Stakeholder Perspectives & Debates

A neutral, structured synthesis of the arguments surrounding the Lawful Access Act

1 Overview

The introduction of Bill C-22, the *Lawful Access Act, 2026*, has ignited a intense national discussion. Balancing the investigative needs of law enforcement against the privacy rights of Canadian citizens is one of the most complex policy challenges of the digital age.

This section presents a balanced, evidence-based overview of the major viewpoints, dividing stakeholders into **Proponents** (advocating for national security and digital modernization) and **Critics** (focusing on constitutional rights, cybersecurity, and regulatory burden).

---

2 1. Proponents: Law Enforcement & Government

Proponents argue that Canada's digital surveillance laws are dangerously out of date, leaving investigators in the dark when addressing modern, digital-native crimes.

2.1 Key Stakeholders:

- Department of Justice and Attorney General of Canada [2].
- Public Safety Canada and the Royal Canadian Mounted Police (RCMP).
- Canadian Association of Chiefs of Police (CACP).

2.2 Core Arguments:

1. **Closing the "Going Dark" Gap:** Law enforcement agencies argue that end-to-end encryption and volatile communication platforms have rendered traditional wiretap warrants ineffective [2]. Modern tools are required to keep pace with cybercriminals [2].
2. **Combating High-Harm Crime:** Proponents stress that subscriber details and metadata are vital for the early stages of investigations into child exploitation, human trafficking, terrorism, and sophisticated cyberattacks on critical infrastructure [2].
3. **Allied Legislative Alignment:** Proponents point out that Canada's allies (such as the UK with its Investigatory Powers Act and the US with its Electronic Communications Privacy Act frameworks) have long had structured subscriber production and international sharing tools [2]. Bill C-22 brings Canada up to speed [2].

---

3 2. Critics: Civil Liberties, Privacy, & Tech Sector

Critics contend that the Bill is an overreach that damages the privacy rights of all Canadians, creates structural security vulnerabilities, and places an unfair burden on local businesses.

3.1 Key Stakeholders:

- Office of the Privacy Commissioner of Canada (OPC) [3].
- Google Canada [10].
- Dr. Michael Geist (Canada Research Chair in Internet and E-Commerce Law, University of Ottawa) [5], [7].
- Canadian Civil Liberties Association (CCLA) and the BC Civil Liberties Association (BCCLA) [4].
- Justice Centre for Constitutional Freedoms (JCCF) and board member Dr. John Robson [9].
- Digital rights organizations (OpenMedia [8], Citizen Lab).
- Canadian tech startups and Electronic Service Providers.

3.2 Core Arguments:

1. **Mass Surveillance & The Metadata Myth:** Privacy advocates dispute the claim that metadata is "harmless non-content" [3], [4]. A year of metadata—revealing whom you speak with, when, from where, and how often—maps a highly intimate profile of an individual's personal life [3], [4]. A blanket 1-year retention mandate is criticized as a form of mass surveillance [4], [8]. Dr. Michael Geist highlighted this gap following the

government's May 2026 briefings [5], noting that while law enforcement presented narrow use cases (e.g. tracking a discarded phone), the bill writes in sweeping, country-wide data retention powers that are vastly disproportionate to those targeted needs [5]. Google added that a blanket one-year metadata mandate forces the retention of highly sensitive transmission data well beyond operational needs, impacts non-suspect users, and amplifies the impact of potential security breaches [10].

2. **Constitutional Section 8 Violations:** Legal experts raise concerns that "Confirmation of Service Demands" require zero judicial oversight [3], [4], [5], and that Subscriber Production Orders only require "reasonable grounds to suspect" (a low legal threshold) [3], [4], [5], which may violate Section 8 of the *Canadian Charter of Rights and Freedoms* (protection against unreasonable search and seizure) [4], [5].
3. **Threats to Cyber Security:** Cybersecurity researchers warn that mandating decryption and "surveillance by design" weakens the security architecture of platforms [6], [7], [8], potentially creating backdoors that could be exploited by malicious foreign actors or hackers [6], [7], [8]. Google similarly warns that the current definition of "systemic vulnerability" is dangerously narrow (only covering unauthorized access, excluding data integrity/availability, and applying only to services rather than hardware), which could be used to force backdoors that break end-to-end encryption and create critical cybersecurity risks [10].
4. **Economic Cost to Local Tech:** Startups and small service providers argue that establishing metadata storage databases and compliance structures is cost-prohibitive, making it difficult for Canadian tech companies to compete with international platforms that might evade enforcement [7]. Furthermore, Geist warns that small local developers capturable under the broad definition of ESPs will face severe compliance and financial hurdles, stifling digital innovation in Canada [7]. Google also contends that these boundless capability obligations undermine companies' ability to innovate, forcing them to support legacy services they would otherwise deprecate, and threatening to fragment the product experience globally [10].
5. **Broad Civic Opposition and National Petition:** A national petition signed by 42,344 Canadians was delivered to Parliament by Dr. John Robson on behalf of the JCCF, calling on Members of Parliament to defeat Bill C-22 [9]. The JCCF argues that privacy is a fundamental pillar of a free society—protecting freedom of thought, expression, and association—and that the legislation's surveillance expansions create a system of disproportionate monitoring [9].

---

4 3. Technical Mandates and the "Tech Exodus" Debate

A central flashpoint of the Bill C-22 debate is the requirement under the *Supporting Authorized Access to Information Act (SAAIA)* for electronic service providers to develop and maintain

technical interception capabilities. This has led to intense pushback from international privacy firms and domestic developers, warning of a potential "tech exodus" from the Canadian market.

4.1 Technical and Juridical Concerns

- **The Threat of Exit (VPN and Messaging Services):**
  - **Signal:** Udbhav Tiwari, Vice President of Strategy and Global Affairs, warned that the company "would rather pull out of the country than be compelled to compromise on the privacy promises we have made to our users." [6]
  - **NordVPN:** Stated that if subjected to mandatory obligations under Bill C-22, "there isn't a scenario in which we would compromise our no-logs architecture or encryption protections. To prevent this, we will consider all viable options, including limiting or, if necessary, removing our presence from Canadian jurisdiction." [6]
  - **Windscribe (Canadian VPN Provider):** CEO Yegor Sak noted the unique threat to domestic companies, stating that they would actively look at relocating their headquarters and corporate taxes outside of Canada rather than destroy the essence of their service. He noted: "Signal isn't headquartered in Canada so they can just shut off Canadian servers, but our HQ is… We'll move HQ and take our taxes elsewhere." [6]
- **Compelled Backdoors and Spyware:** Apple and Meta have warned [6] that the capability mandates could force companies to break end-to-end encryption, install government spyware, or insert backdoors. Apple stated that they would never build backdoors into their products.
- **Google's SECU Committee Brief:** In a formal submission to the House of Commons Standing Committee on Public Safety and National Security (SECU) [10], Google outlined severe technical and legal objections to Part 2 of Bill C-22. The company declared: "Google has never built a backdoor or other mechanism to circumvent end-to-end encryption in our products. If we say a product is end-to-end encrypted, it is end-to-end encrypted." [10] Google warned that the scope of s. 5 and s. 7 obligations is "largely boundless" and could enable the government to compel product design changes, creating severe security vulnerabilities [10]. Google further criticized the secret Ministerial Orders framework (ss. 7-13) as an unnecessary, executive-led replacement for court-supervised assistance warrants, stating that permanent non-disclosure orders insulate executive decisions from scrutiny and expose platforms to severe regulatory and civil liability without a means of legal defense [10]. To resolve these concerns, Google proposed concrete legislative amendments, including the outright elimination of ministerial orders, adding strict restrictions to prohibit government-mandated product design changes, and broadening the definition of "systemic vulnerability" to explicitly protect end-to-end encryption [10].

- **Confidentiality in Governance:** Conservative MP Jacob Mantle highlighted the widespread political reliance on encrypted communication, noting that MPs depend on Signal precisely because it is confidential.
- **U.S. Congressional Intervention:** The heads of the U.S. House Judiciary and Foreign Affairs committees sent a joint letter [6] to Public Safety Minister Gary Anandasangaree, warning that SAAIA would "drastically expand Canada's surveillance and data access powers in ways that create significant cross-border risks to the security and data privacy of Americans." They cautioned that compelling American companies to build backdoors introduces systemic vulnerabilities that could be exploited by hackers, foreign adversaries, and cybercriminals.

4.2 Government Rebuttal and Defenses

- **No Backdoors or Spyware:** Simon Lafortune, spokesperson for the Public Safety Minister's Office, categorically rejected assertions [6] that the bill requires companies to introduce "backdoors" or install spyware on their systems. He stated: "We want to reassure Signal and all service providers that we are not legislating to require them to install capabilities to enable surveillance and any assertions otherwise are false."
- **Warrant Requirements:** The government emphasizes that authorities would still be required to obtain explicit legal authorization, such as a court-issued warrant, to access any user data.
- **Rejection of U.S. Warnings:** Simon Lafortune characterized the joint warning letter [6] from U.S. Congressional committee leaders as reflecting a "misunderstanding" of how the bill would function, maintaining that Bill C-22 is a critical tool to prevent and investigate modern crime in a Charter-compliant manner.

---

5 Comparative Matrix of Key Debates

Issue	Proponents' Position	Critics' Position
Metadata Retention	Necessary for tracing volatile cybercrime connections after the fact.	Massive privacy invasion; database target for hacking. Google argues it duplicates existing targeted Criminal Code preservation tools and impacts non-suspects [10].

Issue	Proponents' Position	Critics' Position
Subscriber Data Standard	"Reasonable suspicion" is appropriate for identity details.	Identity data is highly sensitive; must require a full warrant standard.
Interception Capability	Vital for executing court-ordered interception warrants.	Weakens cybersecurity; discourages local end-to-end encryption. Google warns it stifles innovation, forces legacy support, and risks breaking E2EE unless the definition of systemic vulnerability is broadened to protect encryption [10].
Oversight & Ministerial Orders	Review committees and judicial authorization safeguard citizens; executive orders ensure prompt provider cooperation.	Lack of initial judicial review on Section 1 demands is unconstitutional. Google and civil society argue secret Ministerial Orders bypass judicial oversight, enforce permanent secrecy, and expose platforms to severe regulatory risks [10].
Tech Exodus & Jurisdiction	Capability mandates are narrow; concerns about forced backdoors or spyware are based on "misunderstandings."	Privacy-centric firms (Signal, NordVPN, Windscribe) threaten to withdraw or relocate HQs due to encryption risks. Google notes boundless capability mandates threaten to fragment global product experiences [10].

6 Analytical Conclusions

The debate surrounding Bill C-22 highlights a fundamental tension: the government seeks to expand public safety tools in a borderless digital world, while civil society aims to preserve the privacy and cryptographic security that underpins modern free speech and commerce. As

the bill undergoes committee review, lawmakers are tasked with finding a middle ground—potentially narrowing the scope of metadata retention or increasing the judicial oversight required for subscriber demands.

---

7 Sources

1. Bill C-22: Parliament of Canada: Bill C-22 - Lawful Access Act, 2026 (Date Added: 2026-05-22)
2. Department of Justice: Department of Justice Canada: Legislative Backgrounder (Date Added: 2026-05-21)
3. Office of the Privacy Commissioner of Canada: Submission on Bill C-22 (Date Added: 2026-05-21)
4. Canadian Civil Liberties Association (CCLA): Overreach Concerns on the Lawful Access Act (Date Added: 2026-05-21)
5. Dr. Michael Geist: Critique on the Government's Use Cases and Overreach (Date Added: 2026-05-21)
6. Global News: Tech Companies Threaten Exit Over Lawful Access Mandates (Date Added: 2026-05-22)
7. Dr. Michael Geist: Tech Exodus - SAAIA's Privacy and Security Risks (Date Added: 2026-05-22)
8. OpenMedia Canada: Save Our Encryption Campaign (Date Added: 2026-05-21)
9. Justice Centre for Constitutional Freedoms (JCCF): Canadians Call on Parliament to Stop Bill C-22 (Date Added: 2026-05-24)
10. Google Canada: Submission to the Standing Committee on Public Safety and National Security Regarding Bill C-22 (Date Added: 2026-05-26)

Last Updated: 2026-05-26