Part 2: Service Provider Obligations

An evaluation of technical capability mandates and the 1-year metadata retention rule under Bill C-22

1 Overview

Part 2 of the *Lawful Access Act, 2026* (Bill C-22) represents the most technically disruptive and financially significant aspect of the legislation. It places proactive obligations on Electronic Service Providers (ESPs)—defined broadly to include telecommunication companies, internet service providers (ISPs), and web applications offering messaging or storage—operating within Canada.

This section reviews the requirements under Part 2, focusing on the **Technical Interception Mandate**, the controversial **One-Year Metadata Retention Rule**, and the legal **Penalties for Non-Compliance**.

---

2 1. Technical Interception & Decryption Assistance

Under Section 5 [1] of the Act, service providers can no longer remain passive conduits for information. They are legally required to build "surveillance capability" directly into their products.

2.1 Three Core Mandates (Section 5):

1. **Surveillance by Design:** ESPs must ensure that their systems are designed to facilitate court-ordered interception and data extraction.
2. **Decryption Assistance:** ESPs are obligated to assist law enforcement by decrypting communications or data, provided that the decryption keys are technically controlled or held by the provider.

3. **Standardized Interfaces:** Providers must establish secure, standardized delivery pipelines to transmit intercepted data directly to law enforcement agency receiving points.

2.2 The Encryption Debate

The requirement for decryption assistance has raised alarms among cybersecurity researchers. While the bill specifies that decryption is only required "where technically feasible" (meaning it does not explicitly outlaw end-to-end encrypted apps where the provider does not hold the keys), experts warn that it creates regulatory pressure to weaken security protocols and avoid deploying true end-to-end encryption in Canada.

---

3 2. The One-Year Metadata Retention Rule

Section 6 [1] establishes a sweeping, national metadata retention system, allowing the government to implement regulations requiring ISPs and other web applications to store vast quantities of citizen digital footprint data.

3.1 Scope of Retained Data:

- **Routing & Connections:** All IP addresses, port allocations, routing records, connection timestamps, and cell tower identifiers.
- **Identifiers:** Sender and receiver identifiers, including telephone numbers, email headers, and usernames.
- **Exclusion of Content:** Crucially, Section 6(3) specifies that metadata *must not* include the actual audio or text content of any communication.

Retained for 1 Year (Yes)	Excluded Content (No)
• Connection timestamps • Source/Destination IP addresses • Port numbers & routing data • Cell tower location records	• Email text body • Chat messages • Voice calls • Video calls

3.2 Contrast with Existing Law

Under current Canadian law, telecommunications providers are not subject to blanket, proactive metadata retention mandates. Instead, the Criminal Code requires law enforcement to obtain a specific preservation order or warrant from a judge, compelling a provider to preserve the metadata of a specific individual under active investigation for a limited period (typically 30 to 90 days).

By contrast, Bill C-22 introduces a proactive "regulation-making authority" for "core" telecommunications providers to retain certain metadata types—including transmission and location data—"for reasonable periods of time not exceeding one year." The Minister of Public Safety could also order other Electronic Service Providers (ESPs) to retain such data, subject to approval from the federal Intelligence Commissioner.

3.3 Perspectives on Metadata Retention

3.3.1 Proponents and Investigative Value

- **Standardization of Timelines:** Richard Burchill, Director-General of Technical Investigative Services for the RCMP, testified [2] that internet transmission data and cell tower signaling data are critical for investigations. He argued that the one-year limit creates a "consistent" data retention standard. If a company only keeps data for three days, but a kidnapping investigation is one week old, that key data is lost forever regardless of judicial authorization.
- **Delayed Investigation Support:** Liberal MP Sima Acan noted that historical metadata is often essential for establishing timelines and connections that are not immediately obvious, especially when offenses are reported long after they occur.
- **Call for Extended Timelines:** Some law enforcement leaders have advocated for even longer retention. Thunder Bay Police Chief Darcy Fleury testified that the one-year limit is a "good start" but argued that a two- or three-year limit "would be ideal" for complex policing needs.
- **Scope Assurances:** Simon Lafortune, a spokesperson for the Public Safety Minister's Office, reassured the public that the bill only permits the retention of metadata (e.g., Device ID, IP address, device location, timestamps) and explicitly prohibits the retention of content, web browsing history, or social media activity.

3.3.2 Critics and Constitutional Concerns

- **Section 8 Charter Challenges:** Thompson Rivers University law professor Robert Diab points out [4] that courts have long recognized that the "mosaic of information" assembled from metadata can reveal intimate details of an individual's private life. He warns that compelling a third party to preserve communications records constitutes a

form of surveillance that interferes with Section 8 Charter rights (protection against unreasonable search or seizure), and expects a direct court challenge if the bill is passed.

- **The "Haystack" Analogy:** Dr. Michael Geist, a law professor at the University of Ottawa, argues [3] that building a massive database creates significant privacy and security risks for citizens, stating that the government is "building this massive haystack of data with the thought that they might need to find the needle every once in a while."
- **Department of Justice Stance:** In response to why the metadata provision was not mentioned in the government's official Charter statement, Ian McLeod of the Department of Justice explained [4] that the bill only creates a "regulation-making authority" rather than immediate retention mandates. Any future regulations would separately require a detailed Charter assessment. Additionally, Shannon Hiegel, the national security policy director general at Public Safety Canada, stated [4] that the government does not equate a company's retention of data with a "seizure" under the Charter because no production order is involved until a judicial warrant is approved.

3.4 International Context

The proposed metadata retention timeline places Canada in a unique position relative to its democratic peers:

- **Australia:** Mandates telecommunications metadata retention for up to two years under its lawful access framework.
- **United States:** Has no broad, proactive data retention timeline in federal law, instead relying on targeted preservation requests.
- **European Union:** Does not have a standard data retention timeline. While some member nations (such as Germany) have attempted to legislate blanket retention, these provisions have been repeatedly struck down by the European Court of Justice and domestic constitutional courts as unconstitutional and incompatible with fundamental rights.

3.5 Technical & Administrative Burden

For providers, retaining this data for every transaction in Canada for up to a year requires major investments in database infrastructure, security measures to prevent data breaches, and logging systems. Security experts have also cautioned that consolidating metadata creates attractive targets for malicious actors [5].

---

4 3. Enforcement & Penalties

To ensure compliance with these technical rules, Section 7 outlines heavy financial penalties.

- **Summary Conviction:** A fine of up to **$250,000** for each instance of non-compliance.
- **Conviction on Indictment:** A fine of up to **$1,000,000** for major or ongoing failures to implement interception capabilities or metadata retention databases.

---

5 Analytical Conclusions

Part 2 shifts the burden of national security and crime investigation onto private companies. By mandating "surveillance by design" and a blanket 1-year metadata archive, the Act transforms electronic service providers into active agents of state intelligence. This creates significant technical overhead for startups, raises the risk of massive data breaches of consolidated metadata, and represents a structural change in how digital privacy is configured in Canadian society.

---

6 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. Dr. Michael Geist: Critique on the Government's Use Cases and Overreach (Date Added: 2026-05-21)
4. Global News: Metadata Retention and Privacy Risks Explained (Date Added: 2026-05-22)
5. Dr. Michael Geist: Tech Exodus - SAAIA's Privacy and Security Risks (Date Added: 2026-05-22)

Last Updated: 2026-05-24