October 2026

Google Proposed Amendments to Bill C-22, the *Lawful Access Act, 2026*

Google appreciates that law enforcement and intelligence agencies face significant challenges in protecting the public against crime and terrorism, and we are committed to supporting their efforts. Our work to increase the cybersecurity protections of our users, while supporting law enforcement agencies' mandates to investigate and solve crimes, demonstrates that the goals of public safety and user security are compatible. As a global leader in building safe and secure products, including for government, public sector enterprise customers, and regulated industries, we believe it is critical to find ways to support law enforcement's important work without engineering vulnerabilities into products and services that weaken security for all users.

We take the privacy and security of our users very seriously. Our business is built on users' trust that we will keep their data safe and secure, and respect their privacy. Google products are private and secure by design and protected by one of the world's most advanced security infrastructures. We protect data with multiple layers of security, including leading encryption technologies like end-to-end encryption (E2EE), hypertext transfer protocol secure (HTTPS) and Transport Layer Security (TLS), where appropriate and technologically feasible. 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.

Since Bill C-22 was introduced, a broad cross-section of stakeholders—including technology companies, cybersecurity experts, civil society organizations, and business associations—have raised major concerns regarding its impact on user privacy and security, digital sovereignty, and global cybersecurity. While the House of Commons adopted certain amendments in June 2026, core issues regarding technical assistance mandates, secret ministerial orders, and metadata retention remain unresolved. The government has recently signaled openness to further refine the legislation to strengthen safeguards while preserving its core public safety objectives. Our updated proposed amendments achieve that balance: equipping law enforcement with effective tools while protecting the security and privacy of Canadians.

1. Technical assistance obligations remain overly broad, with the potential to allow the government to demand the creation of new surveillance infrastructure.

- The scope of the technical assistance obligations outlined in Sections 5(2)(a)-(b) of Part 2 is unclear and excessively broad. Without clear boundaries, C-22 could enable the government to require providers to change their products to create new surveillance capabilities on behalf of law enforcement.
- Further, while the regulation-making power Section 5 applies to core providers, Ministerial Orders could also subject any electronic service provider ("ESP") to the same obligations. The definition of ESP is extremely broad, and could be interpreted to apply to any entity or person operating in Canada. Therefore, the technical assistance provisions are potentially limitless in scope in two ways: (1) the substantive powers they grant; and (2) who those powers can be applied to.
- Creating new surveillance infrastructure would give rise to additional security vulnerabilities for users, would undermine user trust, and could pose conflict of laws issues.
- The extensive obligations on providers (both core providers and potential ESPs) may also undermine companies' abilities to innovate, and could force companies to continue supporting services that they would otherwise deprecate in favor of more innovative, useful, or pro-privacy offerings.

Recommendation: Bill C-22 should be amended to place reasonable limits on technical assistance powers.

Proposed Amendments:

Core providers — obligations

5(2) The Governor in Council may make regulations respecting the obligations of core providers~~;~~ respecting

~~(a)~~ the development, implementation, assessment, testing and maintenance of operational and technical capabilities, including capabilities related to extracting and organizing information that is authorized to be accessed and to providing access to such information to authorized persons~~;~~.

~~(b) the installation, use, operation, management, assessment, testing and maintenance of any device, equipment or other thing by core providers that may enable an authorized person to access information;~~

~~(c) notices to be given to the Minister or other persons, including with respect to any capability referred to in paragraph (a) and any device, equipment or other thing referred to in paragraph (b); and~~

~~(d) the retention of categories of metadata — including transmission data, as defined in section 487.011 of the Criminal Code — for reasonable periods of time not exceeding six months.~~

(3) In making a regulation under subsection (2), the Governor in Council must take into account the following factors:

(a) the benefits of the regulation to the administration of justice, in particular to investigations under the *Criminal Code*, and to the exercise of powers and the performance of duties and functions under the *Canadian Security Intelligence Service Act*;

(b) the feasibility of compliance with the regulation for the core providers;

(c) the costs to be incurred by the core providers to ensure compliance with the regulation;

(d) the potential impact of the regulation on the persons to whom the core providers provide services;

(e) the potential impact of the regulation on privacy protection and cybersecurity; ~~and~~

(f) international law and comity; and

~~(f)~~ (g) any other factor that the Governor in Council considers relevant.

Restrictions

(4) ~~Paragraph (2)(d)~~ Subsection (2) does not authorize the making of regulations that require core providers to (including facilitating or providing technical assistance to): ~~retain information that would reveal~~

(a) make changes to its products or services;

(b) collect and retain any data beyond what it requires for its own purposes;

(c) make any changes that would affect the functionality or security or require additional functionality for any products or services it provides; or

~~(a) the content — that is to say the substance, meaning or purpose — of information transmitted in the course of an electronic service;~~

~~(b) a person's web browsing history; or~~

~~(c) a person's social media activities.~~

2. Ministerial Orders undermine the principles of transparency and due process

- The Ministerial Order powers in Section 7 of Part 2 grant the Minister of Public Safety and Emergency Preparedness sweeping powers to mandate technical capability requirements in secret, without judicial authorization.
- This framework is highly problematic from the perspective of due process and the rule of law for many reasons, including:
    a. Public transparency is critical for the effective functioning of a democratic state, particularly in the context of state surveillance. If surveillance directives are made in secret, citizens cannot understand or scrutinize state power.
    b. Under the separation of powers framework, the judiciary plays an essential role as a check on executive power, ensuring that government actions remain constitutional. If a surveillance order is made in secret without judicial scrutiny, it is practically impossible for an affected individual to challenge its constitutionality in court.
    c. There is no automatic stay of a Ministerial Order when a provider applies for judicial review, meaning a company could be forced to deploy a secret capability that introduces security vulnerabilities while a court challenge is pending.
- The provisions that purport to limit the broad powers created by the Ministerial Order framework are inadequate:
    a. Approval by the Intelligence Commissioner of proposed Ministerial Orders is not an adequate substitute for prior judicial review and authorization due to the important role of the courts within Canada's democratic division of powers.
    b. Two-year sunsets on Ministerial Orders have limited practical value because these orders can be renewed indefinitely.

c. Granting the Minister discretion to permit disclosure does not provide sufficient safeguards protecting public transparency and state accountability - these provisions do not mandate or guarantee transparency. It is the orders that are made secret that may be most concerning to the public.

- Further, the creation of broad and unchecked state power through the Ministerial Order framework is unnecessary under Canadian law. The Criminal Code already contains mechanisms for law enforcement to request proportionate and constitutionally compliant judicial assistance orders.

Recommendation: Bill C-22 should be amended to remove the provisions permitting Ministerial Orders, which are fundamentally inconsistent with principles of transparency and due process.

Proposed amendments:

Remove sections 7-13 of Part 2.

3. Metadata mandates impose indiscriminate bulk data retention

- C-22's metadata retention provisions could permit the state to impose blanket metadata retention obligations, without any individualized suspicion. This treats all users as potential criminals. Metadata is not merely "administrative" data - in some cases, metadata can contain core biographical data that is fundamental to a citizen's private life.
- Mandatory metadata retention for the sole purpose of collecting information for law enforcement has been ruled a violation of privacy and protection of personal data numerous times in the Court of Justice of the European Union. Further, the Supreme Court of Canada has repeatedly held that individuals have reasonable expectation of privacy in metadata, attracting the protections against unreasonable search or seizure in section 8 of the *Charter*.
- Despite the reduction in the retention duration from 12 to six months, and the introduction of the "essential" statutory threshold, the framework still fundamentally contemplates general, population-level bulk retention of metadata without requiring targeted, individualized suspicion. Even with a six month window for data retention (as opposed to one year), the core cybersecurity risk of creating centralized, highly attractive "honeypots" for hackers remains.
- If used in combination with technical assistance regulation or Ministerial Order, Bill C-22 could also potentially require core providers or ESPs to proactively seek out and collect

new information they would not otherwise have reason to in the regular course of business.

- These provisions are unnecessary. Canadian law already contains mechanisms for targeted preservation orders, where data retention is constitutionally compliant, necessary and appropriate.

Recommendation: Bill C-22 should be amended to remove the metadata preservation provisions.

Proposed Amendment:

Remove the requirements contained in section 5(2)(d) of Part 2 of C-22.

> 5(2) The Governor in Council may make regulations respecting the obligations of core providers, respecting
>
> ...
>
> ~~(d) the retention of categories of metadata — including transmission data, as defined in section 487.011 of the Criminal Code — for reasonable periods of time not exceeding six months.~~

4. The definition of systemic vulnerability still fails to protect against requirements that could compromise the overall cybersecurity of products and services, including encryption.

- While the definition of systemic vulnerability in C-22 now protects against directly breaking end-to-end encryption, adjacent surveillance architectures—such as on-device client-side scanning—which do not technically "decrypt" data but undermine system security, are not addressed.
- This decryption safeguard purports to bring C-22 in line with U.S. law. However, C-22 continues to apply more broadly than the comparable U.S. statute, the Communications Assistance for Law Enforcement Act (CALEA), which applies only to telecommunications providers and requires prior judicial authorization to impose obligations on these providers.
- As written, the definition of systemic vulnerability is limited to electronic protections, which does not explicitly address other risks, such as to systems or hardware. It also fails to protect against the potential for a mandated introduction of new surveillance

capabilities that could be exploited, or a potential prohibition on new uses of end-to-end encryption or other cybersecurity protections.

- Further, Section 2(1) contains a critical loophole excluding risks that relate only to targets of a warrant, meaning that there is a risk that a "targeted" capability is not considered a "systemic" vulnerability. Even a “targeted” warrant may create an exploitable weakness. This is why any technical assistance requests must be subject to prior judicial authorization, so that an impartial party may weigh the risks to privacy of the individual, the security of the overall system, and the importance to public safety.

Recommendation: The definition of “systemic vulnerabilities” in section 2(1) of Part 2 should be amended to clarify that it protects technical security measures, including but not limited to encryption.

Proposed Amendments:

Remove the definition of "electronic protection” in s. 2(1) of Part 2.

> ~~***electronic protection*** means authentication, encryption and any other prescribed type of data protection. (protection électronique)~~

Replace the definition of “systemic vulnerability” in s. 2(1) of Part 2 as follows:

> ***systemic vulnerability*** means a vulnerability ~~in the electronic protections of an electronic service~~ that creates a credible risk, based on recognized international technical standards, to the confidentiality, integrity, authenticity, security or availability of data, information, services, devices, hardware, firmware or systems. For greater certainty, a systemic vulnerability includes, but is not limited to, any requirement on a core provider or electronic service provider to remove, circumvent or undermine the encryption of information including, but not limited to, end-to-end encryption. ~~that secure information could be accessed by a person who does not have any right or authority to do so, other than a risk that relates only to information related to persons with respect to whom a warrant, order or other authority to access information conferred under the Criminal Code or the Canadian Security Intelligence Service Act — or any similar authority conferred under another Act of Parliament — applies.~~(vulnérabilité systémique)