Canadian Telecommunications Association - Recommendations – Bill C-22

1. Part 1 - Confirmation of service demand

Bill C-22 retains the requirement that **all** confirmation of service demands can require a response in as little as 24 hours of receipt. Such proposal is impractical for three reasons.

(a) Volume of demands

First, the confirmation of service demand is expected to generate a significant increase in the number of requests that telecommunication service providers (TSPs) receive from law enforcement. By way of background, prior to the *R v Spencer* decision[1], when judicial authorization was not generally required to obtain basic subscriber information, a 2011 CTA survey of mobile wireless providers indicated that respondents collectively handled more than 1.1 million requests from law enforcement and government agencies in a single year. Since then, the number of connected Canadians has grown significantly: mobile wireless subscriptions have increased from 27.3 million in 2011 to 37.7 million in the second quarter of 2025 (nearly a 40% rise), while home internet subscriptions have grown from 10.7 million to 14.6 million over the same period (an increase of approximately 36%). As a result, the volume of confirmation of service demands could exceed 2011 levels by a considerable margin, with a corresponding increase in operational demands on TSPs.

(b) Complexity of some searches

Second, the 24-hour response time oversimplifies the verification process. While it may seem that a confirmation of service request requires only a simple lookup of business records, the time required to respond can vary significantly depending on the type of identifier provided by law enforcement.

In some cases, such as when a MSISDN (phone number), Subscriber Identity Module (SIM), or International Mobile Subscriber Identity (IMSI) is provided, the process can be relatively straightforward. Even then, service providers must verify that the identifier was associated with the correct customer account during the relevant timeframe, considering factors such as number re-use or changes in account ownership.

Other identifiers require additional analytical steps. Internet Protocol (IP) addresses are a good example. Generally, most IP addresses are not static or permanently assigned to a single subscriber. In most consumer and many enterprise contexts, IP addresses are dynamically allocated, change over time, and can be shared across multiple users. As a result, an IP address request cannot be processed without a precise timestamp and time zone (and, in wireless cases, a source port). Each IP address must be queried individually. Depending on the network configuration, service providers may need to determine the IP type, map public to private addresses where applicable, identify the associated equipment or service identifier at that specific moment in time, and then confirm the relevant customer account. Some cases may require escalation to specialized technical experts that are not available on a 24/7 basis.

[1] *R. v. Spencer,* 2014 SCC 43

Similarly, an International Mobile Equipment Identity (IMEI) identifies only a device, not a subscriber, meaning service providers must first analyze usage or call detail records to determine the associated service identifiers before confirming that the device is associated with a service account and determine the service period.

In short, the complexity and response time are driven by the identifier supplied and the network context in which it must be analyzed. While some requests can be handled quickly, others require multiple system queries, cross-verification across billing and network records, and in some cases involvement of specialized teams.

While we appreciate law enforcement's desire to receive confirmation in a timely manner, any regulatory regime must recognize that not all requests are alike, and a one-size-fits-all response time is neither operationally practical nor reflective of the varying levels of technical complexity involved.

(c) **Staff availability**

A 24-hour response time presumes that all telecommunication service providers have staff available on a 24/7 basis to respond to confirmation of service demands. This is not the case, particularly on weekends and holidays, and especially for smaller service providers.

While most service providers have developed processes that enable them to respond to the occasional truly urgent request from law enforcement (typically in much less than 24 hours), otherwise known as exigent circumstances, the proposed confirmation of service demand framework envisions that every demand can require a 24-hour level of urgency. No service provider should be required to maintain the staffing, resourcing, and procedural structures needed to treat every confirmation of service demand as an emergency.

A functioning framework must recognize that not all confirmation of service demands are equal and account for the fact that service providers vary greatly in size, technical capability, and operational resources.

Recommendation:

For the above reasons, allowing for response deadlines of as little as 24 hours creates a material risk of unmanageable demand and does not reflect the diversity of service provider capabilities.

The government should amend Part 1 of Bill C-22 to replace the current provision allowing confirmation of service demands with response times as short as 24 hours with a **reasonable** minimum timeline of "**no less than three business days**".

This approach provides a more reasonable timeframe to manage what are expected to be very high volumes of requests, particularly in a regime where there are no judicial or administrative oversight limits on the number of demands that may be issued. It would also better accommodate requests that require more complex or manual analysis, including those involving multiple systems or requiring validation and cross-referencing of records. It also recognizes that not all service providers have staff available on a 24/7 basis and will reduce the risk that compressed timelines could undermine the effectiveness of the very lawful access regime that this legislation seek to establish by diverting service provider resources from other important law enforcement support activities.

This approach would not prevent service providers, as they do today, from responding more quickly where circumstances permit. Rather, it would avoid establishing a statutory expectation that all requests can and must be treated as urgent, thereby supporting a more practical, reliable, and sustainable lawful access framework.

2. Production Orders

Bill C-22 proposes to shorten the timeframe within which recipients of production orders can apply to a court to revoke or vary a production order.[2] The rationale we have been given for this amendment is that law enforcement often has difficulty receiving production documents in a timely manner. This rationale fails to consider the underlying causes for why some production documents are delayed and fails to acknowledge that shortening the time to apply for a review of a production order does not address these causes, nor will it quicken access to information.

In practice, existing law already requires that any application to review a production order be brought before the production date specified in the order. As a result, the current framework does not permit recipients to delay compliance by pursuing a review after the production deadline. Shortening this timeframe further will therefore not accelerate access to information, as it does not change the obligation to produce records by the date set out in the order.

Where delays do occur, they are more often attributable to operational and practical factors unrelated to the review period. These can include the need to seek clarification from law enforcement regarding the scope or technical parameters of a request, to resolve ambiguities in how the order is drafted, or to identify workable alternative approaches where the request as framed cannot be fulfilled. In some cases, timely resolution of these issues is hindered by delays in receiving responses from the officer that requested the order, including situations where responsible officers are unavailable or unable to provide direction.

Absent such circumstances, telecommunications service providers comply with production orders within the timelines specified in the order. The suggestion that delays are driven by the availability of review mechanisms does not reflect operational reality.

Reducing the time available to seek judicial review would therefore not improve the timeliness of production. Instead, it would weaken an important procedural safeguard that allows recipients to challenge orders that may be overly broad, technically infeasible, or inconsistent with legal requirements. This safeguard plays a critical role in protecting the

---

[2] Bill C-22 – Part 1 – s.**10 Subsections 487.0193(1) and (2) of the Act are replaced by the following:**
Application for review of production order
487.0193 (1) A person, financial institution or entity required by an order made under any of sections 487.014 to 487.018 to produce a document may, before the person, institution or entity is required to produce the document but not later than 10 business days after the day on which the order was received, apply in writing to the justice or judge who made the order — or to a judge in the judicial district where the order was received — to revoke or vary the order.

privacy interests of Canadians and in ensuring that lawful access powers are exercised in a manner that is precise, proportionate, and consistent with the rule of law.

Recommendation:

For the above reasons, we respectfully submit that the proposed amendment to the timeframe in which recipients can seek the revocation or varying of a production order be removed from Bill C-22. A more effective approach would be to address the operational sources of delay—particularly communication and clarification processes between law enforcement and service providers—rather than limiting access to judicial oversight.

If, notwithstanding the above, policy-makers insist on shortening the timeframe within which recipients of production orders can apply to a court to revoke or vary a production order, the proposed timeline should be revised to 15 business days after the day on which the order is received. This would strike a more reasonable balance between the objective of ensuring timely access to information for law enforcement and the need to preserve a meaningful opportunity for recipients to assess, and where necessary challenge, production orders that could threaten the privacy interests of Canadians, including for reasons of being overly broad, technically unworkable, or inconsistent with applicable legal requirements.

3. Regulatory Obligations of Core Providers under the SAAIA

Part 2 of Bill C-22 creates the Supporting Authorized Access to Information Act (SAAIA) for the purpose of ensuring that authorized persons can easily obtain information held by electronic service providers in a legal context, for example in police investigations.

It creates two processes by which electronic service providers may be obligated to take measures:

- By regulatory obligations when designated as core providers;
- By ministerial order

(a) Unlimited obligations for core providers

Section 3 of the SAAIA states that the purpose of the Act is to "ensure that electronic service providers can facilitate the exercise of authorities to access information that are conferred on authorized persons."

However, as drafted, the regulation making authority and the corresponding obligations of core providers in subsection 5(2) of the SAAIA are not limited to this purpose:

> **5(2)** The Governor in Council may make regulations respecting the obligations of core providers, **including** regulations 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 that may enable an authorized person to access information; and
> **(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 one year.

As the Library of Parliament states in its legislative summary, subsection 5(2) provides that the obligations of core providers are to be established by regulations that "***potentially have to do with*** technical and operational capabilities require to extract and organize information..."[3] [emphasis added]. Given the potentially significant impact of regulations under subsection 5(2) on electronic service providers and the Canadian public, the authority to impose obligations on core providers should be limited to those specifically listed in the subsection and not open-ended.

Canadian statutory-interpretation and drafting principles presume that when Parliament lists specific subjects, it intends to confine the scope of delegated authority; open-ended powers must be expressed clearly and are not inferred. A closed list ensures that core-provider obligations remain within the bounds contemplated by Parliament and avoids unintended regulatory expansion with substantial cost, privacy, and operational consequences.

Recommendation:

The regulation making authority regarding the obligations of core providers in subsection 5(2) of the Act should be limited to specific items listed in the subsection. This is reflected in the proposed wording changes set out below.

Current Wording	Proposed Wording
5(2) The Governor in Council may make regulations respecting the obligations of core providers, including regulations 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;	**5(2)** The Governor in Council may make regulations respecting the following obligations of core providers~~, including regulations 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;

[3] Legislative Summary, Bill C-2, Preliminary Version, August 27, 2025, paragraph 2.15.1 at page 37.

(b) Obligation to retain metadata

As referenced above, subparagraph 5(2)(d) of the proposed SAAIA would authorize the government to require electronic service providers to retain a broad range of metadata for up to one year, including information that providers do not currently collect or retain for business purposes. While access to this data would still require lawful authorization, the obligation to proactively collect and store it represents a significant expansion in the volume and sensitivity of data held by private sector entities about individuals who are not suspected of any wrongdoing.

This approach raises important security and privacy considerations. Any policy that mandates the retention of large volumes of sensitive data necessarily increases the amount of information that must be protected against unauthorized access. In doing so, it expands the potential attack surface for cyber threats and increases the consequences of any breach. As recent incidents across both the public and private sectors have demonstrated, no system is immune from compromise. The most effective way to reduce risk is therefore to limit the amount of sensitive data that is collected and retained, and to ensure that retention periods are no longer than necessary.

In addition to cybersecurity risks, mandatory bulk retention requirements engage broader concerns regarding proportionality and necessity. Requiring the collection and storage of data relating to individuals not under investigation represents a significant departure from targeted, suspicion-based approaches that have traditionally guided lawful access frameworks in Canada.

Recommendation:

To address these concerns, we respectfully submit that the Committee consider the following before making any regulations or orders regarding metadata:

- **Limit the scope of required data retention** to what is demonstrably necessary and proportionate for specific investigative purposes, rather than permitting broad or open-ended categories of metadata to be prescribed.
- **Adopt a data minimization principle**, ensuring that service providers are not required to collect or retain information that they would not otherwise maintain for legitimate business purposes, unless a clear and compelling justification is established.
- **Reduce retention periods** to the shortest timeframe necessary, well-below the one-year maximum contemplated by subparagraph 5(2)(d), with differentiation based on the sensitivity and utility of the data in question.
- **Encourage targeted preservation mechanisms**, such as preservation orders, as a less intrusive alternative that allows relevant data to be secured in specific cases without requiring the ongoing bulk retention of information about the general population.

Taken together, these measures would better align the proposed framework with core principles of privacy, proportionality, and cybersecurity, while still enabling law enforcement to access the information it needs through appropriate legal channels.

4. Compensation of Core Providers

In the technical briefings regarding SAAIA, Public Safety Canada (PSC) stated that the Act was "developed with the view that the cost regime is a joint responsibility between the federal government, police agencies and ESPs."[4] PSC further stated that "[l]aw enforcement and CSIS would have to pay fees to ESPs for different types of assistance provided which would be laid out in the regulations after mandatory consultations."[5]

Notwithstanding these statements, there is nothing in Bill C-22 that addresses compensation to core providers for fulfilling the obligations imposed on them pursuant to subsection 5(2) of the SAAIA or for responding to confirmation of service demands or production orders under Part 1. Section 46 of the SAAIA provides that the GIC **may make regulations** "respecting any fees payable to electronic service providers for different types of assistance that they provide to persons exercising an authority referred to subsection 2(2)."

However, this permissive language does not establish a framework for compensating telecommunication service providers for responding to confirmation of service demands or the substantial costs associated with developing, testing, and maintaining the technologies and processes required to comply with the SAAIA. These obligations will impose significant financial and operational burdens, particularly for smaller providers, and should not be imposed on providers without a clear and enforceable compensation framework. This position has been supported by lawful enforcement agencies and has been adopted in other jurisdictions.

In a previous government consultation on lawful access, law enforcement agencies submitted that communication service providers "**should be able to recover reasonable costs incurred providing court-ordered assistance.**."[6] The Special Report on the Lawful Access to Communications by Security and Intelligence Organization also references support for this position in the context of its discussion of the Lawful Access Advisory Committee (LAAC) established by the RCMP and CSIS:

> Another key principle includes a commitment to a cost neutral and fair compensation model: ***The lawful access community acknowledges that CSPs are private or semi-private companies and deserve fair compensation for the effort required to develop, maintain, and operate capabilities that is not part of their normal business processes***.[7] [emphasis added]

These economic realities are recognized in other jurisdictions such as the UK which "recognises that telecommunications operators and postal operators incur expenses in complying with requirements in the [Investigatory Powers Act 2016], including the disclosure of communications data…, the retention of communications data… and notices

---

[4] PowerPoint presentation provided by Public Safety Canada to stakeholders, July 2025.
[5] Ibid.
[6] Summary of Submissions to the Lawful Access Consultation (2003) – Chapter 3: Comments by Law Enforcement.
[7] *Special Report on the Lawful Access to Communications by Security and Intelligence Organizations*, The National Security and Intelligence Committee of Parliamentarians, September 2025 – paragraph 118.

to maintain technical capabilities…. The Act, therefore, allows for appropriate contributions to be made to telecommunication operators and postal operators to cover these costs."[8]

The UK Notice Regime Code of Practice further states that:

> "[s]ignificant public funding is made available to telecommunications operators and postal operators to ensure that they can provide, outside of their normal business practices, an effective and efficient response to public authorities' necessary, proportionate, and lawful requirements for the disclosure and acquisition of communications data in support of their investigations and operations to protect the public and to bring to justice those who commit crime.[9]

Under the UK Notice Regime Code of Practice TSPs are eligible to receive compensation for costs incurred because of complying with requests for communications data, including costs associated with business overhead, employing staff, and updating its systems or procuring new technology.[10]

The UK Notice Regime Code of Practice also provides that TSPs are able to recover a contribution towards the costs associated with having the technical capabilities necessary to access communications, including costs to "ensure they can establish, operate and maintain effective, efficient, and secure infrastructure and processes in order to meet their obligations under a technical capability notice and the Act."[11]

As reflected in the *Special Report on the Lawful Access to Communications by Security and Intelligence Organizations* report[12] other Five Eyes countries have various models for funding the development and maintenance of intercept capability and operational fees for producing information requested or ordered to be produced.

Recommendation:

Bill C-22 should be amended to require the government to establish a clear, mandatory, and enforceable compensation framework for electronic service providers, including core provider, that reflects the statements made by Public Safety when the bill was introduced.

This framework should ensure that the substantial capital, operational, infrastructure security and compliance costs associated with developing, testing, and maintaining the technical and operational capabilities required under subsections 5(2) and 7(2) of the SAAIA (including the implementation and maintenance costs associated with mandatory metadata retention obligations, if imposed) are fully and predictably recoverable. It should also make clear that service providers are entitled to charge service fees which cover the costs of processing confirmation of service demands and production orders.

---

[8] UK Government, Notice Regime Code of Practice, June 2025, paragraph 12.1 https://www.gov.uk/government/publications/notices-regime-code-of-practice/notices-regime-code-of-practice-accessible#costs
[9] Ibid, paragraph 12.6
[10] Ibid, paragraphs 12.8-12.10
[11] Ibid., 12.19.
[12] The National Security and Intelligence Committee of Parliamentarians, September 2025, page 14 https://nsicop-cpsnr.ca/reports/rp-2025-09-15-sr/250915_NSICOP_Lawful_access_report.pdf

5. Safe harbour

Clause 11 of Part 1 of Bill C-22 replaces the existing subsection 487.0195 of the *Criminal Code*, and shields from any criminal or civil liability any person who, where not prohibited by law, voluntarily preserves data, keep an account open or active, or provide a document or information in the referenced circumstances.

However, limiting the safe harbour to **voluntary** assistance creates a significant and unnecessary gap. Most disclosures by ESPs will occur **not voluntarily**, but under compulsion of law, through a confirmation of service demand, a production order, or another form of lawful authority. In these situations, a provider has **no discretion** and failure to comply may expose the provider to criminal sanctions, contempt proceedings, or other adverse legal consequences. Yet compliance may also expose the provider to civil liability risks, including claims from affected customers, privacy complaints, or contractual disputes alleging improper disclosure of confidential information.

In the absence of an extended safe harbour, providers may be placed in an untenable position of being compelled by statute to disclose information yet potentially exposed to litigation or complaints for having done so. This risk is particularly acute because production orders may require the disclosure of sensitive personal, transactional, or subscriber information, and individuals may not appreciate that the disclosure was legally compelled. A safe harbour that protects only voluntary assistance fails to reflect the operational realities of lawful access regimes and creates uncertainty that can chill cooperation, slow compliance, or generate unnecessary legal disputes.

Extending the safe harbour to include **good-faith compliance with a confirmation of service demand or production order** is therefore essential. It ensures that providers acting under statutory compulsion are not forced to assume legal risks that Parliament did not intend them to bear. It aligns with the principle that persons who are legally required to act should not be penalized for doing what the law obliges them to do. It also promotes timely and effective cooperation with law enforcement by removing the need for providers to navigate conflicting legal exposures when responding to mandatory requests.

Recommendation:

To close this unintended gap and ensure that service providers are not exposed to legal risk for complying with statutory obligations, Bill C-22 should be amended to extend the safe harbour to include good-faith compliance with any information demand or production order. Suggested language is as follows:

(1) No person shall incur any civil or criminal liability for anything done in good faith in compliance with a confirmation of service demand or a production order under this Act.
(2) Subsection (1) applies whether the confirmation of service demand or production order is subsequently varied, revoked, or found to be invalid, provided that the person acted in good faith and in reliance on its terms at the time of compliance.

This amendment would align the protection with the operational realities of lawful access, prevent providers from facing contradictory legal obligations, and promote timely, effective

cooperation with law enforcement while safeguarding against unwarranted civil or criminal liability.

Conclusion

Bill C-22 introduces far-reaching changes that will significantly affect TSPs, operational practices, and the privacy and security expectations of Canadians. As outlined above, several provisions would be unworkable in practice, impose disproportionate and unfunded obligations on service providers, and/or create uncertainty that risks undermining both investigative effectiveness and public trust. We respectfully urge the Committee to refine these provisions to ensure that lawful-access processes remain efficient, accountable, and proportionate; that regulatory obligations are clearly defined and accompanied by essential safeguards; that providers are adequately compensated for processing confirmation of service demands and production orders and developing mandated capabilities; and that implementation timelines reflect operational realities. With these improvements, the legislation can better achieve its intended objectives.