July 14, 2026

# Decrypting Bill C-22, Part I: Why Canada Needs a Lawful Access Regime

**By:** Alexandra Lyn, Joel Reardon, and Michael Nesbitt

**Legislation Commented On:** Bill C-22, *An Act respecting lawful access* (1st Sess, 45th Parl, 2026)

Bill C-22, *An Act respecting lawful access* (1st Sess, 45th Parl, 2026) is the federal government's long-overdue and contentious attempt to address the intractable issue of lawful access. C-22 has cleared the House and is awaiting Senate study beginning on September 21, 2026, having been fast-tracked through third reading despite ongoing privacy, encryption, and overbreadth objections. The Bill has two parts. Part 1, *Timely Access to Data and Information*, governs law enforcement access to personal information held by communication service providers (think Bell, Rogers, Telus) and other tech companies and services like Signal, Gmail, and WhatsApp, by amending the *Criminal Code* and several related statutes. Part 2 enacts the *Supporting Authorized Access to Information Act* (*SAAIA*), which establishes a framework that requires electronic service providers to facilitate lawful access requests under the *Criminal Code* or the *CSIS Act*. Framed by the government as a response to criminal activity increasingly enabled by the digital environment, the Bill expands the state's powers of search and seizure by conscripting private providers into its investigative apparatus — for example by requiring them, among other things, to retain user metadata that may not otherwise be preserved, and to develop technical capabilities that would otherwise not exist, so that law enforcement can access the data these providers hold. These expanded powers lie in tension with civil liberties and the privacy interests Canadians hold in their digital lives, interests protected by section 8 of the *Charter*. Bill C-22 asks Canadians to decide a question that has become increasingly pressing in a digital world: in the pursuit of public safety, how much of our privacy are we prepared to relinquish, to whom, and at what cost?

What follows is the first in a series of four blog posts. Our aim in this series is to give readers without a background (or at least without a significant background) in constitutional law or computer science the tools to evaluate whether C-22 strikes the appropriate balance. To do so, we seek to explain what the Bill actually does, where the Bill's critics have hit the mark, where the Bill goes right and wrong, and how some of the discussion and analysis to date has, perhaps, misunderstood the technology at play. To that end, this series of posts offer what the polarized debate over C-22 has sometimes lacked: a guide that explores the merits of both the public safety case and privacy objections, and translates them for non-legal and non-technical readers who want to understand the Bill rather than simply pick a side.

Lawful access refers to the legal powers of law enforcement to conduct searches and seizures of private spaces and information for investigatory purposes. In the digital sphere, we think of

lawful access in terms of law enforcement's and national security agencies' ability to intercept communications (for example to acquire Internet Protocol (IP) addresses) and obtain other information (like the subscriber data associated with those IP addresses). A well-designed lawful access framework supports public safety by enabling police and intelligence agencies to gather evidence and investigate serious offences.

And, Canada has a need for an updated, reinvigorated, and well-designed lawful access regime. While Canada does currently have lawful access tools scattered across the *Criminal Code*, RSC 1985, c C-46 (*Criminal Code*), the *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 (*CSIS Act*), the common law, and elsewhere, the regime is scattershot, and it has not kept pace with the speed at which technology continues to develop. There has not been meaningful reform of the lawful access regime, such as it is, in nearly two decades. Furthermore, as a signatory to the Council of Europe's *Convention on Cybercrime* (the *Budapest Convention*) and the Council of Europe's *Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence* (the *Second Protocol*), Canada has committed to modernizing its lawful access framework(s) to bring itself into compliance with its international obligations. This is particularly important given the reality that digital crimes are not constrained to territorial borders, thus necessitating international cooperation to detect, investigate, and prosecute these crimes.

As the only country among the Five Eyes, G7, and European Union without a framework imposing technical obligations on electronic service providers, Canada has also fallen behind its closest allies (Public Safety Canada, "Lawful Access"). Law enforcement agencies and organizations representing their workers, including the Canadian Association of Chiefs of Police, the National Police Federation, and the Canadian Security Intelligence Service, have welcomed the Bill as necessary reform. They argue that C-22 will provide law enforcement with the necessary tools to investigate and collect evidence in a growing number of digitally enabled crimes including fraud, child pornography, and terrorism offences (Canadian Association of Chiefs of Police, News Release, "NPF, CPA and CACP call for passage of Bill C-22 to provide necessary lawful access in Canada" (3 June 2026); Marie Woolf, "Transnational investigations are being hindered by Canada's lack of lawful access powers, CSIS says") These arguments are not without force. But as we explain in this blog post and three forthcoming and related posts, the government's case tends to overstate and oversimplify the lawful access powers of our allies while downplaying the far-reaching and significant privacy implications currently embedded in C-22.

Indeed, in contrast to the government position that C-22 is a necessary and proportionate update to Canada's lawful access framework, some industry professionals, academics, and even politicians, have decried some of the Bill's lawful access provisions as untenable violations of Canadians' right to privacy. Some have gone so far as to call the bill, "…a dire threat to human rights in Canada" (Centre for Free Expression et al, "The Fed's 'Lawful Access' Bill C-22 is an Unprecedented Assault on Canadians' Privacy Rights and Must Be Withdrawn – Letter to the Prime Minister"). Significantly, several major technology companies, among them Signal, DuckDuckGo, and Apple, have warned that they may need to withdraw from the Canadian market if the Bill passes in its current form (Steven Chase, "Signal Warns It Would Pull Out of

Canada if Made to Comply With Lawful Access Bill", Marie Woolf, "Search Engine DuckDuckGo Would Withdraw VPN from Canada If Lawful-Access Bill Passes").

In the end, we argue that the government's description of C-22 as a straightforward and proportionate public safety measure deserves skepticism, but so too does any reflexive counter-narrative that treats any expansion of state investigative capacity as inherently illegitimate. C-22's flaws (and there are many) make it easy to write off as a nefarious attempt to erect a surveillance state cloaked in the language of public safety. Such a position is oversimplified and omits the very real challenges associated with modern police work and public safety challenges in an increasingly digitalized world.

Across the series, we argue that Canada urgently needs the lawful access regime that C-22 promises; we also argue that C-22, as drafted, should not be the Bill that delivers it. We begin in this first post by laying the foundation for our argument, specifically, by acknowledging that law enforcement has pressing investigative needs in a digital world – needs that must be balanced with Canadians' constitutionally guaranteed privacy rights under section 8 of the *Charter*. We also introduce what will become a recurring theme in this series: C-22 does not strike that balance so much as defer it, asking Canadians to trust in executive restraint where the statute itself should impose limits. The remainder of the posts in this series will take up the three criticisms that have dominated the C-22 debate, and continue to persist notwithstanding the minor amendments approved by the Standing Committee on Public Safety and National Security in June 2026 (House of Commons, Standing Committee on Public Safety and National Security, Bill C-22, An Act respecting lawful access: Fifth Report, 45-1 (18 June 2026) (Chair: Hon Jean-Yves Duclos)). These criticisms have thus far been ably catalogued by commentators such as Professors Michael Geist and Robert Diab (referenced below), a dialogue we wish to extend in this series. Blog Post 2 will focus on C-22's mandatory metadata retention requirements. Blog Post 3 will cover the Bill's inadequate systemic vulnerability safeguards, including why guarantees against decryption do not go far enough. Blog Post 4 takes up the problematic lowered threshold for obtaining subscriber information. Punctuating our analysis in each of the posts in this series is an important premise: lawful access is a legitimate investigative function, one that, when done responsibly, is consistent with the *Charter*, and acknowledges that there is a real and pressing case for a modernized framework. With that said, Bill C-22, as currently written, is not the answer to that need. We emphasize that any law that depends on the state's self-discipline rather than statutory and principled limits is a poorly designed and dangerous law.

This post proceeds in three parts. In Part 1 we begin with a primer of two foundational concepts: lawful access and the right to privacy guaranteed by section 8 of the *Charter*. This section lays the groundwork for the analysis that follows in this and later posts. It provides an overview of how section 8 of the *Charter* constrains the state's powers of search and seizure in the digital context and lies in tension with the state's legitimate interest in modernizing its lawful access powers. In Part 2, we canvass C-22's origins in the failed lawful access provisions of Bill C-2, *An Act respecting certain measures relating to the security of the border between Canada and the United States and respecting other related security measures*, 1st Sess, 45th Parl, 2025 (C-2). We then move to Bill C-22's definitional architecture. Specifically, we examine the Bill's definitions of "electronic service provider" and "electronic service" – definitions that are so sweeping and overbroad that they capture nearly every business operating in Canada and are

paired with a discretionary designation framework that leaves the executive to decide who must comply. From there, we consider the two principal justifications the government has offered for the Bill: technological modernization and alignment with Canada's international allies and obligations. We end this part with an overview of the dominant criticisms of C-22, which will be taken up in more detail in our later posts in this series. We conclude this post in Part 3 with a note on the broader costs of enacting constitutionally vulnerable legislation, and why Parliament should not act rashly when passing laws that raise serious and foreseeable *Charter* concerns – particularly when the cost of that rashness is borne not by Parliament, but by the accused, victims, the Canadian taxpayer, and the administration of justice.

**Part 1 - Foundational Concepts: Lawful Access and Section 8 of the *Charter***

***What Is Lawful Access, and Why Does Canada Need It?***

Lawful access is the ability of law enforcement and national security agencies to "legally obtain certain information or intercept communications" (Public Safety Canada, "Lawful Access"). Put simply, lawful access is about the state's powers of search and seizure. It sets the rules for what investigators may and may not collect, and how, including when a warrant is required before a search. In the telecommunications context, it covers the interception of communications and access to information such as an IP address or subscriber information, as authorized by statutes like the *Criminal Code* and the *CSIS Act* (Department of Justice Canada, *Lawful Access – Consultation Document*). A clear, robust lawful access framework gives police and intelligence agencies the legal footing that they need to gather admissible evidence and to prevent, investigate, and prosecute serious offences and threats to national security, while also respecting the constitutional and privacy rights of Canadians in a balanced, proportionate fashion. In that sense, sound lawful access is a genuine component of public safety in a democracy, rather than a threat.

***Section 8 of the Charter and the Right to Privacy***

Lawful access sits in constant tension with the right to privacy guaranteed by section 8 of the Canadian Charter of Rights and Freedoms, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11, which provides that everyone has the right to be secure against unreasonable search and seizure. Because C-22 expands the state's search powers, it must conform to section 8 or risk being struck down. The Canadian government has tended to chronically understate the effect C-22 will have on Canadians' *Charter* protected rights. We lay the foundation for this overarching theme now by undertaking an overview of how section 8 of the *Charter* constrains the state's ability to access private information, even when such access is purported to be authorized by law. Later posts will then explain where Bill C-22 misses the mark in relation to the dominant criticisms of the Bill.

Section 8 applies to state conduct. If the search and/or seizure is not conducted by a state actor or their agent, then it does not amount to a search and/or seizure engaged by section 8 of the *Charter*. Even where the state conducts the search, section 8 only protects against *unreasonable* searches and seizures. So, to conduct a section 8 analysis we must:

1. Ensure that the search is conducted by the state or a state agent;
2. Identify a subject / privacy interest of the purported search by the state or state agent;
3. See if there is a reasonable expectation of privacy (REP) in relation to that subject matter (*R v Evans*, 1996 CanLII 248 (SCC) at para 11); and
4. Assess the reasonableness of the state's action vis-a-vis that individual, the subject matter, and the manner in which the search and seizure is carried out by the state.

In order to determine the reasonableness of state's actions in the search, Canadian courts look to:

i. Whether the search is authorized by law (a common law right to search incidental to arrest for example, or a statutory right to search a house with prior judicial authorization);
ii. Whether the law itself is reasonable; and
iii. Whether the search is carried out in a reasonable manner (*R v Collins*, 1987 CanLII 84 (SCC) at para 23).

Identifying the subject matter of a search is becoming increasingly complex in Canadian law. The Supreme Court has identified various "categories" of subject matter / privacy interests that are protected under section 8: personal privacy, territorial privacy, and informational privacy interests (*R v Tessling*, 2004 SCC 67 at para 20).

Questions relating to digital privacy can engage more than one of these interests – and is a hot button topic for current litigation in this area – but frequently it is dealt with by the courts as informational privacy. As the Supreme Court of Canada stated in *R v Dyment*, 1988 CanLII 10 (SCC), [1988] 2 SCR 417, informational privacy rests on the idea that, "information about a person is in a fundamental way [the person's] own, for [that person] to communicate or retain for [themselves] as [they see] fit" (at para 22). Significantly, this framing vests a degree of ownership and control by the data subject, who governs disclosure, audience, and use according to their own preferences. As society has digitized, the volume and sensitivity of the information we generate has grown, and the courts have had to decide which kinds of data attract a reasonable expectation of privacy, particularly as the concept of data ownership and control has become increasingly hard to reconcile with the realities of modern data flows. The result is a patchwork of cases that tend to answer specific questions of informational privacy, in specific contexts, as opposed to a comprehensive framework for lawful access.

The scope of informational privacy protections under section 8 has evolved through a line of modern section 8 cases where the Supreme Court has confirmed that Canadians can reasonably expect privacy in, among other things*:* the personal information on a work laptop (*R v Cole*, 2012 SCC 53 at para 8); their subscriber information (*R v Spencer*, 2014 SCC 43 at para 51); text messages stored on a recipient's device (*R v Marakah*, 2017 SCC 59 at para 4); and their IP address (*R v Bykovets*, 2024 SCC 6 at para 3). Importantly, the underlying context of each of these cases were applications by an accused to exclude evidence that they argued was obtained unlawfully (in violation of their section 8 rights) by law enforcement. In each case, the Supreme Court considered, for the first time, the particular type of information at issue, finding a reasonable expectation of privacy in each that had not been previously recognized by the court. The section 8 breach was then identified by the courts retrospectively, meaning the police could not have known in advance that the search would be found unconstitutional. The consequence is

that officers have been left to operate without clear *ex ante* guidance, such that that the privacy interest, and the corresponding limit on police power, becomes apparent only once the court rules after the fact.

In the result, these cases raise an important question: does Canada's existing lawful access patchwork give citizens and the state enough clarity and certainty? Canadians want meaningful protection for their informational privacy; law enforcement needs clear statutory authority to obtain digital evidence lawfully. C-22 is, in many respects, an attempt to strike that balance where the courts have not. As the rest of this series argues, C-22 does not succeed, but the balance it is reaching for is an important one.

**Part 2 - An Overview of Bill C-22, Its Origins, Justifications and Discontents**

***Bill C-22's Predecessor: The Lawful Access Provisions of Bill C-2 (2025)***

Bill C-22 is a follow-up attempt to the lawful access regime proposed in Bill C-2, which was first tabled in the spring of 2025. C-2 was targeted (and marketed) as an improvement to Canada's border security, particularly in response to stated concerns from the United States about Canada's border controls and enforcement. As one component of the broader Bill, C-2 contained lawful access provisions, which were poorly constructed and, as a result, faced significant backlash. These provisions were the subject of a previous ABLawg post by University of Calgary students Dav More and Tulika Bali and can be read here.

One of the most controversial elements of C-2 was the inclusion of "Information Demands", which gave law enforcement sweeping warrantless access to a wide range of personal subscriber information on a diminished evidentiary standard – reasonable grounds to suspect instead of reasonable grounds to believe (C-2, Part 14 s 158). This provision applied to all offences and had the potential to apply extra-territorially (Michael Geist, "Privacy At Risk: Government Buries Lawful Access Provisions in New Border Bill").

Bill C-2 also required designated electronic service providers to cooperate in developing and implementing the state's lawful access capabilities (C-2, Part 15 ss 5, 7). This, coupled with the failure of the government to include adequate safeguards against the creation and exploitation of systemic vulnerabilities, including failing to define "systemic vulnerability" and "encryption" at all, gave rise to concerns that the state could require companies to weaken encryption or install backdoors, in large part, because C-2 did not explicitly prohibit these actions (Robert Diab, "Canada's Lawful Access Bill: Heavy on Secrecy, Light on Accountability"; Robert Diab, "Bill C-2 Backgrounder: New Search Powers in the Strong Borders Act and Their Charter Compliance" (2025) 73:3 Crim LQ 257).

Following public outcry, the lawful access provisions were ultimately removed, and C-2 was passed without these provisions (Michael Geist, "Government Reverses on Bill C-2: Removes Lawful Access Warrantless Demand Powers in New Border Bill"). Bill C-22 is the government's revised attempt at modernizing Canada's lawful access framework.

***Bill C-22: its Definitional Framework, Justifications, and Discontents***

As stated above, Bill C-22 is the government's follow up to Bill C-2 – a second attempt to amend the lawful access regime – and this time the Bill focuses solely on lawful access. We turn now to Part 2 of Bill C-22, namely the foundational definitions, which determine the reach of the *SAAIA*.

*Clarifying the Framework and Definitional Structure of C-22*

Bill C-22 is built on a set of interlocking definitions, and the Bill is hard to assess without first understanding certain foundational definitions that define the scope of C-22: "Electronic Service Providers" and "Electronic Service".

*Electronic Service Providers*

The *SAAIA* defines an electronic service provider as a person that, alone or as part of a group, provides an electronic service (including to enable communications) and either provides the service to persons in Canada or carries on all or part of its business in Canada (*SAAIA*, s 2(1)).

This is an extraordinarily broad definition. Any business, individual, or group providing an electronic service to people in Canada, or carrying on business here, is caught by the definition. The territorial reach extends beyond Canadian-incorporated companies to foreign firms operating digitally in Canada, to ensure that major global technology companies fall within the regime as long as they serve Canadian users. How wide the net stretches, though, turns on what counts as an "electronic service."

*Electronic Service*

The *SAAIA* defines an electronic service as "a service, or a feature of a service, involving the creation, recording, storage, processing, transmission, reception, emission, or making available of information in electronic, digital, or any other intangible form, by electronic, digital, magnetic, optical, biometric, acoustic, or other technological means, or any combination of them" (*SAAIA*, s 2(1)).

Read literally, this definition is an inventory of the digital world, and then some. A calculator processes digital information. An FM radio processes electrical signals. A sundial keeps time by optical means; a compass gives direction by magnetic means. A magic 8-ball furnishes information in intangible form and a Ouija board purports to do the same. The drafters presumably would not pursue children running a tin-can telephone, but the point stands: the everyday devices comfortably within scope include every mobile phone, every router and switch forming the backbone of the internet, smart-home devices such as always-on video doorbells and voice assistants, and the open-source software (Linux among it) running on all of them. Any website with a password login provides an electronic service.

*From Sweeping Definitions to Executive Discretion*

Faced with this breadth, the government insists it is taking a "more targeted approach" to the technical capability requirements and does not intend to capture whole sectors or small enterprises. Only providers designated as core providers under section 5(2), or named through ministerial order under section 7(1), will have to build and maintain lawful access capabilities (Public Safety Canada, "Backgrounder – Securing Access to Information in Bill C-22").

That reassurance is weaker than it sounds. Core providers are not listed in the statute; they are to be designated by regulation. The *SAAIA* sets out factors to consider in identifying a core provider but requires only that those factors be taken into account, a light constraint on the designation of cabinet power. The section 7(1) ministerial order power extends the regime further, letting the Minister impose capability obligations on essentially any person or entity, core provider or not, for up to two years.

This is a regime whose definitions reach nearly every business operating in Canada, paired with sweeping executive discretion to decide who must actually comply. In practical terms, Parliament has delegated the job of defining the scope of the lawful access framework to the executive, through regulation and ministerial order, rather than fixing clear limits in the statute itself. Governmental assurances that capability requirements will not fall on entire sectors or smaller firms therefore deserve skepticism, not because officials will necessarily act in bad faith, but because the legislation expressly confers the authority to do exactly what they promise to avoid. The framework leans on public trust in executive restraint rather than on clear statutory constraint. As we will see throughout this series, this is a recurring theme in C-22, and a dangerous one at that; the Bill asks Canadians to trust the discretion of the state rather than to rely on a narrowly tailored, fit-for-purpose law. So, why enact C-22 at all? The government offers two principal justifications, which we explore below.

*Government's Rationale for C-22*

The Canadian government has provided several (albeit overlapping) justifications for Bill C-22 across several documents. For simplicity and by way of introduction we have grouped these justifications into two broad themes:

1. The current lawful access frameworks are not adequate in a rapidly evolving technological environment. The government wishes to maintain lawful access capabilities in the face of new technologies (Department of Justice Canada, "Introduction" in Lawful Access – Consultation Document) (DOJ Consultation Document).

2. The government wishes to align Canada's lawful access capabilities with like-minded partners and implement the Council of Europe's *Convention on Cybercrime* (the *Budapest Convention*) (see also DOJ Consultation Document).

As we will discuss below, the factual underpinnings of both of these rationales for updates *of some kind* are substantially correct. That is to say, broadly speaking the government has correctly identified a problem and has compelling reasons to address it. However, that is not to say that C-22 has properly identified the solutions or appropriate response. One may accept that Canada's lawful access framework has genuine gaps and that alignment with international partners is

needed while still concluding that the particular mechanisms C-22 adopts to achieve those goals are insufficiently safeguarded, or constitutionally vulnerable. Accordingly, we undertake an evaluation of the government's purported ends below, to ascertain whether a factual basis exists for the state's justification of C-22.

*Current Lawful Access Frameworks Require Modernization for Digital Evidence*

The ubiquity of digital technology means that all people in Canada are "digital by default" (Council of Canadian Academies, *Vulnerable Connections Expert Panel on Public Safety in the Digital Age* at xvi). Widespread adoption of information and communication technologies has created new opportunities and methods for individuals to engage in both pro-social and truly harmful (and criminal) behaviour. These often-significant digital harms (think online fraud or child exploitation) pose unique challenges for prevention, containment and investigation efforts (Council of Canadian Academies at 36).

Reported cybercrime incidents rose 22.4% annually between 2014 and 2017 (Canada, Department of Justice, *Evaluation of the Investigative Powers for the 21st Century Initiative* at s 4). The increase was broken down as follows:

| **% of Increase attributable to specific criminal activity** | **Criminal Activity** |
|---|---|
| 47-48% | Cyber aided fraud |
| 13-17% | Possession and distribution of child pornography |
| 5-10% | Indecent or harassing communications |

(Source: Department of Justice, s 4)

Encryption technologies have seriously affected law enforcement's capacity to collect digital evidence, and the issue of encryption has, understandably, factored heavily into the C-22 dialogue. In short, encryption is a dual-use technology in that it serves both protective and obstructive functions in the context of public safety, national security, and law enforcement. As criminal actors employ increasingly sophisticated encryption methods, law enforcement agencies have been forced to engage increasingly sophisticated investigative tools and methodologies. Indeed, law enforcement agencies, together with security and intelligence organizations, contend that "encryption and the increasing volume, variety, and velocity of digitally generated data makes it difficult and sometimes impossible to gather the information needed to carry out effective investigations" (National Security and Intelligence Committee of Parliamentarians, *Special Report on the Lawful Access to Communications by Security and Intelligence Organizations* at 1).

The common law cannot close this gap on its own, and definitely not in a timely and efficient manner. Courts have been increasingly asked to consider what a reasonable expectation of privacy means in the digital age; courts, however, can only answer the questions put before them, so the resulting jurisprudence often covers discrete problems rather than the full landscape of digital information – and often, with the pace of justice in Canada, courts do so only years after the question arises. As a result, the judicial reasoning tends to be narrowly tailored to the facts before the judge in the case at hand, which makes it hard to generalize or to use as guidance for police (see Simon Stern, "Textual Privacy and Mobile Information" (2018) 55:2 Osgoode Hall LJ 398 at 402, 405). Furthermore, waiting for the common law to assemble a comprehensive framework is slow, costly, and risks jeopardizing ongoing prosecutions in the meantime, leaving investigators (and then prosecutors, defence lawyers, and trial judges) to operate amid legal uncertainty and technological complexity. Significantly, it can also depend on individuals charged with crimes, but not found guilty, to essentially fund the constitutional debate around lawful access (through legal fees).

C-22 therefore reflects a real operational need in law enforcement and Canadian justice more broadly. The growing inability of Canadian security and law enforcement agencies to intercept, access, and act on digital communications in a landscape that has outpaced the legal tools available to them is a legitimate public safety concern that must be addressed. Importantly, this landscape is not limited to Canadian territorial borders, and amendments are required for Canada to keep pace with its international obligations and allies.

*Modernization of Canada's Lawful Access Frameworks Necessary to Meet International Obligations*

Canada remains an outlier among its allies, lacking the kind of lawful access framework that many comparable countries already have in place. C-22 has thus been pitched by the government as bringing Canada into line with its partners and toward compliance with the *Budapest Convention* and the *Second Protocol* on cross-border access to electronic evidence. The *Budapest Convention* established a common framework for harmonizing domestic cybercrime laws and enabling cross-border investigative cooperation. The *Second Protocol* modernized that framework by providing expedited tools for accessing electronic evidence stored across jurisdictions, including through direct cooperation with service providers (Gemma Davies & DeBrae Kennedy-Mayo, "The Promise and Pitfalls of the Second Protocol to the Budapest Convention: Assessing its Impact on EU and UK Cross-Border Criminal Investigations" (2026) 17:1 New J Eur Crim L 101). Canada ratified the *Budapest Convention* in 2015 but has not yet ratified the *Second Protocol*.

Unfortunately, the government has framed Bill C-22 as merely bringing Canada "up to the basement" of its allies (Catharine Tunney, "Federal officials on the defensive as momentum grows against lawful access bill"). As we will discuss in our forthcoming blog posts, with the possible exception of Australia's lawful access regime, this is inaccurate. The government's statements tend to overstate the maturity and reach of allied regimes. In fact, in some cases C-22 confers upon the Canadian government powers that far exceed those of its allies, and in some cases have actually been struck down by our allies as violating their own fundamental norms.

The need for reform is genuine; the suggestion that C-22 is merely a modest exercise of catch-up with our allies is not. It is precisely this distance between the government's framing and the Bill's substance that has drawn sustained criticism.

*Dominant Criticisms of C-22*

Like its predecessor C-2, Bill C-22 has faced intense criticism. Most of this criticism centers around three main issues. We will explore each of these criticisms in detail in the three subsequent blog posts in this series; we introduce them here to illustrate that Bill C-22 hardly represents a meaningful departure from the troubling path charted by C-2, and in some cases even represents a deeper intrusion into the privacy of Canadians.

First, Bill C-22 largely maintained Bill C-2's provisions compelling electronic service providers to cooperate in, facilitate, and in some cases augment the state's lawful access capabilities. It also added dangerous new provisions requiring mandatory metadata retention by electronic service providers like Telus, Rogers, Bell, Signal, Apple, and others (C-22, Part 2 ss 5(2)(a)-(b),(d) 7(1), 12, 13, and 14).

Second, although the government responded to criticisms of Bill C-2 by defining "systemic vulnerability" in C-22 (Part 2, s 2(1)) and later adding a provision confirming that electronic service providers cannot be compelled to decrypt data they lack the technical ability to decrypt (Part 2, s 2(4)), these safeguards remain insufficient to guarantee that privacy-enhancing technologies will not be intentionally weakened by other means. The focus on encryption is far too narrow, and the revised safeguards are still insufficient to ensure Canadians' data security is not compromised in favour of enhanced lawful access powers.

Finally, C-22 lowers the production order threshold for subscriber information from reasonable grounds to *believe* to reasonable grounds to *suspect* (C-22, Part 1 s 6). On a positive note, the "Information Demands" in C-2 were replaced with a narrower "Confirmation of Service Demand", which requires telecommunication service providers to confirm "whether or not they provide or have provided telecommunication services to any subscriber or client, or to any account or identifier, specified in the demand" (C-22, Part 1 s 5). The balance of the subscriber information originally accessible under C-2 without a warrant must now be the subject of a production order, although the government maintained the lower evidentiary threshold: reasonable grounds to suspect (see e.g. Michael Geist, "A Tale of Two Bills: Lawful Access Returns With Changes to Warrantless Access But Dangerous Backdoor Surveillance Risks Remain"). By reducing the evidentiary standard required to obtain a production order, the government is making it easier for law enforcement to obtain Canadians' private data, notwithstanding the Supreme Court's ruling that Canadians have a reasonable expectation of privacy in their internet subscriber information (*R v Spencer)* and their IP address (*R v Bykovets)*. The foregoing criticisms are not merely academic. The uncertainty they describe has concrete consequences for ordinary Canadians and will surely result in long and expensive litigation.

**Part 3 - A Note on *Charter* Scrutiny and the Harms of Shaky Legislation**

In the posts that follow, and with particular reference to the metadata retention requirements and the reduced evidentiary threshold for production orders targeting subscriber information (discussed in our second forthcoming post), we argue that significant portions of Bill C-22 may fail to withstand *Charter* scrutiny. At the outset, we want to make explicit the concerns that such a conclusion raises. The issue is not simply whether the legislation will ultimately survive a *Charter* challenge. It is whether Parliament should rush to enact legislation that raises such obvious constitutional concerns in the first place and will burden the courts with their inevitable resolution.

Relying on the judicial process to determine the constitutional validity of legislation is an inefficient and costly means of legislative refinement. Constitutional challenges can result in years of uncertain litigation, substantial public resources, and often conflicting judicial decisions before legal certainty is achieved. In the interim, the legislation remains operative, shaping the conduct of law enforcement, service providers, and ordinary Canadians.
More fundamentally, the costs of constitutional uncertainty are borne by real people. A challenge to Bill C-22 is unlikely to arise in the abstract; it will almost certainly emerge in the context of a criminal investigation or prosecution. As a result, constitutional deficiencies in the legislation may have profound consequences not only for accused persons whose privacy rights are at stake, but also for victims, witnesses, and the broader administration of justice. If key provisions are ultimately found unconstitutional, years of investigative effort, prosecutions, and judicial proceedings may be called into question. Such outcomes do little to promote public confidence in either the criminal justice system or the legislative process.

In the next post, we turn to the first and most far-reaching of our three central criticisms: the Bill's mandatory metadata retention provisions, what metadata is, why its retention matters, and why section 5(2)(d) of the *SAAIA* raises serious section 8 concerns.

---

This post may be cited as: Alexandra Lyn, Joel Reardon & Michael Nesbitt "Decrypting Bill C-22, Part I: Why Canada Needs a Lawful Access Regime" (14 July 2026), online: ABlawg, http://ablawg.ca/wp-content/uploads/2026/07/Blog_AL_BillC-22.pdf