EXPLANATION OF PROPOSED AMENDMENTS TO THE THIRD READING OF C-22

Introduction

The Canadian government clearly heard and acknowledged several concerns that were raised about Part 2 of C-22, the Lawful Access Act (LAA). Though well intended, the amendments incorporated in the third reading of the bill in the House of Commons fall short of giving Electronic Service Providers (ESPs), Canadian internet users, and governments around the world confidence that this framework offers meaningful protections and legal certainty for privacy, security, and due process. Part 2 continues to raise four primary concerns:

1. **Technical Assistance Authorities Could Still Significantly Undermine Canadians' Digital Security and Privacy:** Provisions that allow authorities to order technical assistance from electronic service providers could jeopardize the ability of service providers to offer encrypted services and guarantee the security and integrity of the hardware and software that operates their global networks. The drafters' intentions to resolve concerns related to breaking encryption are clear in the amendments reflected in the bill's third reading. Unfortunately, because of the complexities of how these technologies and leading security architectures work, and how these changes would operate in the context of the larger legal framework being established, they do not achieve their intended goal.

2. **Data Retention Obligations Treat All Canadians like Potential Criminals:** Data retention provisions still require companies to collect and retain data fields that they do not already log for business purposes. Companies should not be compelled to build new technical and collection capabilities to indiscriminately ingest and store Canadians' data solely for the purpose of assisting prospective government surveillance.

3. **Secrecy Requirements Disproportionately Gag Providers and Undermine User Trust:** Default secrecy obligations pertaining to technical assistance demands raise significant concerns around proportionality, conflicts of law, and user trust.

4. **Illegal Warrantless Searches Cannot Hide Behind the Guise of Civil Regulatory Enforcement:** Warrantless search and seizure authorities included in C-22's enforcement provisions are extraordinarily broad and lack necessary due process and oversight protections.

This paper is intended to serve as a guide to proposed changes to the amended version of C-22 Part 2. It explains what issue each change is intended to address and why they would effectively

address the most significant outstanding concerns.

Technical Assistance Authorities Could Still Significantly Undermine Canadians' Digital Security and Privacy

C-22's Technical Definitions Don't Technically Make Sense

Encryption and similar zero-knowledge security tools – many of which rely on cryptography as part of their architecture – are the strongest defenses that the Canadian government, businesses, and individuals can rely on to keep sensitive data safe from unauthorized access, use, alteration, or exfiltration. We appreciate that the amendments include a prohibition on requiring ***"decryption"*** in a technical assistance order. However, that definition and the definitions for ***"electronic protection"*** and ***"systemic vulnerability"*** still leave open the possibility that orders for technical assistance may be served on service providers that require them to break, undermine, or circumvent these protections.

Ensuring that these technologies are not vulnerable to exceptional access mandates under this law now or under the leadership of future governments requires more specificity as to the nature of the functions that are being exempted than the current definitions provide. As these definitions form the basis of the bill's most critical safeguards, the proposed changes are drafted to be technologically neutral, ensuring the definitions remain applicable as technology evolves.

Additionally, the amendments to definitions in the bill, and explanations of those proposed changes, align with guidance promulgated by globally recognized expert bodies. For example, they align with the Internet Engineering Taskforce's (IETF) detailed guidance on the definitions of "encryption" and "end-to-end encryption;" necessary features of end-to-end encrypted systems; and the role of public expectations and trust in maintaining the efficacy of encryption as a primary tool for ensuring the security, integrity, and privacy of data stored on or transmitted across digital technologies. The proposed amendments also align with the guidance of the U.S. National Institute of Standards and Technology (NIST), which runs a process for reviewing and recommending cryptographic standards that relies on public and expert consultation and an open deliberation at every stage, to ensure public confidence in the technical body's recommendations. NIST achieves long term "quality assurance" concerning its recommendations through the Crypto Publication Review Project and Board, which also relies heavily on transparency and public consultation with technical experts.

"Decryption"

The proposed amendments to the "decryption" provision in C-22's definitions section addresses the concern that the protection against compelled decryption may apply only to the cryptographic algorithm itself, and therefore may be interpreted to permit other actions that would break, undermine, or circumvent core cryptographic protections. They also clarify that the decryption protection applies to encrypted applications and devices, as well as information:

> **Decryption**
>
> **(4)** No obligations under this Act ~~are to~~ may be construed as compelling an electronic service provider to build or implement technical capabilities to decrypt

or otherwise circumvent, break or undermine cryptographic protections, or to ensure that an authorized person is able to decrypt or otherwise circumvent, break or undermine cryptographic protections, any information, application, or device that is encrypted ~~by a person to whom the electronic service provider provides services,~~ unless the encryption was provided by the electronic service provider and the provider possesses the information and technical capabilities necessary to decrypt the information.

The current definition of "decryption" appears to be drawn from a carve-out for encrypted communications in the U.S.'s Communications Assistance for Law Enforcement Act (CALEA), a 32 year old law governing obligations for technical intercept capabilities. While at first glance, adapting this definition for use in C-22 seems like a reasonable approach, in practice, it does not provide an effective protection against encryption backdoor demands.

CALEA applies only to telecommunications providers like phone companies and ISPs whereas C-22 brings a much wider range of services in scope of technical assistance obligations, including application-layer services that are exempt under CALEA. As such, the carve-out is drafted to protect subject telecommunications service providers from having to decrypt communications that were encrypted by a third party and are transiting their networks. CALEA's narrow protection was neither designed nor intended to account for the differences in how internet-based services are developed and deployed, or how data stored by or transiting those services are secured.

C-22's current "decryption" definition could be interpreted and applied in a manner that only protects against requirements to break the cryptographic algorithm; it does not necessarily account for how that algorithm is implemented by extending necessary safeguards to the larger cryptographic system. As a result, while decryption may not be mandated, demands to undertake other technical measures like client-side scanning, surreptitiously adding a third party to encrypted communications, or requiring providers to ship malware, or software or operating system updates with known vulnerabilities would still be permitted. By bypassing the cryptographic algorithm and the current definition of decryption, these tactics can open a pathway to introduce a critical vulnerability for all users without running afoul of the limitation on mandated "decryption."

"Electronic Protection"

The proposed amendments to the "electronic protection" definition address the concern that the definition as amended at third reading lacks the specificity and nuance necessary to ensure it would be interpreted in a manner that is consistent with how technologies operate. Often, electronic protections are not individual processes that operate autonomously; rather they are often the result of the interdependence and interoperation of separate tools and features that can operate on any level of the technical stack.

> ***electronic protection*** means a system, tool, or feature that performs or contributes to critical functions of the security of hardware, software, or networks. For greater clarity, this includes but is not limited to

(a) authentication processes,
(b) auditability mechanisms,
(c) encryption as applied to devices, hardware, or data in motion or at rest, and
(d) any other ~~prescribed type of data protection~~ measure that renders the service provider's access to data, devices, hardware, or networks technically infeasible. (*protection électronique*)

As with "decryption," the definition for "electronic protection" requires greater specificity in order to provide needed confidence around the bill's safeguards. These amendments reflect the technical reality that functions like authentication and encryption are not singular actions that occur in a vacuum, but are part of more complex processes and systems that can apply to different layers of the technology stack and often involve auditability as an essential component.

For example, best practices in building cryptographic systems require designs that not only use a strong cryptographic algorithm, but also include:

- Treating the server (service provider) as an adversary by:
  - Using client-centric architecture that puts application logic on the person's device;
  - Limiting data collection and storage;
  - Transmitting content and metadata on separate encrypted channels;
- Deploying robust key management systems with properties that include:
  - Decryption keys do not leave users devices;
  - Forward secrecy, where keys change after each use;
  - Key transparency and auditability with cryptographic proofs; and
  - Revocation secrecy for when a device or user is removed from access.

These processes are built to be interdependent so that if a malicious or unintended third party tries to circumvent one aspect of these protections, it can be identified and blocked.

Finally, the proposed amendments reinforce that all forms of zero-knowledge security architectures (e.g. encryption) – whether as applied to stored data or real-time communications, irrespective of the nature of the application – constitute an electronic protection. This clarification is necessary as "encryption" remains undefined in C-22, and section 47(1) authorizes the Governor in Council (GIC) to unilaterally make regulations "respecting the meaning of any term or expression for the purposes of this Act." Therefore, the proposed legislation could allow for the GIC to adopt a problematic definition of encryption, e.g., to allow for communications interception on devices before data is encrypted in transit (akin to many client side scanning proposals) or after it is decrypted on the recipient's device; or to apply only to certain types of encryption (data at rest vs. data in motion, or cryptographic algorithms).

"Systemic Vulnerability"

The definition for systemic vulnerability is generally well thought out, but requires the changes reflected in the below proposed amendments to effectively guard against a technical order that could result in security risks for all users, or otherwise introduce catastrophic or cascading risks to the digital ecosystem. The proposed changes also remove significant uncertainty introduced

by an exception that undermines the entire purpose of the definition.

> ***systemic vulnerability*** means a measure that would weaken, undermine, or circumvent ~~vulnerability in the~~ any electronic protections deployed or made available by ~~of~~ an electronic service provider to ensure the confidentiality, integrity or availability of data. This includes, but is not limited to, any requirement to implement, modify, or build a capability, or take any other action or prohibit any action that is likely to introduce a material risk that ~~secure d~~igital information, devices, or hardware 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*)

These amendments serve three primary functions. First, they incorporate concepts that are central to modern cybersecurity: protecting the confidentiality, integrity, and availability of data. Second, they ensure that a technical assistance order cannot be used to force a service provider to abandon or delay the deployment of new security features, software updates that resolve existing security risks, or deprecations of features or tools where their continued use would undermine the security of the product. Finally, and most importantly, the carve-out that was added to the definition during Third Reading of C-22 entirely undermines the purpose of defining and safeguarding against a systemic vulnerability.

If taking an action with respect to the design of a technology would introduce a risk to all users related to the confidentiality, integrity, or availability of their data, it is incoherent to then exempt that action from meeting the definition of a “systemic vulnerability” simply because that action in intended to access only a particular target’s data. The fact that there is valid legal process authorizing law enforcement bodies to search for and – if found – obtain certain data, or that it is only a particular target whose data is sought, does not change the technical reality that such an action would introduce a “systemic vulnerability.”

Therefore, while all of the proposed changes to this definition are important to ensuring that it is technically coherent and operationally reasonable, removing the carve-out at the end of the definition is of the utmost importance. Failure to remove this carve-out clause would render the “systemic vulnerability” definition as nothing more than a mirage intended to convince Canadians’ of privacy and security protections that do not exist in practice and which they cannot rely upon.

Forcing Third Party Spyware on Private Sector Systems is Dangerous and Anti-Democratic

If C-22’s definitions are effectively amended to protect Canadians’ privacy and cybersecurity, as proposed above, the primary obligation in section 5(2)(a) is appropriately robust to address law enforcement’s occasional need for assistance from providers. However, there remain significant outstanding concerns related to obligations under subparagraphs (b) and (c).

The amendments propose striking the obligations in subsections (b) and (c) which could be used to compel core providers to integrate and use government or third party spyware on their systems. This kind of requirement would severely undermine user trust and domestically and internationally chill adoption or use of Canadian products and services that could be in scope of this law.

> **Core providers — obligations**
>
> **(2)** The Governor in Council may make regulations relating to 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

The struck provision is extraordinarily overbroad and akin to an obligation one might expect from a non-democratic or otherwise oppressive government. It authorizes the requestor to commandeer private companies to act as an arm of government for criminal investigative purposes, and to dedicate resources to install, deploy, and maintain technologies the government will force them to use to surreptitiously surveil their customers or users.

Additionally, the current language does not acknowledge the technical reality of how internet based communications services and tools are built and deployed. Providers typically test and iterate extensively on changes or updates to their technologies that may have significant performance implications. This enables the provider to understand and mitigate any impacts on performance before widely deploying the technology. If an assistance demand compelled a service provider to adopt a technology developed by a third party, the third-party developers would not be able conduct that testing to ensure their technology is fit for purposes and adaptable to a particular service.
New risks could arise or existing risks could be exacerbated if third parties that develop the code/technology an in-scope provider is required to use had less robust security resources or technical expertise than the provider itself. Finally, in practice, there is also always a security risk associated with the individuals responsible for developing and deploying the technology which service providers account for in designing internal policies, auditing, and technical limits, that would not be accounted for in the context of a government issued demand for specific, prescribed technical assistance, particularly if that assistance involves the use of third party surveillance tools.

Data Retention Obligations Treat All Canadians like Potential Criminals

Data retention obligations are hugely problematic legally, technically, operationally, and economically. Meta is not subject to any such data retention obligations anywhere else in the world. This amendment strikes the data retention provisions (preferred) or - in the alternative - imposes limitations on the data that can be in-scope of such a retention requirement to ensure providers are not required to begin collecting and retaining new fields of data solely for prospective surveillance purposes.

> **Core providers — obligations**
>
> **(2)** The Governor in Council may make regulations relating to 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.~~
>
> ***The following amendment to "Restrictions" should only be incorporated if the proposal to remove data retention altogether is not adopted.***
>
> **Restrictions**
>
> **(4.1)** Paragraph (2)(d) does not authorize the making of regulations that require core providers to retain information that
>
> **(a)** would reveal
>
> **(~~a1~~)** the content — that is to say the substance, meaning or purpose — of information transmitted in the course of an electronic service;
>
> **(~~b2~~)** a person's web browsing history; or
>
> **(~~c3~~)** a person's social media or private messaging activities; or
>
> **(b)** the core provider does not already store or retain for business purposes for some duration of time.

Data retention mandates create significant legal uncertainty as data is often shared by individuals in different jurisdictions and subject to different bodies of law. As such, a provider that must navigate these differing laws may face a legal conflict whereby Canadian law obligates them to retain data, even when a foreign law that also asserts jurisdiction over that shared data requires it to be deleted. This risk is heightened by the fact that data retention obligations inherently incentivize over-retention of data contrary to privacy best practices.

Compliance with data retention obligations also introduces significant technical and operational challenges. Identifying the subject data, segregating it, and storing it for long enough to meet the retention requirement but no longer, so as to avoid conflict with data protection laws that require deletion and minimization, all require exceptionally complex technical processes that interrupt a provider's normal operations and impose significant

monetary cost. Storing and securing the data exacerbates these challenges. Additionally, these obligations may compel providers to engineer entirely new logging capabilities to retain data not previously retained for business purposes.

These challenges disproportionately burden small and medium-sized businesses. However, mandating indiscriminate metadata storage for any period of time heightens cybersecurity and privacy risks for any provider subject to the requirement, and as such for all of their users and customers as well. It also establishes a system that treats all Canadians as potential criminal suspects, where Canadians' metadata are logged and retained in bulk solely for the purpose of prospective surveillance.

While they are consistently under consideration in many jurisdictions, data retention mandates have been routinely struck down by the Court of Justice for the European Union for violating fundamental rights guarantees. Data retention mandates have also been considered and rejected by the US Congress on the basis of the same concerns raised here, and no such obligation applies to application layer services.

Rather than imposing problematic data retention obligations on core providers, Parliament should consider building out Canada's legal framework for making targeted data preservation requests to advance a criminal investigation. Most global service providers comply with preservation requests that adhere to international standards in permissive as well as compulsory contexts. Preservation frameworks provide more streamlined processes for requests than is required for data production, and they ensure that data which may later become subject to valid legal process compelling production remain available before the legal process has issued. Preservation request frameworks achieve many of the same goals as data retention mandates in a proportionate and targeted manner, and without jeopardizing the privacy or security of Canadians' data.

That said, if an amendment to altogether remove data retention from C-22 is not adopted, the below proposed amendments include a limitation in the "restrictions" section to ensure that core providers cannot be required to start storing fields or categories of data that they do not already store for some period of time for business purposes. This would at least protect providers from having to re-engineer their systems to collect and store new or additional data solely for the purpose of prospective government surveillance. The amendment to "restrictions" under subsection 4 need not be incorporated if the data retention mandate is removed.

Secrecy Requirements Disproportionately Gag Providers and Undermine User Trust

The following proposed amendments address concerns about the overbroad and unilateral authority to impose secrecy requirements on providers who are subject to technical assistance orders. The changes would implement changes to address the need for proportionality and independent oversight and approval, create narrow exceptions to avoid conflicts of law, and establish a means to challenge secrecy obligations in specific limited circumstances.

Prohibition on disclosure

14 (1) On *ex parte* application by the Minister or a person designated by the Minister, a justice of the peace may issue an order for a period not to exceed [XXX] days requiring that ~~A~~an electronic service provider and any person acting on its behalf, or as otherwise specified in subsection (4), ~~must n~~ot disclose any of the following information, except as permitted under this Act or the *Canada Evidence Act*:

(a) information contained in an order made under subsection 6(1) or 7(1);

~~**(b)** information on which the Minister relied in making the order;~~

(c) the fact that the electronic service provider is or was subject to the order;

(d) information provided in the course of representations made under section 8 or in any response given by the Minister and the fact that the Minister has invited the representations;

(e) information contained in an application referred to in subsection 6(1) or in a decision made under subsection 6(4);

(f) any prescribed information.

Conditions for making order

(2) Before making the order as described in subsection (1), a justice of the peace must be satisfied that disclosure of the information as set out in subsection (1) during the period specified in the order would pose a serious risk to:

(a) an individual's health, safety, and security;

(b) critical infrastructure; or

(c) national security; or

(d) the conduct of a criminal investigation of an offence to which the information relates.

Renewal of an order

(3) On application by the Minister or a person designated by the Minister, in writing to a justice of the peace, the justice of the peace may, from time to time, renew an order under subsection (1) for a period not exceeding the period set out in the original order, if satisfied by evidence on oath that the order continues to be required for one or more of the reasons set out in subsection (2).

Foreign subjects

(4) Where the subject of an order under subsection (1) is either a citizen of a foreign state or is established in or otherwise subject to the jurisdiction of a foreign state, the order does not prohibit or limit communications between the subject of an order, or someone acting on their behalf, and the appropriate national authorities of that foreign state. Appropriate national authorities include officials in the justice or foreign ministries, or equivalent departments or agencies, established in the foreign state, or the bodies in the national legislatures of those governments responsible for overseeing those ministries.

Challenge of Prohibition Against Disclosure

(5) An electronic service provider in receipt of an order prohibiting disclosure under this section may petition the a justice of the peace to quash or amend the order in cases where

(A) The non-disclosure obligations are

(i) over-broad; or

(ii) may impede the internal operations or delivery of goods or services of the electronic service provider;

(B) A product change required by the order is likely to or has resulted in public scrutiny or a loss of trust in the product, service, or brand; or

(C) The fact of the order has become public.

C-22 establishes broad secrecy mandates on service providers that are subject to technical assistance demands which could undermine public confidence of ESPs since users cannot be confident in the integrity and security of their products and services. It could also exacerbate conflicts of law faced by service providers that are based or operate abroad, arising from Canadian assistance obligations, by limiting their ability to consult with the government or counsel in the jurisdiction where they are headquartered.

Broad secrecy requirements may also be technically incompatible with the development, deployment, and public access to software-based technologies, and in particular, end-to-end encrypted messaging services that are based on open source protocols, such as the widely used Signal Protocol. This is for a variety of reasons, including that the complexity of building, maintaining, and providing E2EE messaging services to large populations of internet users (in some cases many billions of people) requires that large teams of engineers and technical experts be able to push software updates in real time.

In practice, it is not possible to keep a material change to source code secret from all cryptographers and other engineers on staff at an in-scope service provider. Even if it were theoretically possible, instituting that sort of technical blindness to the product would create significant risks of causing unintended harms and vulnerabilities each time an update or change is made to the software.
Moreover, independent security experts regularly decompile and reverse engineer the software and operating systems of applications and devices. This is how many leaks about new product features that are in beta testing phases occur. These same researchers would almost certainly identify the changes to the code base that are made to comply with technical assistance demands, determine the purpose or function of these changes, and publish their findings. Subject service providers would then be rendered unable to explain that the changes were required by the Canadian government, which would result in severe, global degradation of user trust.

With these considerations in mind, the proposed amendments enable secrecy obligations to operate in a proportionate way that incorporates key elements of due process, including independent oversight and the ability for a provider to challenge a secrecy obligation. The amendments propose incorporating approval and oversight of secrecy orders by a judicial or otherwise independent body. They also incorporate protections that should be adopted regardless of whether judicial review is adopted, requiring the secrecy obligations to be: ● Narrowly tailored

- Time limited
- Inapplicable when notifying the government of a provider's primary jurisdiction; and ● Subject to challenge by the provider.

Warrantless Searches Cannot Hide Behind the Guise of Civil Regulatory Enforcement

The provisions of the bill that would authorize warrantless searches and data or document seizures to confirm compliance with technical assistance orders are extremely problematic. These proposed amendments subject these search authorities to necessary judicial approval and oversight, and clarifies to whom the "duty to assist" may apply.

Authority to enter place

20 (1) A designated person is not authorized to enter a place (other than a dwelling-house) without the occupant's consent for the purpose of verifying compliance or preventing non-compliance with this Act, except under the authority of a warrant issued under subsection (2).

(2) A justice of the peace may, on *ex parte* application, issue a warrant authorizing the designated person named in it to enter a place (other than a dwelling-house) to investigate whether the owner or occupant of the location to be searched is in compliance with applicable obligations under Section 5 or orders under Section 7 only if satisfied by information established under oath that there is reasonable grounds to believe that the place contains evidence or information relevant to that investigation. ~~Subject to subsection 21(1), a designated person may, for the purpose of verifying compliance or preventing non-compliance with this Act, at any reasonable time enter any place if they have reasonable grounds to believe that anything relevant to that purpose, including any document or electronic data, is located in that place or that an activity regulated by this Act is conducted in that place.~~

Duty to assist

(6~~5~~) If a warrant is issued under subsection (2), the justice of the peace who issues the warrant may order a person to provide assistance, if the person's assistance may reasonably be considered to be required to give effect to the warrant. ~~Every owner or person in charge of a place that is entered by the designated person and every person found in the place must give all assistance that is reasonably required to enable the designated person to exercise their powers or perform their duties and functions under this section and provide the~~

~~designated person with any document or electronic data that they may reasonably require.~~

It is true that under Canadian law similar searches may be conducted in civil regulatory enforcement contexts. While these warrantless searches also raise significant concerns, they are far less problematic than the warrantless search authorities conferred on law enforcement under this bill. The contemplated warrantless searches that would be conducted under this bill relate to enforcement of criminal law and are therefore fundamentally different from civil regulatory enforcement authorities.

The underlying purpose of the technical assistance order is to facilitate evidence collection in criminal investigations. Additionally, these orders, and subsequent enforcement measures – including warrantless searches – will be served and carried out by law enforcement officers, not civil regulatory authorities. That makes the search inherently criminal in nature, but this is exacerbated by the fact that the officers carrying out the search may well do so with the express intent of also seeking out potential evidence of unrelated crimes. Moreover, violations for non-compliance with the order carry fines that can be levied on individuals or employees of targeted ESPs as high as $100,000 per day, or $500,000 per day for the ESP. Finally, other violations included in the bill are also commonly seen in criminal enforcement contexts, like “obstruction” and “false or misleading statements.”

In order to adhere to basic principles of fundamental rights and due process that govern traditional searches by law enforcement, and to prevent abuse or misuse of these authorities, any search conducted by law enforcement must be pursuant to an order that is approved and overseen by an independent judicial authority, and substantiated based on a reasonable evidentiary threshold. Ideally, the order would also include:

- Clear limitations as to place, time, and manner of the search;
- Procedures to protect privacy of persons unrelated to the purpose of the search; and
- Protections against commandeering the assistance of persons who are merely in or near the search premises.

The above amendments to these search authorities are necessary to protect both Canadian employees and Canadian data.