A Critique of Bill C-22 through a Systems Engineering Lens

Abstract

The debate surrounding Canadian digital policy and "lawful access" has re-emerged with the introduction of Bill C-22. Proponents argue that the legislation is a necessary modernization to equip law enforcement with the tools required to navigate the digital landscape. However, when evaluated through the lens of systems engineering, cryptography, and modern threat modelling, the mandate for telecommunications and service providers to build and maintain "interception-capable systems" can significantly weaken security, making the audience feel concerned about vulnerabilities that could be exploited.

The Architectural Paradox of Exceptional Access

At the core of the proposed lawful access framework in Bill C-22 is the requirement for service providers to architect systems that are interception-capable (Geist, 2026). This design choice directly introduces systemic vulnerabilities, as cryptographic and security communities recognize this as a mandate for "exceptional access" or, more colloquially, a backdoor. Highlighting this connection helps focus on how system architecture flaws compromise security.

The policy discourse frequently treats this requirement as a mere administrative hurdle - a feature that law enforcement can securely bolt onto existing networks. This demonstrates a fundamental disconnect from the mathematical reality of cryptography. A system cannot be engineered to be mathematically secure against unauthorized intrusion while simultaneously maintaining a deliberate, systemic vulnerability designed for authorized use.

From a systems engineering perspective, robust security relies on "institutional friction." Secure architectures intentionally design bureaucratic and technical hurdles, such as multi-party computation, quorum requirements for key generation, and split-knowledge protocols, to ensure that no single actor can compromise the system. The proposition that a system can bypass this friction to be "completely secure, except for law enforcement" is an architectural paradox. As highlighted in the seminal cryptology report *Keys Under Doormats*, building exceptional access into digital infrastructure reverses forward security design practices, exponentially increases system complexity, and creates vulnerabilities that are equally exploitable by a police officer holding a warrant, an advanced persistent threat, or a rogue employee(Abelson et al., 2015). A

mandated bypass cannot be used to cryptographically determine the intent or legal authorization of the entity exploiting it (Ossowski, 2026).

Threat Modelling and the Cloud Migration Conflict

The requirements of Bill C-22 are incompatible with modern enterprise infrastructure, which emphasizes decentralization through cloud-native environments like AWS and GCP. These platforms are governed by Zero Trust Architecture principles, assuming threats both inside and outside the network, and requiring continuous verification (NIST, 2020). Emphasizing this contrast highlights the risks of centralization mandated by Bill C-22 and its threat to security.

In modern cloud deployments, security is enforced through extreme decentralization. Concepts such as Workload Identity Federation, ephemeral, short-lived credentials, and the principle of least privilege are deployed to ensure that no single entity, even a root system administrator, has persistent, unfettered access to encrypted data payloads.

Bill C-22 proposes a legislative inversion of this standard, demanding a systemic "Full Trust" mechanism for state actors. When telecommunications and digital service providers are legally compelled to design interception capabilities, they must artificially centralize access controls and engineer long-lived, omnipotent access pathways. By legally mandating these capabilities, the state is effectively requiring SRE and DevOps teams to architect deliberate Single Points of failure into highly available systems. This artificially inflates the attack surface of the nation's critical digital infrastructure, directly contradicting the fundamental design principles of modern cloud security.

The argument that Canada's international allies have already implemented similar regimes is frequently invoked to justify these reforms. However, adopting a flawed architectural standard merely to align with international standards is poor engineering and worse policy. Emulating systems that inherently weaken national cybersecurity postures is not progress; it is the replication of a demonstrable architectural failure.

Not only do these architectural changes contradict security best practices, but they also make the audience feel wary of increased vulnerabilities. By legally compelling the creation of centralized, omnipotent access pathways, the legislation risks turning Canadian networks into high-value Single Points of Failure, which are attractive targets for bad actors. This shift can make the audience feel concerned that the entire infrastructure could be compromised by a single breach.

From a technical standpoint, creating the level of centralization this would require creates an enormous single point of failure. The Single Points of Failure that are the stated goal of the act would not just provide technical failures, but would also run headlong into the process of undermining all of the demonstrated best practices for data governance and privacy, compromising the online safety of Canadians, not just on the technical front but also on the organizational front.

Data Minimization and the Structural Panopticon

Beyond the risks to cryptography, the legislation poses significant challenges to modern data governance and privacy frameworks. The most effective method of securing sensitive data is to adhere strictly to the principle of data minimization: data that is not collected or retained cannot be intercepted, breached, or abused.

Bill C-22 incentivizes the opposite. By establishing frameworks for compelled information production and interception capabilities, it necessitates retaining and structuring vast amounts of subscriber and communication data. This effectively shifts the burden of maintaining a passive, state-accessible surveillance apparatus onto private enterprises, forcing infrastructure engineers to function as de facto surveillance administrators. While the mechanism proposed in Bill C-22 may appear to bridge the perceived capability gap faced by law enforcement in their goal to maintain the ability to investigate serious crimes in the encrypted age, that bridge will unfortunately fail due to the underlying architectural requirements being self-defeating. Mass data retention optimizes for data volume rather than actionable intelligence, and they are not the same thing. This may be a failure in requirements gathering, resulting in a system that is mathematically guaranteed to degrade the security of the infrastructure it aims to protect. Preferring continuous, passive data harvesting over leveraging or improving the existing legal and technical requirements and tools for targeted investigation poses other problems.

Information Fatigue Syndrome and Data Paralysis

The preference for mass retention introduces a key counterintuitive system failure, noise. Effective investigation requires reliable and clearly relevant information. Establishing frameworks that necessitate retaining and structuring vast amounts of low-value, almost-certainly irrelevant data can lead to data paralysis. An immense volume of noise will have the opposite effect of what is desired and ultimately lead to slower, less focused, poorer investigations. This is an example of Information Fatigue Syndrome as described recently by Dobrica Savic in The Grey Journal in 2023. Even Dell has conducted research showing that 70% of businesses are collecting data faster than they can use or analyze it, and 64% of organizations report having too much data to meet their security and compliance requirements.

The societal implications of constructing this infrastructure cannot be ignored. The creation of a turn-key surveillance capability requires an absolute, sustained trust that the institutions wielding it will remain infallible and completely resistant to scope creep. Recent domestic legal challenges to the use of extraordinary state powers highlight the inherent friction between state authority and civil liberties. The capabilities detailed in the proposed reforms represent an unprecedented consolidation of informational power, operating under the assumption that future administrations will never misuse the tools constructed today even if we were to allow for the perfect trust in those that hold the keys, not just now, but forever; even so we would have to admit that this would necessarily alter public behaviour and generate a psychological sense of hazard that could conceivably have long lasting effects.

A Strategic Framework for Engineering Solutions

Pushing towards "Surveillance by design" could be undermined by constitutional risks (notably R. v. Spencer and R. v. Bykovets). These precedents establish high bars for privacy in digital metadata. Furthermore, mandatory mass data collection led to poor investigative outcomes due to the aforementioned Information Fatigue Syndrome. To maintain the best possible outcomes and ensure effective, surgical policing, evidence shows that law enforcement must pivot away from indiscriminate retention toward actionable, intelligence-led systems.

The following non-invasive systems provide proven alternatives to the proposals in Bill C-22.

Federated Metadata Indexing Protocol

The first is precision metadata analytics and statistical intelligence. The idea is to shift the goal from bulk storage to targeted statistical search. The priority should be data quality over quantity. Here we intend to replace mass data retention with a pull-based, warrant-verified query architecture.

Architectural Components

Provider-side Metadata Nodes

Service providers will still be expected to contribute to these solutions. In this initial way, they should be expected to maintain standardized, isolated databases containing only non-content metadata, such as connection logs or routing information.

Mediator API

A hardened interface using Mutual TLS (RFC 8446) will need to be architected and built to accept cryptographically signed queries from authorized law enforcement agencies.

Judicial Validator

A centralized, offline hardware security module implementing FIPS 140-3 Level 4 standards that generates one-time session keys upon the digital signing of a warrant by a judge.

Engineering Requirements

Zero-Copy Search

The protocol must use Homomorphic Encryption (it is proposed to use Brakerski-Gentry-Vaikuntanthan scheme via HElib) to process data in place. This allows law enforcement to query provider databases without the provider ever seeing the query parameters, and without law enforcement being able to see the entire dataset. Requestors cannot move data to government or law enforcement servers. The query is to be sent to the data via the mediator API, and the specific filtered result is returned to the requester.

Schema Standardization

Metadata must be mapped to a universal schema (STIX 2.1 OASIS) designed to be useful for law enforcement without requiring investigators to understand the provider's underlying internal architecture.

Cryptographic Audit Trails

Every query must be appended to a permissioned, append-only ledger using Merkle Tree Proofs (RFC 9162). This is how one can ensure a necessary amount of institutional friction, and any "fishing expeditions" are visible during oversight audits.

Targeted Endpoint Forensics Interfaces

The second concrete element of a functional framework is targeted endpoint forensics. Rather than introducing systemic vulnerabilities directly into the network backbone, success is much more effectively achieved by targeting specific compromised endpoints. This shifts the "interception" requirement from the transport layer to the application layer, thereby preserving end-to-end encryption while enabling lawful access to a suspect's specific data.

Architectural Components

Standards-Based Non-Invasive API

A standardized interoperability framework can be developed, designed to leverage existing hardware-level forensic hooks and industry-standard pairing protocols such as FIDO2 or WebAuthn. It enables secure, warrant-based access through existing manufacturer-approved diagnostic interfaces.

Sandbox-based Remote Evidence Acquisition

A protocol developed for deploying a temporary, isolated forensic container to a suspect's device using the Open Container Initiative.

Engineering Requirements

Volatile Memory Analysis

Instead of breaking encryption in transit, we leverage the ability to capture data while it is decrypted in device memory for the user's use.

Ephemeral Deployments

The remote evidence acquisition container must be self-destructing validated using dm-verity. It cannot persist beyond the duration of the warrant and must not be able to modify user data.

A full technical description and roadmap for these proposed systems will be found in an upcoming Appendix to this document.

Financial Feasibility

Overall, the projected cost of the adjusted proposal described above is approximately CAD$25M, broken down as follows. The initial design work is projected to cost CAD$5M, and can be supported by the NRC's "Tier 2" Collaborative R&D model.

The initial implementation, integration, and scaling work is projected to cost CAD$12.5M, which the DI Assist fund can support. As a bonus, this allows increased defence spending to be reinvested in Canadian Software Engineers and Subject Matter Experts.

The specialized training required to make some of these proposed new systems work can be covered by the Canadian Police College for CAD$7.5M.

Overall, that puts the combined cost at CAD$25M. This is far lower than the projected direct cost of Bill C-22 as it stands written today. A more detailed breakdown of how these cost numbers were arrived at can be found in a separate Appendix.

Conclusion: Security Through Mathematics, Not Mandates

Governing in the digital age requires confronting complex threats without compromising the structural integrity of the networks upon which society relies. The "lawful access" mechanisms proposed in Bill C-22 attempt to bridge a perceived law enforcement gap by legally mandating the creation of technical vulnerabilities.

This approach is fundamentally incompatible with the realities of modern cybersecurity and cloud infrastructure. True national security cannot be achieved by weakening the cryptographic foundations of our communications. Legislation governing digital infrastructure must be grounded in mathematical reality, emphasizing end-to-end encryption, data minimization, and decentralized trust models. Championing policies that demonstrably degrade the security of Canadian networks in the pursuit of lawful access is an architectural misstep that leaves the public significantly more vulnerable to the very threats the state seeks to mitigate.

References

Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Diffie, W., ... & Schiller, J. I. (2015). **Keys under doormats: Mandating insecurity by requiring government access to**

all data and communications. Computer Science and Artificial Intelligence Laboratory, Massachusetts Institute of Technology.

Brakerski, Z., Gentry, C., & Vaikuntanathan, V. (2014). **(Leveled) fully homomorphic encryption without bootstrapping**. *ACM Transactions on Computation Theory*, *6*(3), 1–36. https://doi.org/10.1145/2633600 (Blindenbach et al., 2024).

Dell Technologies. (n.d.). **The data paradox: Research findings**. Retrieved from https://www.delltechnologies.com/asset/es-co/solutions/infrastructure-solutions/industry-market/data-paradox-research-findings.pdf

Dimitriadis, A., Prassas, C., Flores, J. L., Kulvatunyou, B., Ivezic, N., Gritzalis, D. A., & Mavridis, I. K. (2021). Contextualized filtering for shared cyber threat information. *Sensors*, *21*(14), 4890. https://doi.org/10.3390/s21144890

Geist, M. (2026, March 13). A tale of two bills: Lawful access returns with changes to warrantless access, but dangerous backdoor surveillance risks remain. **MichaelGeist.ca**.

Laurie, B., Messeri, E., & Stradling, R. (2021). *Certificate Transparency Version 2.0* (RFC 9162). Internet Engineering Task Force. https://datatracker.ietf.org/doc/html/rfc9162

National Institute of Standards and Technology. (2019). *Security Requirements for Cryptographic Modules* (FIPS PUB 140-3). U.S. Department of Commerce. https://doi.org/10.6028/NIST.FIPS.140-3

National Institute of Standards and Technology. (2020). **Zero trust architecture** (Special Publication 800-207). U.S. Department of Commerce.

Open Container Initiative. (2021). *OCI Image Format Specification* (v1.0.2). https://github.com/opencontainers/image-spec (Giallorenzo et al., 2021).

Ossowski, Y. (2026, March 22). Canada's lawful access act is a backdoor by another name. **Yael.ca**.

R. v. Bykovets, 2024 SCC 6.

R. v. Spencer, 2014 SCC 43, [2014] 2 S.C.R. 212. (Laidlaw, 2017).

Rescorla, E. (2018). *The Transport Layer Security (TLS) Protocol Version 1.3* (RFC 8446). Internet Engineering Task Force. https://doi.org/10.17487/RFC8446

Rivera-Dourado, M., Gestal, M., Pazos, A., & Vázquez-Naya, J. (2024). A novel protocol using captive portals for FIDO2 network authentication. Applied Sciences, 14(9), 3610. https://doi.org/10.3390/app14093610

Savic, D. (2023). Information fatigue and digital burnout. **The Grey Journal**, **19**(2).