CANADIAN MUSLIM PUBLIC AFFAIRS COUNCIL

Bill C-22: CMPAC Submission to the Standing Committee on Public Safety and National Security

---

Introduction

The Canadian Muslim Public Affairs Council (CMPAC) is a non-partisan organization dedicated to advancing civil liberties, democratic participation, and the protection of human rights in Canada. Through its advocacy and public policy work, CMPAC has consistently engaged issues relating to discrimination, government accountability, and the impact of public policy on marginalized communities.

Legislative efforts to expand state surveillance and information-gathering powers have repeatedly raised concerns regarding the protection of fundamental rights and freedoms. While protecting public safety is a legitimate and important objective, such measures must remain consistent with the Canadian Charter of Rights and Freedoms and Canada's broader human rights obligations.

Bill C-22 would expand state access to personal information while weakening important safeguards designed to protect fundamental rights and freedoms. The legislation raises significant concerns for privacy, freedom of expression, freedom of association, freedom of religion, and equality rights, particularly given the documented impact surveillance and security measures have had on different communities and racialized groups.

For these reasons, CMPAC urges Parliament to carefully scrutinize the necessity, proportionality, and potential consequences of the powers proposed in Bill C-22.

Position on Bill C-22

CMPAC is concerned that if enacted, Bill C-22 will significantly expand state surveillance powers while lowering important privacy safeguards governing access to personal information. These changes raise serious concerns regarding privacy rights, freedom of expression, freedom of association, freedom of religion, and equality rights protected under the Canadian Charter of Rights and Freedoms.

Such concerns cannot be separated from the lived experience of communities that have historically[1] been disproportionately affected by Canada's national security and law enforcement frameworks. Muslim communities in Canada have long experienced the consequences of intelligence gathering, information sharing, and security investigations that were later shown to be based on flawed assumptions, unreliable intelligence, or discriminatory profiling. As a result, proposals that expand surveillance authorities without sufficient evidence of necessity warrant particularly careful scrutiny.

Based on these concerns, CMPAC calls on Members of Parliament to reject Bill C-22 and vote against its adoption. Should the legislation proceed through Parliament, substantial amendments must be made to

---

[1] Reem Bahdi, ""All Arabs Are Liars": Arab and Muslim Stereotypes in Canadian Human Rights Law" (2019) 31:1 J L & Soc Pol'y 92.

strengthen safeguards, increase oversight, and mitigate discriminatory impacts on racialized and religious minority communities.

Part 1: Timely Access to Data and Information

a. Lowering Standards to "Reasonable Grounds to Suspect"

Under Bill C-22, law enforcement would be authorized to obtain subscriber information based on the lower evidentiary threshold of "reasonable grounds to suspect" rather than "reasonable grounds to believe". While subscriber information is often characterized as simple identifying details, the information captured under the legislation extends to usernames, pseudonyms, device data, and online identifiers

Lowering this evidentiary threshold normalizes broader state access to personal information while providing insufficient safeguards against discriminatory or overbroad investigations. Where surveillance powers are exercised on the basis of mere suspicion, there is a heightened risk that individual or institutional biases will influence investigative decision-making. For Muslim, Arab, and Palestinian Canadians who frequently face unwarranted flags due to naming conventions[2], charitable giving[3], or foreign connections[4], this standard heightens the risk of unfair law enforcement targeting. The threshold for obtaining subscriber information must remain "reasonable grounds to believe".

b. Deterrence of Advocacy and Infringement on Charter Rights

The expansion of lawful access powers directly deters civic engagement, producing severe chilling effects on Charter-protected civil liberties, including the protection against unreasonable search and seizure[5], freedom of expression[6], freedom of peaceful assembly[7], freedom of association[8], and freedom of religion[9].

Numerous studies[10] have documented that individuals who believe they may be subject to monitoring are more likely to self-censor their speech, limit their participation in civil society activities, and avoid engagement with controversial political issues.

For Muslim, Arab, and Palestinian advocacy groups, raising awareness on foreign policy and human rights is frequently subjected to scrutiny and mischaracterization. Lowering privacy protections signals that active democratic engagement carries personal and digital risk. This risk is reinforced by a post-9/11[11]

---

[2] Richard Marcuse, ed, Racial Profiling: A Special BCCLA Report on Racial Profiling in Canada (Vancouver: BC Civil Liberties Association, 2010).
[3] "Project Profile: Under Layered Suspicion", online: University of Toronto Digital Humanities Networkhttps://dhn.utoronto.ca/project/under-layered-suspicion/.
[4] Uzma Jamil, "Can Muslims Fly? The No Fly List as a Tool of the “War on Terror”" (2017) 4:1 Islamophobia Studies J 72 [Jamil].
[5] Canadian Charter of Rights and Freedoms, s 8, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11.
[6] *Ibid*, s 2(b).
[7] *Ibid*, s 2(c).
[8] *Ibid,* s 2(d).
[9] *Ibid*, s 2(a).
[10] Karen Gullo, "Surveillance Chills Speech—As New Studies Show—And Free Association Suffers", (19 May 2016), online: *Electronic Frontier Foundation* https://www.eff.org/deeplinks/2016/05/when-surveillance-chills-speech-new-studies-show-our-rights-free-association.
[11] Tabasum Akseer, *Understanding the Impact of Surveillance and Security Measures on Muslim Men in Canada*, Martello Papers No 42 (Kingston: Centre for International and Defence Policy, Queen’s University, 2018), online: https://www.queensu.ca/cidp/sites/cidpwww/files/uploaded_files/Martello42EN.pdf.

national security environment marked by long-standing surveillance of mosques[12], charitable organizations[13], student associations[14], and community leaders[15].

Expanding state access to personal information transforms these concerns into active deterrents, eroding core Charter guarantees and undermining trust between affected communities and public institutions.

c. Expansion of Warrantless Emergency Powers (Section 14)

Section 14 of Bill C-22[16] proposes to amend section 487.11 of the Criminal Code to expand powers that may be exercised when "by reason of exigent circumstances it would be impracticable to obtain a warrant". Currently, in an emergency situation, an officer may without a warrant exercise general search authority under section 487 or place a tracking device on things under section 492.1. If adopted, in addition to these powers, police officers would be able to, without a warrant:

- Installing a tracking device on a person, a power provided for in section 492.1(2), which typically requires a warrant based on reasonable grounds to believe;
- Installing a transmission data recorder, a power provided for in section 492.2(1);
- Obtaining the disclosure of transmission data, a power provided for in section 487.016;
- Obtaining the disclosure of location data, a power provided for in section 487.017;
- Obtaining the disclosure of subscriber information under section 487.0142.

The authority to install a tracking device on an individual, rather than an object, enables real-time tracking of a person's physical movements. This power would be exercised without any prior judicial authorization, based solely on an officer's subjective assessment that urgency justifies it, and without the affected person ever being informed.

Leaving the determination of an "emergency situation" to police discretion poses acute risks to Muslim, Arab, and Palestinian community members who attend public demonstrations, political rallies, or places of worship, exposing them to arbitrary tracking without judicial oversight. Specifically, removing prior judicial authorization allows pre-existing institutional biases within law enforcement to reframe lawful religious gatherings, community mobilization, or Palestinian human rights advocacy as urgent security threats, resulting in unchecked location tracking and the profiling of entire racialized and faith communities under the guise of exigent circumstances.

---

[12] Baljit Nagra & Paula Maurutto, "Anti-Muslim Surveillance: Canadian Muslims' Experiences with CSIS" (2023) 9:3 Soc Race & Ethnicity 311.

[13] "Report: Humanitarianism and the Exclusion of Muslim Charities from the Financial Sector", (30 April 2026), online: *Institute of Islamic Studies, University of Toronto* https://islamicstudies.artsci.utoronto.ca/report-humanitarianism-and-the-exclusion-of-muslim-charities-from-the-financial-sector/.

[14] Paula Maurutto & Baljit Nagra, "Racializing Surveillance: The Impact of the Security Certificate Regime on Young Canadian Muslims" (2022) 13:1 Islamophobia Studies J 73.

[15] *Ibid.* at 11.

[16] Ligue des droits et libertés, *Bill C-22: An Act Respecting Lawful Access — Establishing a Surveillance Architecture in Canada* (Brief submitted to the Standing Senate Committee on National Security, Defence and Veterans Affairs, 29 October 2026), online: https://liguedesdroits.ca/wp-content/fichiers/2026/11/brief_ligue_C22_Senate_20261029.pdf.

d. Authorization of "Publicly Available Information"

Bill C-22 permits law enforcement to obtain and act on any "publicly available information" without requiring a production order or warrant, yet fails to provide a legal definition of what constitutes such information.

Allowing law enforcement agencies unlimited authority to gather and utilize information simply because it is accessible online poses serious risks. Personal data posted on public platforms or social media does not grant state authorities free license to collect, aggregate, or monitor that data without consent or judicial oversight, as reinforced by privacy standards in the Clearview AI decision.[17] Palestinian rights organizers, Arab civil society groups, and Muslim youth groups rely heavily on public digital platforms for community outreach. Without strict statutory limits, unrestricted social media monitoring will be weaponized to map lawful political dissent and advocacy under the guise of open-source intelligence collection.

e. Facilitating Transnational Repression and International Data Sharing

Transnational repression[18] is an ongoing threat in Canada[19], where foreign state actors intimidate, monitor, and harass diaspora communities to silence criticism and undermine democratic participation. Rather than insulating vulnerable populations, Bill C-22 contains provisions that will actively facilitate cross-border abuse by foreign governments.

Section 29 of Bill C-22 amends the Mutual Legal Assistance in Criminal Matters Act (MLACMA) to allow Canadian authorities to enforce foreign orders and share subscriber and transmission data held in Canada with foreign governments based on the low evidentiary standard of "reasonable grounds to suspect". Furthermore, proposed section 487.0181 allows Canadian authorities to request and process data from foreign telecommunications entities under the same reduced standard.

This cross-border information sharing framework establishes a dangerous channel for foreign interference. Canadian Muslim, Arab, and Palestinian communities frequently maintain active ties with family members living under authoritarian regimes or foreign military occupations. Under Bill C-22, foreign states could exploit these data-sharing provisions to request information on Canadian activists, journalists, or dissenters under the pretext of investigating foreign offenses. Transmitting private user data or online identifiers to foreign entities exposes Canadian residents and their relatives abroad to threats, harassment, arbitrary arrest, and physical harm, effectively weaponizing Canadian state infrastructure to assist foreign repression.

---

[17] Office of the Privacy Commissioner of Canada, *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta*, PIPEDA Findings #2021-001 (2 February 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/.

[18] Phil Gurski & Marie Lamensch, *Transnational Repression in Canada: A Threat to Democracy and Public Safety*(Montreal: Montreal Institute for Global Security, 2026), online: https://migsinstitute.org/wp-content/uploads/2026/02/Transnational-repression-in-Canada_MIGS.pdf.

[19] Noura Al-Jizawi et al, *Psychological and Emotional War: Digital Transnational Repression in Canada*, Citizen Lab Research Report No 151 (Toronto: Citizen Lab, University of Toronto, 2022), online: https://utoronto.scholaris.ca/server/api/core/bitstreams/84d7937d-3383-48e7-9b0d-51ba9a70b4ef/content.

CANADIAN MUSLIM PUBLIC AFFAIRS COUNCIL

Part 2: Supporting Authorized Access to Information Act (SAAIA)

a. The SAAIA Creates a Framework for Discriminatory Surveillance

Of greatest concern in Bill C-22 is the proposed creation of the Supporting Authorized Access to Information Act (SAAIA).

Through both public regulations and secret ministerial orders, the SAAIA would permit the government to require electronic service providers (ESPs) to develop, maintain, and modify systems that facilitate access to information by law enforcement and intelligence agencies. While these powers are presented as tools for addressing serious criminal activity, the legislation fails to adequately consider how expanded surveillance infrastructure may disproportionately impact communities that have historically been subjected to heightened scrutiny.

CMPAC is also concerned by the exceptionally broad definition of “electronic service provider” contained within the legislation. The scope of the definition appears capable of extending well beyond telecommunications companies to encompass a wide range of organizations that Canadians rely upon for communication, financial services, travel, education, health services, and community engagement. The breadth of this definition substantially expands the potential reach of surveillance authorities and raises important questions regarding necessity, proportionality, and the scope of information that may become accessible to the state.

Canada's national security framework must be understood in light of its impact on affected communities. Muslims have disproportionately borne the burden of security measures and surveillance practices. This history underscores the importance of ensuring that any expansion of state powers is accompanied by robust safeguards and meaningful oversight.

While Bill C-22 is technologically different from previous national security legislation, it raises similar concerns. Expanded access to communications-related information, metadata, and network data creates opportunities for authorities to identify, map, and monitor entire communities rather than focusing on individuals for whom there exists credible evidence of wrongdoing.

CMPAC is further concerned that powers authorizing the modification of technical systems may create cybersecurity vulnerabilities that undermine the security of Canadians' communications and personal information. Any framework that facilitates government access to digital information should ensure that it does not weaken encryption protections, create new technical vulnerabilities, or increase the risk of unauthorized access by malicious actors, foreign governments, or cybercriminals. Measures introduced in the name of public safety should not come at the expense of the security and integrity of digital communications.

The government has not demonstrated why existing investigative authorities are insufficient, nor has it assessed whether these new powers may disproportionately impact racialized and religious minority communities. For these reasons, CMPAC recommends that Parliament require a comprehensive Charter and Equality Impact Assessment prior to the implementation of any powers authorized under the SAAIA.

Such an assessment should evaluate:

- Potential impacts on freedom of religion, freedom of expression, and freedom of association;
- Potential discriminatory effects on racialized, Indigenous, immigrant, refugee, and religious minority communities;
- Whether less intrusive alternatives exist;
- Whether the proposed powers are necessary and proportionate to their stated objectives.

Without such an assessment, Parliament cannot adequately evaluate whether the legislation complies with Canada's constitutional and human rights obligations.

b. Market Withdrawal

The technical access mandates under the SAAIA threaten to isolate Canada from the global secure communications ecosystem. Encrypted messaging provider Signal[20] has publicly stated that it would rather pull out of Canada entirely than be compelled to compromise on the privacy promises it has made to its users. Technical researchers have emphasized that Bill C-22 could force application makers to collect intrusive user metadata, including conversation mappings and location details. If platforms like Signal withdraw from the Canadian market, Canadian citizens, human rights defenders, and advocacy groups will be stripped of vital digital security shields.

Losing access to these secure tools leaves vulnerable Muslim, Arab, and Palestinian communities directly exposed to cyberthreats, hostile state interception, and illegal surveillance. This market withdrawal would disproportionately impact these communities by removing the confidential channels they rely on to organize, engage in human rights advocacy, and communicate with families in foreign regimes without fear of state reprisal or targeted harassment.

Recommendations

CMPAC's recommendations are intended to minimize harm and to ensure the bill is implemented in a manner that effectively addresses public safety while remaining consistent with the Canadian Charter of Rights and Freedoms and the longstanding principles within the Criminal Code of Canada. Without substantial amendments, the bill risks undermining the rights and freedoms it seeks to protect.

Given the concerns outlined above, CMPAC recommends that Parliament:

1. Reject Bill C-22 in its current form
2. Withdraw Part 2 (Supporting Authorized Access to Information Act) in its entirety pending further consultation and independent review.

Should Parliament proceed with Part 2, CMPAC recommends:

1. Conducting a Charter and Equality Impact Assessment prior to implementation.

---

[20] Martin Shelton, "Signal could leave Canada over metadata bill", (20 May 2026), online: *Freedom of the Press Foundation* https://freedom.press/digisec/blog/signal-could-leave-canada-over-metadata-bill/.

2. Repealing the mandatory metadata retention provisions entirely, or, at minimum, converting them into a judicial production order regime that replaces the standard of "reasonable suspicion" with "reasonable grounds to believe".
3. Upgrading the oversight of secret ministerial orders from a standard of semi-judicial approval by the Intelligence Commissioner to a requirement for full, prior judicial authorization by a superior court judge.
4. Expanding NSIRA's review authority and access to information regarding the operation of the SAAIA.
5. Establishing mandatory transparency and public reporting requirements.
6. Creating a permanent advisory body including representatives from affected communities and civil society organizations.
7. Requiring regular parliamentary review of the regime.
8. Ensuring that all powers exercised under the SAAIA comply with Canada's domestic and international human rights obligations, including protections relating to privacy, equality, freedom of religion, freedom of expression, and freedom of association.
9. Prohibiting cross-border data transfers under MLACMA or proposed section 487.0181 without prior judicial authorization satisfying the court that the disclosure will not facilitate transnational repression, human rights violations, or targeted harassment of Canadian residents and their families abroad.
10. Adding an explicit statutory guarantee that no regulation, order, or directive can force service providers to weaken end-to-end encryption, mandate backdoor channels, implement client-side scanning, or compromise digital security.

Conclusion

Bill C-22 proposes a significant expansion of state surveillance powers while weakening important safeguards governing access to personal information. Although framed as a response to evolving technological challenges, the government has not demonstrated that existing authorities are insufficient or that the powers contained in this legislation are necessary and proportionate.

The concerns raised extend beyond privacy rights alone. Expanded state access to personal information, tracking capabilities, and communications infrastructure directly threatens freedom of expression, freedom of association, freedom of religion, and equality rights under the Charter. These impacts fall disproportionately on communities that have historically experienced heightened scrutiny under Canada's national security framework, including Muslim, Arab, and Palestinian communities.

Compromising encryption protocols, permitting warrantless tracking, facilitating international data sharing, and driving secure platforms like Signal out of Canada weakens national digital security and exposes citizens to foreign interference and transnational repression.

CMPAC supports legitimate efforts to protect public safety. However, such efforts must remain consistent with Canada's constitutional values and international human rights obligations. For these reasons, CMPAC urges Members of Parliament to reject Bill C-22. Should the legislation proceed, significant amendments are required to strengthen safeguards, enhance accountability, and ensure that expanded surveillance authorities do not come at the expense of fundamental rights and freedoms.