

October 19, 2026

Decrypting Bill C-22, Part 2: Keeping Tabs: C-22 and the Year (Now Half-Year) of Metadata Retention

By: Alexandra Lyn, Joel Reardon, and Michael Nesbitt

Legislation Commented On: [Bill C-22, *An Act respecting lawful access*, 1st Sess, 45th Parl, 2026 \(as passed by the House of Commons 18 June 2026\)](#)

This is the second post in our four-part series that translates the ongoing debate over Bill C-22 for non-technical and non-legal readers. The first post introduced Bill C-22 and provided background information to help understand the justifications and criticisms of the Bill, including a brief primer on the legal concept of “lawful access” and search and seizure law under section 8 of the *Charter*, which readers may wish to review as it forms a backdrop to this blog post. Part I can be found [here](#). In that post, we promised three subsequent blog posts on three core criticisms of Bill C-22. This installment tackles one of the most far-reaching of those three core criticisms of Bill C-22: the Bill's mandatory metadata retention provisions.

In pursuit of modernizing its lawful access powers, C-22 introduces a novel metadata retention regime found in section 5(2) of Part 2 of the Bill (the *Supporting Authorized Access to Information Act*, s 5, being Part 2 of Bill C-22, [An Act respecting lawful access](#), 1st Sess, 45th Parl, 2026 (as passed by the House of Commons 18 June 2026) (*SAAIA*). The regime requires certain electronic service providers (ESPs), for example Telus or Rogers but also Signal or Whatsapp, to retain some categories of metadata—essentially, data about data—for up to six months (*SAAIA*, s 5(2)). The regime does not require individualized suspicion of wrongdoing and dispenses with judicial pre-authorization for the major telecommunications and internet providers it principally targets. It excludes only three ambiguous categories from retention: content, web-browsing history, and social-media activity (*SAAIA*, s 5(4)). Despite sustained criticism, the government did not further define the categories of metadata to be retained, adding instead a vague requirement that the metadata be “essential” (*SAAIA*, s 5(4.1)), without further information as to what constitutes “essential” metadata.

The result, as this post argues, is legislation that not only conscripts ESPs into being quasi-agents of the state, compelled to seize and store their users' data, but may also force privacy-preserving services like Signal out of the Canadian market. Far from delivering the “public safety” it promises, C-22 may leave Canadians less secure—not only from their own government, but from the malicious actors inevitably drawn to the troves of data collected under its mandate. Indeed, in the case of the Bill's metadata retention regime, it may create more safety concerns than it solves.

This post proceeds in four parts. Part 1 sets out the metadata retention regime in section 5(2)(d) of the *SAIA* and canvasses the range of entities it may capture, from telecommunications carriers to cloud computing, social media, and online game providers. Part 2 delineates what metadata is and why its power lies in the aggregation of such data. It then examines the three exclusions in section 5(4) and the "essential" criterion in section 5(4.1) and assesses the justifications that government officials and police have offered for the regime. Part 3 assesses the regime against section 8 of the *Charter*. We contend that C-22 transforms ESPs into quasi agents of the state, that Canadians hold a reasonable expectation of privacy in the metadata it retains, that retention amounts to a warrantless seizure, and that section 1 of the *Charter* is unlikely to save the regime as currently constructed. Part 4 concludes with our recommended amendments to Bill C-22's metadata regime.

1. Reviewing Bill C-22's Metadata Provisions

Part 2 of Bill C-22, the *SAIA*, contains the Bill's metadata regime (*SAIA*, s 5). Unlike other aspects of the Bill, the metadata retention powers are a novel addition to Canada's latest attempt to modernize its lawful access powers, not simply a remnant from the Bill's ill-fated predecessor, Bill C-2 (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 (first reading 3 June 2025)). C-22's metadata retention regime is set out in section 5(2)(d) of the *SAIA*. It reads as follows:

5(2) The Governor in Council may make regulations respecting the obligations of core providers, including regulations 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.

Section 5(2)(d) empowers the Governor in Council to require "core providers" to retain categories of metadata—including "transmission data" as defined in section 487.011 of the *Criminal Code*—for up to six months. Transmission data is defined as data that:

(a) relates to the telecommunication functions of dialling, routing, addressing or signalling;

(b) is transmitted to identify, activate or configure a device, including a computer program as defined in subsection 342.1(2), in order to establish or maintain access to a telecommunication service for the purpose of enabling a communication, or is generated during the creation, transmission or reception of a communication and identifies or purports to identify the type, direction, date, time, duration, size, origin, destination or termination of the communication; and

(c) does not reveal the substance, meaning or purpose of the communication (*Criminal Code*, s 487.011).

Bill C-22 attaches its metadata retention obligation to "core providers", which it defines as ESPs belonging to a class set out in the schedule to the *SAIA* (s 2(1)). The government will eventually designate which entities are "core providers" by regulation (*SAIA*, s 5(1)); that is, the government has given itself authority to list at a later date those whom it deems to be a core provider and who will thus be covered by the regime. Section 7(1) then allows the Minister, by order, to impose the same obligations on any electronic service provider, whether or not it is a core provider. Each order is valid for up to two years (*ibid*). An order is not valid unless the Intelligence Commissioner—a quasi-judicial actor whose office was created in 2019 by the *Intelligence Commissioner Act*, SC 2019, c 13, s 50, who is responsible for various oversight and review functions, primarily of the *Communications Security Establishment (CSE)*—approves it (*SAIA*, s 7(2)). An order may also include provisions restricting disclosure of its contents and of the fact that a provider is subject to it (*SAIA*, s 7(1.1)). In other words, the Minister may extend the retention obligation to a provider outside the scheduled classes for up to two years, by an instrument the public may never see.

An "electronic service provider" is defined in C-22 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 (*SAIA*, s 2(1)). As we detailed in our previous post, this definition is so expansive that it effectively amounts to an inventory of the digital world. Cumulatively, the metadata retention regime including the powers to compel ESPs coupled with the section 2(1) definition of ESPs permits the government to compel virtually any entity collecting metadata about Canadians to retain this data for up to six months, as well as force those not already collecting metadata to begin to do so.

While telecommunications carriers, such as Bell, Rogers, and Telus, are the most likely candidates for core provider status, it is doubtful that the government will stop at these entities. Public Safety officials have reportedly signalled an intent to cover not only traditional telecommunications and internet service providers, but also cloud computing providers, social media providers, and online game services (see David TS Fraser, "[The Deeply Problematic Part 2 of Bill C-22: The Supporting Authorized Access to Information Act](#)" (20 April 2026), online (blog): *Canadian Privacy Law Blog*). If true, this means that large online platforms, such as Apple, Meta, and Google, will also fall within the regime. While we can speculate as to which entities the government will ultimately designate as core providers, the troubling reality is that the spectre of who may be captured by C-22's metadata retention obligation is not limited by the Bill itself, but instead left to government discretion with limited oversight and transparency.

To understand why this is troubling it helps to better understand what metadata is and what categories of it the Bill captures. We answer this question below along with a necessary corollary, that being why exactly the government is seeking access to ESP metadata in this way.

2. What is "Metadata" and What Categories of Metadata Does C-22 Capture?

2.1 What is metadata?

Simply put, "metadata" is data about data: information generated as a byproduct of digital activity rather than its substance—who contacted whom, from where, and for how long, rather than what was said. A single metadata record can look trivial. In the aggregate, however, when individual

metadata records are compiled, linked, and analyzed across time, metadata can reveal deeply sensitive personal information about the people who create the data it describes, including a person's movements, associations, health, politics, sexual orientation, and beliefs (Jonathan Mayer, Patrick Mutchler & John C Mitchell, "[Evaluating the Privacy Properties of Telephone Metadata](#)" (2016) 113:20 PNAS 5536; Office of the Privacy Commissioner of Canada, [Metadata and Privacy: A Technical and Legal Overview](#) (Gatineau: OPC, 2014)). It is this aggregating power that makes large-scale retention so dangerous.

Metadata is also pervasive. In computer storage systems, it can mean a file's name, size, when it was created, and who created it. When a smartphone stores a photograph, it often includes metadata such as the phone's make and model, lens focal properties, and the GPS coordinates where the photograph was taken. The creation of a PDF file may include the name and version of the software used to produce it.

In the telecommunications context, metadata includes *who* is talking to *whom* precisely *when* and for *how long*—such as the length and frequency of text messages between people. Such information can be revealing in and of itself—are two people close associates? Friends? Might they be having an affair given the frequency and timing of communication? In short, “telephone metadata is densely interconnected, can trivially be reidentified, enables automated location and relationship inferences, and can be used to determine highly sensitive traits” (Mayer, Mutchler & Mitchell, *supra* at 5536).

2.2 Metadata captured and excluded by C-22

The kinds of metadata potentially captured by C-22 are expansive. It encompasses the full range of metadata described above, from traditional file- and device-level information to the "digital exhaust" unavoidably generated by everyday Internet usage. Amid criticism over the lack of clarity about the scope of metadata that could be retained, the Minister of Public Safety promised on May 27, 2026, [that the government would amend C-22 to clarify what metadata must be stored under the Bill](#). This promise never materialized. Instead, the government added further ambiguous criteria to determine which metadata may be retained under C-22. The promise of clarity has turned into a reality of greater uncertainty.

Section 5(4.1) provides that, before mandating retention of a category of metadata, the Governor in Council must be satisfied that the category and all its elements are "essential for facilitating effective and timely investigations" under the *Criminal Code*, RSC 1985, c C-46 or the exercise of powers under the *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 (*CSIS Act*) (*SAAILA*, s 5(4.1)). Pragmatically, section 5(4.1) does not function as a constraint on metadata retention at all. Rather than defining what metadata may be retained, it substitutes a vague precondition that a "category [of metadata] and all its elements" be "essential" for criminal or national security investigations. Because "essential" is left undefined, it is difficult to conceive that it will limit collection in any meaningful way, absent clarification by the courts (after expensive and resource-intensive litigation) as to what qualifies. In the interim, it would seem that the government will self-assess what constitutes “essential” metadata.

Unfortunately, the term "elements" of metadata is also undefined, and so its intended meaning cannot be drawn from established technical usage. Does it refer to individual data fields, protocol-level attributes, or something else entirely? The Bill does not say. One is therefore left to speculate as to the true scope of what may be retained. The text of the legislation does little to limit its scope. Any meaningful limits will instead have to come from opaque government practice or, again, from costly litigation.

This capacious category of metadata collectable under C-22 is “constrained” by the three exclusions in section 5(4) of the *SAAILA*, which bars the retention of "... the content — that is to say the substance, meaning or purpose — of information transmitted in the course of an electronic service; a person's web browsing history; or a person's social media activities" (*SAAILA*, s 5(4)(a)-(c)). We explore these categories of exclusion below but can summarize now by saying that a category this broad, limited only by a handful of ill-defined exclusions, marks almost no meaningful limit at all.

2.2.1 Exclusions of “content”

Under section 5(4)(a), the retention power does not extend to communication content, meaning information that would reveal the substance, meaning, or purpose of what is transmitted through an electronic service (*SAAILA*, s 5(4)(a)). Excluding such content is not unwelcome, but it does little to address the privacy risks posed by metadata retention itself, in large part because it misses the point. Specifically, the premise of metadata is that sensitive information can be discerned without ever seeing the content. Yet the government seems to rely on the fact that it is not accessing content to assuage concerns about metadata collection. The government’s Charter Statement is illustrative of this point.

In its Charter Statement, the government failed to explicitly address C-22’s metadata retention requirement. Instead, it speaks of "subscriber information" and "transmission data". Each of these appears to be a reference to a “type” of metadata without saying as much. Section 5(2)(d) of the *SAAILA* seems to confirm as much in its wording, which specifically mentions: "...categories of metadata—including transmission data." By disaggregating metadata into a series of narrow, technical-sounding categories, each described as not "particularly sensitive" when taken "by itself", the government repeatedly obscures the defining feature of metadata: that its power lies in the aggregate, which is also precisely why the government, police, and security services want this information. In discussing the production of subscriber information, for example, the government reassures that "[t]he subscriber information sought does not by itself constitute particularly sensitive information, since it is limited to information that identifies clients and services, and does not include the contents of communications" (Department of Justice Canada, [Charter Statement — Bill C-22: An Act respecting lawful access](#) (24 April 2026), emphasis added).

The government's reliance on the absence of content as evidence of diminished sensitivity is deeply misleading. It sidesteps the very feature that makes the collection of this data so intrusive: its capacity, in aggregate, to expose the intimate details of lifestyle and personal choice. These are the very details, those that go to the “biographical core of personal information”, that the Supreme Court recognized that individuals would wish to “maintain and control from dissemination to the state” (*R v Spencer*, [2014 SCC 43 \(CanLII\)](#) at para 27) (*Spencer*). The content exclusion is

welcome as far as it goes, but does little to address the privacy risks that metadata retention itself creates.

The government's analysis also seems to ignore how readily metadata can become an instrument of state surveillance. Former NSA and CIA director Michael Hayden famously said: “[We kill people based on metadata](#).” Aggregated metadata can be used to build a complete picture of a person. Section 5(2)(d) could ostensibly capture the metadata of almost every member of Canadian society.

2.2.2 Exclusion of “browsing history”

Section 5(4)(b) of the *SAIA* carves web browsing out of C-22's retention regime, providing that regulations made under section 5(2)(d) may not require core providers to retain any information that would reveal a person's web browsing history (*SAIA*, s 5(4)(b)). The boundaries of this exclusion are unclear. While a plain reading of the Bill clearly precludes the retention of browser history as we conventionally conceive of the term (that is, the list of websites a user has visited, as recorded by their browser), it does not clearly exclude excellent proxies for this information, like Domain Name System (DNS) server data, which companies could be forced to retain as metadata. In short, by the government being so vague about how it defines metadata, the meagre privacy assurances they are willing to afford are greatly diminished. Let us explain.

Internet users make frequent use of the DNS, which is a crucial backbone of the Internet. DNS is akin to a phonebook that converts hostnames, like [plannedparenthood.org](#), into IP addresses—sequences of numbers like 172.64.80.1. Computers cannot talk to each other based on hostnames; they need IP addresses in the same way that telephones cannot call a business name but rather telephone numbers. DNS is used hundreds of billions to trillions of times a day for this purpose. Thus, DNS can produce an enormous amount of exhaust metadata. DNS, and its secure extension, DNSsec, provide no privacy or confidentiality to users. Things like DoH (DNS-over-HTTPS) protect users' DNS queries from local eavesdroppers, such as other people in the same cafe, airport, or hotel, but ultimately the entity that turns the hostname to an IP address, e.g., users' ISPs, employers, or the Canadian Internet Registration Authority, can be designated as an ESP. Doing so would force them to retain detailed records of every single hostname that a user visits, which is a proxy for a great deal of data reasonably considered sensitive, such as health concerns, political affiliations, and sexual orientation. Significantly, it is not possible to say with any degree of certainty that DNS data will be exempt from collection under the browsing history exclusion.

A DNS query is the routing-and-addressing step that identifies the destination a user is trying to reach, without disclosing the content of the page itself. It is not clear whether such data is excluded as “web browsing history” or authorized for retention as “transmission data”. Recall that transmission data is data relating to “the telecommunication functions of dialling, routing, addressing or signalling” that identifies the “destination” of a communication but “does not reveal [its] substance, meaning or purpose” (*Criminal Code*, s 487.011, and adopted into the *SAIA* in s 5(2)(d)). A DNS query fits this definition closely.

DNS query logs are not obviously “web browsing history” in the ordinary sense of a browser's record of visited pages; they are network-level records generated by the resolution process

necessary to route traffic to the destination. In other words, they are a record of which sites a user's device asked to reach, produced by the network rather than stored by the browser. Yet DNS data functions as an excellent proxy for browsing history. In the aggregate it exposes the same sensitive information about health, politics, and sexual orientation, and it may well qualify as retainable "transmission data" notwithstanding the browsing history exclusion.

Until the government clarifies where DNS data falls, and more generally, the scope of the exclusions to metadata retention under C-22, Canadians cannot know whether one of the most revealing categories of digital exhaust is protected by section 5(4)(b) or authorized for collection under 5(2)(d). DNS data is illustrative of a larger problem posed by C-22: one cannot identify, on a plain reading of the Bill, the scope of data captured by the metadata retention regime.

2.2.3 Exclusion of "social media activities"

Similarly, subsection 5(4)(c) of Bill C-22 creates a metadata exclusion for "social media activities". This exclusion presents a similar interpretive problem to the web browsing history exclusion discussed above, because the term "social media activities" is likewise left undefined. On a narrow reading, the current provision might capture only the substantive content a user generates on a platform—the posts, photographs, videos, and messages they create and share. On a broader reading, it might extend to the metadata that surrounds that content: when a user logs in and out, how frequently and for how long they are active, which features they use, and from where. These two readings produce very different results. The authors very much doubt a broader exclusion is intended, or it would have been clarified. If "social media activities" means only content, then the behavioural metadata of social media use—the patterns of when and how often a person engages—would remain fair game for retention under section 5(2)(d), notwithstanding that such patterns can be every bit as revealing as the content itself. The rhythm of a person's logins can disclose sleep patterns, work schedules, periods of distress, or association with others who are active at the same time. If "social media activities" is read to include this surrounding metadata, the exclusion is considerably broader (and better) than the government's framing suggests. The Bill does not say which reading is intended, and once again the protection Canadians actually enjoy depends on how an undefined term is later construed by the state, and ultimately, if it gets there, by courts.

2.3 Why does the government want increased access to Canadians' metadata?

2.3.1 Public safety, but at what cost?

Two chiefs of police appeared before the Standing Committee on Public Safety and National Security on 7 May 2026: Chief Darcy Fleury of the Thunder Bay Police Service and Chief Myron Demkiw of the Toronto Police Service, both arguing in support of C-22. Their case rested on operational need. Fleury framed the Bill as "about closing [a] gap" opened by digital crime, offering "practical, measured updates that would allow investigators to access certain information more efficiently, always with lawful authority, judicial oversight and a full respect for the charter" (House of Commons, [Standing Committee on Public Safety and National Security, Evidence](#), 45-1, No 37 (7 May 2026) at 1545 (Darcy Fleury)). The Canadian Association of Chiefs of Police, he added, has endorsed it (*ibid*).

Demkiw described the current task of identifying which provider holds a suspect's data as "time-consuming" and prone to "loss of evidence", noting that his detectives had filed 1,900 production orders over twenty months just to locate the right providers (*ibid* at 1550, 1615 (Myron Demkiw)). On the retention period itself, the chiefs wanted more, not less. Asked whether twelve months was reasonable, Fleury answered that "12 months is a good start", but that for long investigations "retention beyond the 12 months—24 months or 36 months—would be ideal" (*ibid* at 1620 (Darcy Fleury)). The evidence provided was anecdotal, and ought to be considered in that light. After all, law enforcement has urged that C-22 be brought into law, and it is conceivable that the evidence given was tailored to serve that purpose. Still, it would be a mistake to discount it completely: police are closest to these investigations, and their account of the delays they face deserves consideration.

Asked to justify C-22's metadata retention regime specifically, the representative from Public Safety Canada said little about investigative need. Appearing before the Standing Committee on Public Safety and National Security, Shannon Hiegel, director general of national security policy at Public Safety Canada, explained that the Bill fixes no specific retention obligation. Instead, it defers both the categories of metadata to be kept and the periods for which they must be kept to a later regulatory process (House of Commons, [Standing Committee on Public Safety and National Security, Evidence](#), 45-1, No 36 (5 May 2026) at 1610 (Shannon Hiegel)). The one-year ceiling in the earlier draft was justified by comparison: Canada had "come in about the middle" between Australia's and the United Kingdom's respective regimes (*ibid*).

Professor Leah West, appearing at the same meeting, accepted that Canada's lawful access framework needs reform but singled out the retention power as problematic. West noted that "[t]he current one-year framework departs significantly from existing 90-day preservation limits, and [that she had] yet to hear a compelling argument for the need for a blanket retention obligation not tied to any specific collection authority or subset of offences such as serious crime" (House of Commons, [Standing Committee on Public Safety and National Security, Evidence](#), 45-1, No 37 (7 May 2026) at 1540 (Leah West)).

We note that the retention period was shortened from one year to six months in the most recent amendments to the Bill on June 18, 2026, ostensibly in response to security [concerns and criticisms](#) raised by privacy scholars and advocates (see also Robert Diab, "[Canada's Metadata Retention Plan Would Make It an Outlier](#)" (14 May 2026)). The government offered no explanation as to why the new six-month retention period was necessary, and it is unclear if the reduction reflects an evidence-based assessment of investigative need, or a meagre attempt to placate critics, some of whom have called for the retention period to be reduced to 30 days to minimize the security risks associated with long-term metadata storage (House of Commons, [Standing Committee on Public Safety and National Security, Evidence](#), 45-1, No 37 (7 May 2026) at 1645 (Michael Geist)).

Whatever the period, the continuing issue is that C-22 authorizes prospective, suspicionless retention of the entire population's metadata, untethered to any specific investigation. This represents a significant deviation from existing lawful access mechanisms. For example, tools like preservation demands and preservation orders (*Criminal Code*, ss 487.012–487.013), production orders (*ibid*, ss 487.014–487.018), and interception of private communications (wiretaps) (*ibid*, s 186), each require context for the request, evidentiary thresholds that must be met, and oversight.

Preservation orders deserve particular attention in this regard. A preservation order allows police to require a company, such as a telecommunications provider, to keep specific computer data (including metadata) that the company has in its possession, so that the data does not disappear while investigators seek the legal authority to obtain it (*ibid*, s 487.013(1)). In other words, Parliament has already given investigators a tool to require organizations to preserve metadata, thereby preventing it from disappearing before investigators have an opportunity to undertake the steps to lawfully access such data. Importantly, preservation orders operate on a case-by-case basis, under judicial supervision, and only where there is reasonable ground to suspect that an offence has or will be committed and that the data will assist in the investigation (*ibid*, s 487.013(2)). It is not clear nor has compelling evidence been presented by the state as to why this existing power is insufficient to meet investigatory and public safety needs. Absent such evidence, the necessity of the population-wide retention that C-22 contemplates remains dubious.

In comparison to existing lawful access mechanisms, C-22 requires no prior authorization for core providers, no threshold of suspicion, and no identified target. An obligation imposed on any other (non-core) ESP by Ministerial order requires the Intelligence Commissioner's approval (*SAIA*, s 7(2)), but that approval attaches to the order, not to any person whose data is retained. In effect, C-22 authorizes the prospective collection and storage of metadata relating to individuals who are not suspected of any wrongdoing—permitting the government to mandate the bulk retention of Canadians' data "just in case" the information, or some portion of it, later acquires evidentiary or intelligence value, regardless of whether any connection to criminality exists at the time of collection. It is unclear, other than the general (and generalized) assertions of police and other state organizations, as to why existing mechanisms, with these safeguards, are inadequate to meet the needs of modern investigations, or why the attempt at modernization requires (in their view) what can only be described as a significant departure from the traditional safeguards accompanying lawful access powers. The result of C-22 is to create a powerful surveillance tool, free from traditional constraints as to breadth and duration associated with existing lawful access tools. The result is a regime that creates the possibility for significant privacy harms to befall virtually all Canadians.

Data that would otherwise be ephemeral and not necessary to retain in the first place thus becomes a systemic risk to *everyone*—not only those for whom probable cause or even reasonable suspicion has been first established—so as to provide law enforcement with a digital time machine to go back and decide who they should have been following when they did not have a warrant. This risk manifests as a dragnet digital dossier on all citizens. Worse, the very nature of this data means that the dossier needs to be both easily available for ESPs to continually update while ensuring it is protected from all manner of unauthorized access: threat actors, foreign intelligence, rogue employees of the ESPs, and future governments. This is not easy, and recent history is replete with examples of data breaches of such data.

The inconvenient reality for the government, which is relying on public safety justifications in support of C-22, is that mandatory metadata retention *undermines* data security, and thereby constitutes a very real public safety harm. Every database of retained communication data immediately becomes a high-value target, and the larger and more centralized the trove, the greater the harm when it is inevitably breached by hackers from organized crime or foreign state adversaries.

3. C-22 Metadata Retention Regime is Inconsistent with Section 8 of the *Charter*

3.1 C-22 transforms ESPs into agents of the state

We reviewed section 8 of the *Charter* in our [first blog post](#) and encourage readers to review it for the legal details on how it works and how it is applied. In it, we provided more detail on when section 8 applies, but generally it only applies to a state agent (government actor) who conducts a search or seizure of a person, place or thing to which a privacy interest attaches.

The implementation of Bill C-22's data retention mandates falls to third-party ESPs, which are of course not state agents. However, by mandating pre-emptive cooperation and collection, the effect is to transform ESPs into agents of the state for the purposes of metadata retention. In *Eldridge v British Columbia*, the Supreme Court held that “[i]n order for the *Charter* to apply to a private entity, it must be found to be implementing a specific governmental policy or program” (*Eldridge v British Columbia* (Attorney General), [1997 CanLII 327 \(SCC\)](#), [1997] 3 SCR 624 at para 43, affirmed in *R v Buhay*, [2003 SCC 30 \(CanLII\)](#) at para 28, emphasis added) (*Buhay*). In the case of Bill C-22, ESPs are required to implement a mandatory metadata retention regime not of their own commercial volition, but because the statute compels them to do so on the state's behalf. This is the precise circumstance contemplated in *Eldridge*. The ESP is not merely a private actor incidentally cooperating with law enforcement, but an entity “implementing a specific governmental policy or program”—namely, the legislative scheme of data retention designed to facilitate state access to metadata. The ESP becomes the instrument through which the state accomplishes the warrantless preservation of information that it may later seek to compel.

The salient question in this context is whether the search or seizure would have taken place *but for* the intervention of the state (*Buhay* at para 29, citing *R v Broyles*, [1991 CanLII 15 \(SCC\)](#), [1991] 3 SCR 595). The answer is less clear, particularly given the lack of clarity on which ESPs are covered and what metadata will be captured by C-22, as well as what metadata ESPs were collecting and retaining beforehand; however, to the extent that ESPs are not already collecting and retaining metadata as prescribed by C-22, the answer is plainly no. It is theoretically possible that some ESPs are already collecting and retaining metadata in the manner contemplated by C-22. It is difficult to conclude on this question in the abstract, particularly given the lack of specificity in C-22's metadata provisions, but it does raise the question: were ESPs already compliant with these provisions, what purpose is served by enacting them? In short, ESPs were already compliant, thus significantly lessening or obliterating the need for the legislation; or, ESPs were not already compliant, in which case section 8 of the *Charter* is engaged.

It seems far more likely that these provisions are directing metadata retention practices that are not already common practice in the market. Having concluded that C-22 transforms ESPs into agents of the state, we now consider whether Canadians hold a reasonable expectation of privacy in their metadata, and whether retention of metadata as mandated by C-22 amounts to a seizure under section 8 of the *Charter*.

3.2 Reasonable expectations of privacy and seizure under section 8 of the Charter

Section 8 protects an individual's "reasonable expectation of privacy" (*Hunter et al v Southam Inc*, [1984 CanLII 33 \(SCC\)](#), [1984] 2 SCR 145 at 159) (*Hunter*). Where the state intrudes on that expectation, a search has occurred (*ibid*; *R v Tessling*, [2004 SCC 67 \(CanLII\)](#) at para 18; *R v Cole*, [2012 SCC 53 \(CanLII\)](#) at para 34; *Spencer* at para 16). Where the state takes a thing from a person without that person's consent, a seizure has occurred (*R v Dymnt*, [1988 CanLII 10 \(SCC\)](#), [1988] 2 SCR 417 at para 26) (*Dymnt*). Section 8 protects people, not property, so a claimant need not establish a proprietary interest in the thing searched or seized (*Hunter* at 158; James A Fontana & David Keeshan, *The Law of Search and Seizure in Canada*, 13th ed (Toronto: LexisNexis Canada, 2023) at 5).

The threshold question for C-22 is therefore whether Canadians hold a reasonable expectation of privacy in the metadata the Bill requires ESPs to retain. The short answer to this is, 'clearly'. In the leading case of *R v Spencer*, the Supreme Court recognized that informational privacy embraces anonymity, and that linking seemingly innocuous data (like metadata) to an identifiable individual can reveal intimate details of that person's lifestyle and personal choices (*Spencer* at paras 27, 47). C-22's retention regime is useful to the state only because each retained record can later be linked to an identifiable subscriber or device. We now consider whether the retention of that metadata amounts to a seizure.

Under *Dymnt*, a seizure is the taking of a thing from a person by a public authority without that person's consent (*Dymnt* at para 26). C-22's mandate creates the store of data that the state may later search. Indeed, absent C-22, we can presume that much of the data captured by C-22 would never be stored, and a later production order would find nothing to produce—production orders being used routinely to access data from ESPs. To suggest otherwise would mean that existing lawful access powers are more than sufficient and the retention regime under C-22 totally unnecessary to achieve the government's stated public safety purposes. The retention of metadata under C-22 by an ESP, acting as an agent of the state without the consent of the individual to whom the metadata relates, is therefore a warrantless seizure under section 8 of the *Charter*. Establishing a seizure, however, is only the threshold question; section 8 only protects against *unreasonable* seizures.

A valid search or seizure under the *Charter* ordinarily requires prior judicial authorization, and to obtain a warrant the state must show reasonable and probable grounds both that an offence has been committed and that evidence of it will be found (*Hunter* at 168). A warrantless search or seizure is *prima facie* unreasonable under section 8 of the *Charter* (*Hunter* at 161; *R v Collins*, [1987 CanLII 84 \(SCC\)](#), [1987] 1 SCR 265 at para 22) (*Collins*). Once the claimant establishes that a search or seizure occurred without prior authorization, the burden shifts to the Crown to demonstrate, on a balance of probabilities, that it was nonetheless reasonable (*Collins* at para 22). A search will be reasonable only if (1) it is authorized by law, (2) the law itself is reasonable, and (3) the search is carried out in a reasonable manner (*ibid* at para 23).

The second requirement—that the authorizing law itself be reasonable—is likely to be problematic for C-22. The reasonableness of the law is assessed by weighing the individual's reasonable expectation of privacy in the subject matter against the state interest the law advances. In criminal cases, "courts presume the standards in *Hunter* should apply, with departures from them needing

to be justified by either a lower expectation of privacy, a pressing state interest arising in the situation, or both” (Robert Diab & Chris D L Hunt, *Search and Seizure* (Toronto: Irwin Law, 2023) at 254, citing *R v Grant*, [1993 CanLII 68 \(SCC\)](#), [1993] 3 SCR 223 at 239–240). The court will look to whether the state has a strong or compelling interest that warrants a deviation from the *Hunter* standard, the measure’s intrusiveness and reliability (generally the law should try to use the least intrusive measure to advance its objective), as well as the oversight and accountability safeguards in the law itself, for example, the requirement that the state secure a warrant before performing the search (*ibid* at 256–260).

We generally accept that the government has a compelling interest in modernizing Canada's lawful access framework, which engages both national security and public safety objectives. C-22, however, represents a significant and sweeping intrusion on Canadians’ privacy interests absent any of the constitutional safeguards in *Hunter*. While legitimate and compelling state objectives can justify a departure from the *Hunter* standard, such departures are narrowly circumscribed (see e.g., *R v Fearon*, [2014 SCC 77 \(CanLII\)](#) at para 83). C-22 cannot be said to be minimally intrusive or carefully tailored—as we discussed, above, many of its key definitions provide no limits or real explanations at all. Rather than targeting individuals on reasonable suspicion, it compels the prospective, indiscriminate retention of metadata drawn from the entire population, in anticipation that the state may later wish to access it. The vast majority of those swept in will never fall under suspicion; their data is retained not for its relevance to any investigation, but as an apparently acceptable casualty of dragnet warrantless surveillance in the pursuit of “public safety”. A scheme that sweeps in the data of every Canadian to capture the few of future investigative interest is the antithesis of a minimally intrusive measure.

The collection of metadata authorized by C-22 is warrantless and triggered by no evidentiary threshold whatsoever. Rather than requiring individualized suspicion or prior judicial authorization, it compels the prospective seizure of vast quantities of data drawn from the entire Canadian population. As such, the metadata retention regime authorized by C-22 is likely to violate section 8 of the *Charter*. Establishing a section 8 breach does not end the inquiry, however. A law that infringes a *Charter* right may nonetheless survive if the government can justify it under section 1.

3.3 C-22’s metadata retention regime unlikely to be saved by section 1 of the Charter

Section 1 of the *Charter* affords the government an opportunity to argue that a law should be upheld even if it infringes upon a *Charter* right. Section 1 “permit[s] [reasonable] limits to be placed on guaranteed rights and freedoms” but only to the extent that those limits “[can be demonstrably justified in a free and democratic society](#)” (*Charter*, s 1). Whether or not a limit on a constitutionally guaranteed right is “reasonable” and “justifiable in a free and democratic society” is answered using a test originally set out by the Supreme Court in *R v Oakes*, [1986 CanLII 46 \(SCC\)](#), [1986] 1 SCR 103 (*Oakes*), known as the *Oakes* test. Broadly, the *Oakes* test considers whether the government has a pressing and substantial legislative objective, and balances that objective against the means used to achieve that objective (*Oakes* at paras 69–70). When undertaking the proportionality analysis, the court will consider whether the legislation is rationally connected to the stated objective, whether the law impairs the *Charter*-protected right

as little as possible, and finally, whether there is proportionality between the positive and negative effects of the legislation.

C-22's metadata retention regime is unlikely to be saved under section 1 of the *Charter*. The government would almost certainly clear the first hurdle. There are legitimate investigatory, public safety, and national security objectives underpinning C-22. The retention of metadata is, at least at a general level, rationally connected to those ends. As we have discussed in this post, metadata, particularly in the aggregate, is a powerful tool that can reveal significant sensitive information about an individual. It is at the minimal impairment stage that C-22's framework is most likely to fail.

The question at the minimal impairment stage is whether the limit impairs the right no more than is reasonably necessary to achieve the objective. We suggest that the answer in the case of C-22 must be that it does not. It is conceivable that the government would argue that the six-month retention cap alongside the exclusions in section 5(4) and "essential" criteria from section 5(4.1) is sufficient to tailor the law in a manner required by the minimal impairment standard. While these limits may narrow what is retained (and as we discussed, even that is dubious), they do nothing to introduce a standard of individualized suspicion or judicial pre-authorization as *Hunter* requires in relation to designating core providers. Further, section 7(2) signals that independent approval is feasible; after all, it is a requirement for the secret Ministerial orders in section 7(1), so, not extending it to regulations designating core providers is a less-impairing option that the government could have reasonably exercised.

Indeed, a blanket, warrantless six-month retention mandate, applied to the entire population, is difficult to defend as minimally impairing. This is particularly true where far more targeted alternatives exist. Canadian law already provides for a host of preservation demands and orders (see *Criminal Code*, ss 487.012–487.013) and production orders (see *Criminal Code*, ss 487.014–487.018). We have ways of getting at this data and law enforcement (and intelligence agencies) do it regularly for the purposes of specific criminal investigations.

Importantly, with the exception of short-lived preservation demands, each of the existing lawful access tools permits the state to act only in connection with a specific investigation, on a threshold of articulable suspicion or belief, against an identified target, and with advance authorization. C-22, by comparison, requires no degree of suspicion and no identified target. Regulations under section 5(2)(d) require no prior authorization at all. Ministerial orders under section 7(1) require the Intelligence Commissioner's approval (*SAIA*, s 7(2)), but the Commissioner approves the order as it relates to the designated entity, not the retention of any particular *person's* data. While we have accepted the notion that Canada's lawful access regime requires updating, modernization in such a manner that deviates significantly from established standards ought to be viewed with intense scrutiny. Anecdotal assertions of public safety cannot justify so significant a departure from the well-established principles of search and seizure that safeguard Canadians' constitutionally guaranteed rights.

It is also unlikely that C-22 will succeed at the final stage of the *Oakes* analysis—the balancing of salutary against deleterious effects. There may well be certain investigatory benefits to the mass retention of metadata but these benefits are speculative: they may only materialize in some cases

while the burden of the regime will be borne by virtually all Canadians. Under C-22, the data is retained not because it is known to be relevant to any investigation, but in anticipation that some portion of it may one day (or at least within six months) prove useful. The impact of a regime requiring this sort of retention is to place every Canadian who participates in the digital sphere—the overwhelming majority of whom will never be the subject of any investigation—at a heightened and continuing risk of privacy harm, whether through unauthorized access, data breach, function creep, or the simple fact of the state assembling a standing record of the population's associations and movements. In our view, a speculative and occasional benefit to law enforcement cannot outweigh a definite and population-wide intrusion on a substantial privacy interest. The deleterious effects of the regime are therefore disproportionate to its salutary ones, and on this final branch, as on minimal impairment, we contend that the section 1 justification fails.

4. Recommended Amendments to C-22

We offer the following recommendations to amend C-22 in the event that the metadata retention regime proceeds. We do not, however, accept that the regime is necessary. As discussed above, the most effective way to secure Canadians' data is not to store it at all; any retention of data increases the risk of a leak, breach, or other compromise. Canada may need lawful access reform, but no compelling evidence demonstrates that C-22's metadata retention regime is necessary given the tools that Canadian law already provides. The recommendations below therefore aim to mitigate the regime's risks, not to endorse it.

At a minimum, we suggest that C-22 should be amended to:

1. **Define, on the face of the statute, the categories of metadata that may be retained, and clarify the scope of the section 5(4) exclusions and section 5(4.1) criteria.** The Bill should specify what "metadata" is subject to retention rather than leaving the question to regulation. It goes without saying that metadata categories subject to retention should also be carefully defined and scrutinized by experts. The exclusions under section 5(4), namely "web browsing history" and "social media activities", must be defined so that their boundaries are clear. Amendments should be explicit as to whether DNS query data is excluded as web browsing history or captured as transmission data. Furthermore, the government should specify what "essential" means for the purpose of the section 5(4.1) criteria and what constitutes an "element of metadata". Specificity ought to be prioritized before the Bill becomes law, not after.
2. **Confirm that ESPs not already collecting a given category of metadata will not be compelled to build new collection systems to do so.** The retention obligation should attach only to data a provider already holds in the ordinary course of business, not require the creation of novel collection infrastructure that increases every Canadian's exposure to breach.

3. **Reduce the metadata retention period and create a framework for extensions of this period that requires judicial authorization.** The period should be no longer than law enforcement reasonably needs to conduct preliminary investigative steps and obtain judicial authorization to search the data. Extensions beyond that initial period should be available only on judicial authorization. At House of Common hearings, Dr. West mentioned the usual 90-day period found for retention in the *Criminal Code*; that seems a good place to start.
4. **Guarantee a high level of data protection and security for retained data and require Canadian storage.**
5. **Explicitly require that retained metadata be safeguarded in line with industry best practices for data security, including measures such as encryption, strict access controls, and breach notification.**
6. **Explicitly provide for the irreversible destruction of retained data at the end of the retention period.**
7. **Consider extending independent judicial oversight to every retention obligation.**

This post may be cited as: Alexandra Lyn, Joel Reardon & Michael Nesbitt, “Decrypting Bill C-22, Part 2: Keeping Tabs: C-22 and the Year (Now Half-Year) of Metadata Retention” (19 October 2026), online: ABlawg, http://ablawg.ca/wp-content/uploads/2026/10/Blog_AL_Part2_BillC-22.pdf

To subscribe to ABlawg by email or RSS feed, please go to <http://ablawg.ca>

Follow us on Twitter [@ABlawg](https://twitter.com/ABlawg)

