess flagged ChatGPT conversations.” The Globe and Mail. March 04, 2026. https://www.theglobeandmail.com/business/article-ai-minister-tells-altman-canadian-experts-must-assess-flagged-chatgpt/ Accessed April 10, 2026.

Cecco, Leyland. “Canada seeks answers from OpenAI for failing to alert police after suspending school shooter’s account.” The Guardian. February 23, 2026. https://www.theguardian.com/world/2026/feb/23/openai-tumber-ridge-shooter-account-suspended

Chatterji, Aaron, Cunningham, Deming, et al. “How People Use ChatGPT.” National Bureau of Economic Research. Working Paper. September 2025. https://www.nber.org/system/files/working_papers/w34255/w34255.pdf

European Parliament. “EU AI Act: First Regulation on Artificial Intelligence.” Accessed April 10, 2026. https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence.

Geist, Michael. “A Tale of Two Bills: Lawful Access Returns with Changes to Warrantless Access but Dangerous Backdoor Surveillance Risks Remain.” *Michael Geist Blog*. March 2026. https://www.michaelgeist.ca/2026/03/a-tale-of-two-bills-lawful-access-returns-with-changes-to-warrantless-access-but-dangerous-backdoor-surveillance-risks-remains/.

Geist, Michael. “The Lawful Access Privacy Risks: Unpacking Bill C-22’s Expansive Metadata Retention Requirements.” *Michael Geist Blog*. March 2026. https://www.michaelgeist.ca/2026/03/the-lawful-access-privacy-risks-unpacking-bill-c-22s-expansive-metadata-retention-requirements/.

Government of Canada. Department of Justice. *Canadian Charter of Rights and Freedoms*. Section 2. Accessed April 10, 2026. https://www.justice.gc.ca/eng/csj-sjc/pl/*Charter*-charte/c2_2.html.

Government of Canada. Innovation, Science and Economic Development Canada. “Government of Canada Launches AI Strategy Task Force and Public Engagement on the Development of the Next AI Strategy.” September 2025. https://www.canada.ca/en/innovation-science-economic-development/news/2025/09/government-of-canada-launches-ai-strategy-task-force-and-public-engagement-on-the-development-of-the-next-ai-strategy.html.

Hunter, Justine and Joe Castaldo. “OpenAI says recent policy changes would have flagged Tumbler Ridge shooter’s messages to police.” The Globe and Mail. February 26, 2026. https://www.theglobeandmail.com/canada/article-openai-chatgpt-tumbler-ridge-shooter-reporting-policies-changes/. Accessed April 10, 2026.

Justice Centre for Constitutional Freedoms. “Federal Court Upholds Ruling Against Government Use of the Emergencies Act.” Accessed April 10, 2026. https://www.jccf.ca/western-standard-freedom-wins-again-federal-court-upholds-ruling-against-trudeaus-emergencies-act-overreach/.

Justice Centre for Constitutional Freedoms. *Mission Creep: Is It Time to Abolish the CRTC?* Calgary: Justice Centre for Constitutional Freedoms, March 21, 2026. https://www.jccf.ca/wp-content/uploads/2026/03/Mission-creep-It-it-time-to-abolish-the-CRTC_Final_March-21-2026-1.pdf.pdf.

Justice Centre for Constitutional Freedoms. *Privacy Collapse and the Expanding Surveillance State*. Calgary: Justice Centre for Constitutional Freedoms, February 2026. https://www.jccf.ca/wp-content/uploads/2026/02/Privacy-collapse-and-the-expanding-surveillance-state_FINAL.pdf.

Malik, Aisha. “ChatGPT reaches 900M weekly active users” TechCrunch. February 27, 2026. https://techcrunch.com/2026/02/27/chatgpt-reaches-900m-weekly-active-users/

Office of the Privacy Commissioner of Canada. *Personal Information Protection and Electronic Documents Act (PIPEDA).* Accessed April 10, 2026. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

Parliament of Canada. *Bill C-22: An Act Respecting Lawful Access*. 45th Parliament, 1st Session. First Reading. Accessed April 10, 2026. https://www.parl.ca/legisinfo/en/bill/45-1/c-22.

Parliament of Canada. *Bill C-8: An Act to Amend Certain Acts and to Make Certain Consequential Amendments (Digital Charter Implementation).* 45th Parliament, 1st Session. Accessed April 10, 2026. https://www.parl.ca/legisinfo/en/bill/45-1/c-8.

Parliament of Canada. *Bill C-11: The Online Streaming Act.* 44th Parliament, 1st session. Accessed April 10, 2026. https://www.parl.ca/legisinfo/en/bill/44-1/c-11

Parliament of Canada. *Bill C-18: The Online News Act.* 44th Parliament, 1st session. Accessed April 10, 2026. https://www.parl.ca/legisinfo/en/bill/44-1/c-18

Parliament of Canada. *Bill C-2: An Act Respecting Certain Measures Relating to Public Safety and National Security.* 45th Parliament, 1st Session. Accessed April 10, 2026. https://www.parl.ca/legisinfo/en/bill/45-1/c-2.

Parliament of Canada. Bill C-74: *Modernization of Investigative Techniques Act.* 38th Parliament, 1st Session. Accessed April 10, 2026. https://www.parl.ca/DocumentViewer/en/38-1/bill/C-74/first-reading

Pillay, Tharin. "AI Emotional Intelligence Support Bots." *Time Magazine*. Accessed April 10, 2026. https://time.com/7379564/ai-emotional-intelligence-support-bots/.

Pruden, Jana G, Matthew Scace, and Alanna Smith. "United in grief: Tight-knit Tumbler Ridge community pulls together in face of 'unimaginable' tragedy." Published February 13, 2026. Accessed April 28, 2026. https://www.theglobeandmail.com/canada/article-tumbler-ridge-community-tragedy-school-shooting/

Sanders, Nathan E., and Bruce Schneier. "OpenAI Has Shown It Cannot Be Trusted. Canada Needs Nationalized, Public AI." Schneier on Security. March 01, 2026. https://www.schneier.com/essays/archives/2026/03/openai-has-shown-it-cannot-be-trusted-canada-needs-nationalized-public-ai.html

Singh, Divyadeep. "ChatGPT's parent company, OpenAI, banned Tumbler Ridge, B.C., school shooter's account, mulled alerting Canadian police, but held back over this reason." The Economic Times. February 21, 2026. https://economictimes.indiatimes.com/news/international/canada/chatgpts-parent-company-openai-banned-tumbler-ridge-b-c-school-shooters-account-mulled-alerting-canadian-police-but-held-back-over-this-reason/articleshow/128636101.cms

Supreme Court of Canada. R. v. Duarte, [1990] 1 S.C.R. 30.

Supreme Court of Canada. R. v. Marakah, 2017 SCC 59, [2017] 2 S.C.R. 608.

Supreme Court of Canada. R. v. Reeves, 2018 SCC 56, [2018] 3 S.C.R. 531.

Supreme Court of Canada. R. v. Spencer, 2014 SCC 43, [2014] 2 S.C.R. 212.

Supreme Court of Canada. *Saskatchewan (Human Rights Commission) v. Whatcott*, 2013 SCC 11, [2013] 1 S.C.R. 467

The FDR Group. "Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor." November 12, 2013. https://pen.org/report/chilling-effects/

Tumilty, Ryan. "Canada's AI minister says OpenAI to change ChatGPT after Tumbler Ridge shooting." The Star. March 06, 2026. https://www.thestar.com/politics/federal/canada-s-ai-minister-says-openai-to-change-chatgpt-after-tumbler-ridge-shooting/article_0c5daccf-e6dd-4bfd-b657-6e154a5caf23.html. Accessed April 10, 2026.

Woolf, Marie. February 25, 2026. “Ottawa warns of legislation if OpenAI doesn’t make changes after chat history raised red flags.” The Globe and Mail. February 25, 2026. https://www.theglobeandmail.com/politics/article-openai-justice-minister-legislation-tumbler-ridge-shooter-chat-history/