— A Justice Centre Report —

February 24, 2026

Privacy collapse: Canada's expanding surveillance state

How Canada's expanding digital identity and Bills C-2 and C-8 threaten privacy, autonomy, and dignity.

Author: Nigel Hannaford

Justice Centre
for Constitutional Freedoms

We Defend
Freedom
in Canada

Abstract

How politicians wielded the extraordinary powers of the *Emergencies Act* – illegally invoked by Prime Minister Trudeau in February 2022 – exposed how rapidly Canada's surveillance state has advanced, undermining Canadians' privacy, anonymity, security, autonomy and dignity. Now, under border security and cybersecurity pretexts, parliamentary Bills C-2 and C-8 would, if passed, extend the reach of the federal government's surveillance apparatus to online service providers, which would compel online service providers to provide confidential subscriber data without a warrant, weaken encryption, and disconnect users without judicial oversight or notice to users. This report warns of a fundamental reordering of the relationship between citizen and state, urges Canadians to demand that their Members of Parliament defeat or amend these bills, and further urges those in power to strengthen legislative protections for privacy in Canada.

Acknowledgements

We thank the thousands of Canadians who continue to support the Justice Centre with their donations. Their generosity empowers the Justice Centre to defend freedom in Canada and to shape public policy that respects *Charter* rights and freedoms.

Updates to this report

This is Version 1.0 of this report, which may be updated periodically.

About the author

This report was written by veteran journalist and public policy analyst Nigel Hannaford.

Contents

Abstract **2**

Executive summary **4**

Introduction **6**

The emerging surveillance state in Canada **7**

Privacy, a right under attack 7

The imperative of anonymity 8

Digital ID platforms empower surveillance states 9

Bills C-2 and C-8: An authoritarian surveillance combo **11**

Bill C-2 – Warrantless data demands 11

Bill C-8 – Government-forced "deplatforming" 13

The resulting dragnet: total surveillance **14**

Deterring bad actors: existing tools are sufficient 14

Will Canadians retain any privacy? **15**

Conclusion **17**

Privacy must be protected, and state surveillance power strictly limited 17

Bibliography **19**

23

Executive summary

Canada's emerging surveillance state, accelerated by Bills C-2 and C-8 (before Parliament at time of writing), profoundly threatens personal freedoms, privacy, anonymity, and other core and historic liberties protected under the *Canadian Charter of Rights and Freedoms*.

When Prime Minister Justin Trudeau invoked the *Emergencies Act* in 2022, Canadians first realised how vulnerable was their long-standing "reasonable expectation of privacy," enshrined in part in the *Charter* section 8 right to be free from unreasonable search and seizure.[1] Canadians' privacy was breached when the Government of Canada ordered financial institutions to freeze the bank accounts of donors to the Freedom Convoy, who had committed no crime and were afforded no opportunity to defend themselves.

This compelled disclosure of financial transactions was later ruled illegal by the Federal Court (2024) and the Federal Court of Appeal (2026).[2]

The illegal use of the *Emergencies Act* only exposed an already advanced framework of social monitoring. In addition to the Government of Canada's invasion of Canadians' financial privacy, it was also revealed that the Public Health Agency of Canada had quietly tracked the movements of more than 33 million cellphones[3] for almost a year during Covid, and that the RCMP had conducted unauthorised experiments with facial recognition technology in 2019.[4]

Then, in mid-2025, the Government of Canada introduced Bills C-2 (*Strong Borders Act*) and C-8 (*An Act respecting cyber security*...).[5, 6] Still in parliamentary hearings as of February 2026,[7] they will, if passed, extend surveillance deep into digital realms. Presented

[1] Nick. "Understanding the Reasonable Expectation of Privacy in Canadian Criminal Law." Canadian Criminal Lawyer. July 02, 2025. https://canadacriminallawyer.ca/understanding-the-reasonable-expectation-of-privacy/

[2] In 2022, the Justice Centre funded legal representation for four Canadians who sued the federal government for violating Canadians' *Charter* rights and freedoms through the illegal use of emergency measures. In January 2026, a Federal court upheld the previous ruling that the decision was illegal: https://www.cbc.ca/news/politics/convoy-protest-emergencies-act-appeal-9.7046769

[3] Postmedia News. "Feds admit tracking 33 million mobile phone devices during lockdowns." Toronto Sun. December 21, 2021. https://torontosun.com/news/national/feds-admit-tracking-33-million-mobile-phone-devices-during-lockdowns

[4] Karadeglija, Anja. "Privacy watchdogs call for laws limiting police use of facial recognition." National Post. May 02, 2022. https://nationalpost.com/news/politics/privacy-watchdogs-call-for-laws-limiting-police-use-of-facial-recognition

[5] The full title of Bill C-8 is: "An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts." This report uses only the first portion as an abbreviation: "Bill C-8: An Act respecting cyber security."

[6] Government of Canada. "Charter Statement: Bill C-8." Department of Justice Canada. September 23, 2025. https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c8_2.html

[7] As of February 07, 2026, C-2 remains at second reading, and C-8 in committee after second reading. Source: https://www.parl.ca/legisinfo/en/bill/45-1/c-2 and https://www.parl.ca/legisinfo/en/bill/45-1/c-8

as measures for border security, immigration integrity, and critical infrastructure protection against cyber threats, these bills nevertheless pose serious threats to Canadians' privacy.

Key dangers include:

- **Warrantless access to private information**: Warrantless or suspicion-based access to subscriber information, metadata, communications details, and online activity from a wide array of providers, often with gag orders preventing notification of affected Canadian internet users.
- **Government-forced "deplatforming" and secret data demands**: Secret, binding ministerial orders under C-8 could compel telecoms and critical operators to remove products and access systems from individual Canadians, potentially weakening encryption and disconnecting individuals from the internet without transparency, judicial review, or clear proportionality safeguards.
- **Centralised identity information**: Integration with existing tools – financial surveillance, digital identity frameworks (theoretically interoperable across sectors despite no claimed mandatory adoption), algorithmic risk-scoring,[8] and cash limits – enables a "surveillance web" of total visibility, identity tracking of individuals across time, attributable finances, accessible communications, and deputized private-sector data collection.

These measures suggest that the Government of Canada prefers "safety" and "cohesion" over constitutional rights and freedoms. They normalize oversight of private and confidential information. They reduce functional privacy to offline interactions and cash transactions of less than $10,000. Fully developed, these powers erode privacy and anonymity (considered essential for personal security), autonomy (dissent, free speech, and intellectual exploration), and dignity.

Surveillance infrastructure, once built, rarely contracts. Recent history during the Freedom Convoy shows mission creep from targeted threats to broad domestic control, risking abuse by future governments – especially if already well-developed cross-platform digital identity and digital currency systems become fully adopted.

This report warns of a fundamental reordering of state-citizen relations, akin – in kind, though not yet in degree – to those of authoritarian regimes. Canadians face a red alert: stay informed, resist digital ID/central bank digital currency adoption, demand that Members of Parliament defeat or amend these bills, and defend privacy as the shield of a free people. Failure to act risks permanent loss of the private sphere without which true freedom is quickly extinguished.

---

[8] Government of Canada. "Algorithmic Impact Assessment tool." Government of Canada. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html (Accessed, February 07, 2026)

Introduction

Canadians seemed shocked when, in February 2022, they learned that the *Emergencies Act* allowed the Government of Canada to order financial institutions to freeze bank accounts.[9]

Yet, for thirty years, surveillance technology has developed as Canadians embraced convenient online transactions while rarely considering that all online activity and transactions are recordable.

To think such data would never be accessed by the state was always unrealistic. Not only were accounts frozen without judicial process (or even an opportunity for victims to respond and defend themselves), but banks were compelled to disclose transaction records and sources of funds to the *government*.

With expanded data-sharing now possible between government departments and between government and the private sector, with algorithmic decision-making,[10] and with the legislative normalization of surveillance, Canada has become a developed surveillance state, with weakened privacy and compromised personal freedoms.

As the Supreme Court of Canada warned in 1990, the unchecked power of electronic surveillance could "annihilate any expectation that our communications will remain private."[11]

Today, that applies not only to "our communications" but to financial transactions, cellular location data, online interactions, identity, and personal information.

The Justice Centre and others[12] warned of this.[13] Until now, privacy regulations[14] have

---

[9] Tasker, John Paul. "Banks are moving to freeze accounts linked to convoy protests. Here's what you need to know." CBC News. February 16, 2022. https://www.cbc.ca/news/politics/emergencies-act-banks-ottawa-protests-1.6353968

[10] Government of Canada. "Directive on Automated Decision-Making." Government of Canada. https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592 (Accessed February 07, 2026)

[11] R. v. Duarte, 1990 CanLII 150 (SCC), [1990] 1 SCR 30, https://canlii.ca/t/1fszz, Retrieved on 2026-02-07

[12] Canadian Civil Liberties Association. "CCLA and Coalition of Coalitions call for withdrawal of Bill C-2. July 11, 2025. https://ccla.org/privacy/ccla-joins-calls-for-withdrawal-of-bill-c-2/

[13] Our litigation and research – including challenges to the Emergencies Act financial freezes and Luke Neilson's reports *Digital ID, Surveillance, and the Value of Privacy* (2023)[13] – document how centralized databases, function creep, and eroded consent threaten autonomy.

[14] Government of Canada. "Summary of privacy laws in Canada." Office of the Privacy Commissioner of Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15

limited the sharing of private information between government departments, or forcing private companies to disclose user data. But policies under parliamentary consideration would vastly expand government access to Canadians' private data. Bills C-2[15] (*Strong Borders Act*) and C-8[16] (*An Act respecting cyber security*...)[17] do not merely address discrete threats, as claimed. Passed, they empower governments to conduct warrantless searches of private internet-provider data, monitoring what sites Canadians visit and even their text and email correspondence.

Surveillance capacity, once built, rarely contracts.

These new proposed laws are not a temporary emergency response. They are a structural redirection that prioritizes promised safety and cohesion over actual privacy. Should these Bills pass, functional privacy for Canadians will be a thing of the past.

The emerging surveillance state in Canada

Privacy, a right under attack

Privacy is not secrecy. It is freedom from unjustified surveillance and a person's right and ability to control whether, when, why and with whom personal information is shared or accessed, as well as which information and how much.

Contrary to the popular claim that "those with nothing to hide have nothing to fear," privacy underpins **security** (from malicious actors online, not just from government abuse), **autonomy** (protecting free speech, dissent and intellectual exploration), and **human dignity** itself.[18]

Edward Snowden's[19] observation on this remains apt: arguing against privacy because one has nothing to hide is equivalent to rejecting free speech because one has nothing to say.[20]

---

[15] Government of Canada. "Charter Statement: Bill C-2." Department of Justice Canada. June 19, 2025. https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c2_2.html

[16] Government of Canada. "Charter Statement: Bill C-8." Department of Justice Canada. September 23, 2025. https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c8_2.html

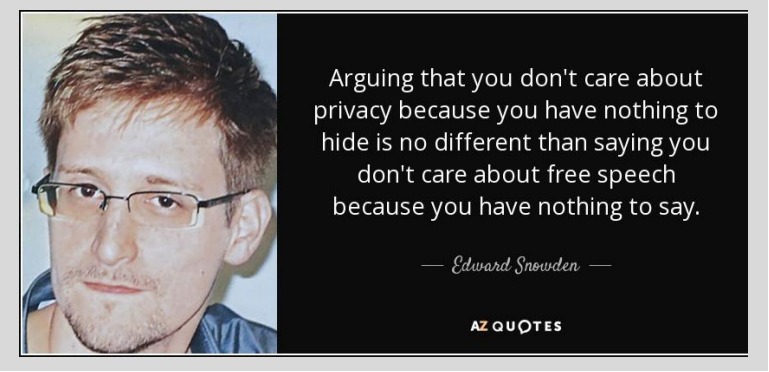
[17] The full title of Bill C-8 is: "An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts." This report uses only the first portion as an abbreviation: "Bill C-8: An Act respecting cyber security."

[18] Neilson, Luke. "Digital ID, Surveillance, and the Value of Privacy." Justice Centre for Constitutional Freedoms. August 09, 2023. https://www.jccf.ca/reports-10/

[19] Wikipedia. "Edward Snowden." https://en.wikipedia.org/wiki/Edward_Snowden (Accessed February 01, 2026)

[20] Goodreads. "Edward Snowden > Quotes > Quotable Quote." https://www.goodreads.com/quotes/7308507-ultimately-arguing-that-you-don-t-care-about-the-right-to.

Rights do not require justification; infringements do.



Unfortunately, the *Canadian Charter of Rights and Freedoms* does not expressly protect "privacy" as such. However, both the *Charter* section 8 protection "unreasonable search or seizure," and section 7 right to "life, liberty and security of the person" have been interpreted by the Supreme Court of Canada to include privacy rights.

Moreover, for more than 150 years of post-Confederation jurisprudence (itself based upon centuries of British Common Law), the Supreme Court of Canada has consistently recognized the principle of the "Reasonable Expectation of Privacy."[21] As such, Canadians had a solid basis to believe and expect that their bank accounts were beyond government scrutiny.

The imperative of anonymity

Privacy, then, has historically been considered essential to personal autonomy and dignity. But what gives privacy and autonomy their force is anonymity.

True privacy – anonymity – means data cannot be traced back to particular individuals.[22] Breaking the link between identity and data can be accomplished by removing personally identifiable information from data sets (or never capturing it in the first place), so that the people to whom the data refers remain anonymous.[23] (Governments, for example, can record and analyze health care data while respecting patient confidentiality.)

Legislative priorities have shifted, however, from preserving anonymity toward the blanket acquisition of personally identifying information. Meanwhile, politicians assure the public that the best safeguard against governments abusing this newfound power is not anonymity but the trustworthiness of governments themselves.

But, the freezing of bank accounts in 2022 proved the GoC cannot be trusted to curtail its worst instincts.

(Accessed February 07, 2026).

[21] Government of Canada. "Section 8 – Search and seizure." Department of Justice Canada. https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art8.html (Accessed February 07, 2026)

[22] Ibid.

[23] Neilson, Luke. "Digital ID, Surveillance, and the Value of Privacy." Justice Centre for Constitutional Freedoms. August 09, 2023. https://www.jccf.ca/reports-10/

Digital ID platforms empower surveillance states

Federal and provincial initiatives increasingly link essential services – banking, travel, benefits, healthcare, and telecommunications – to verified digital identity.

The Government of Canada insists that there's nothing to worry about, that there are no plans to implement a national, mandatory digital identification system, and that no such systems are currently in development.[24] Thus, Ottawa claims it is not phasing out paper or plastic identification; digital versions of existing documents would remain optional, user-controlled, and limited to digital equivalents of what people already carry.

In a narrow sense, this may be so. However, history offers a cautionary example: the Social Insurance Number was introduced in the 1960s for the limited purpose of administering unemployment insurance. Today, however, it is effectively impossible to work, open a bank account, or meaningfully interact with the government without one. This evolved gradually, through subtle policy changes, not sweeping legislation. Unless strongly opposed by Canadians, a similar trajectory is highly likely for digital surveillance.

The greater concern, therefore, is not whether Canadians are handed a mandatory digital ID card or app, but in the underlying existing architecture that potentially enables cross-silo access to all personal identifying information.

Linkage of identity information tends to expand. For example, Canadian development of digital ID began in British Columbia in 2001.[25] Initially linking just health and driver information, the BC Services Card can now be used to log in to more than two dozen discrete government agencies, including the federal government.[26]

However, in 2012, the Digital Identification and Authentication Council of Canada (DIACC)[27] was established to add banks and industry to government, in pursuit of a "one-card-does-it-all" form of digital ID.[28] DIACC's 100+ membership list combines the federal

[24] Written response to question from Conservative MP Marilyn Gladu. https://www.ourcommons.ca/written-questions/45-1/q-537/13856577?showQuestion=true&section=all

[25] https://www.oag.bc.ca/app/uploads/sites/963/2024/08/OAGBC-2010-02-03-bcoag-electronic-health-records-ehr.pdf

[26] https://id.gov.bc.ca/account/services

[27] DIACC, "Written Submission for the 2023 Pre-Budget Consultations." The Digital ID & Authentication Council of Canada (DIACC). October 07, 2022. https://www.ourcommons.ca/Content/Committee/441/FINA/Brief/BR11976963/br-external/DigitalIDAndAuthenticationCouncilOfCanada-e.pdf

[28] The lead agency developing digital ID in Canada is the public-private Digital Identification and Authentication Council of Canada (DIACC). Established in 2012, its purpose is to "develop a Canadian framework for digital identification and authentication." Its stated goal is to provide Canadians with a "robust, secure, scalable, inclusive, and privacy-enhancing digital ecosystem that will allow them to 'securely participate in the global digital economy.'" Certainly, there is enormous momentum toward a global system of personal, digital ID for all people. It is a UN Sustainability goal, a World Economic Forum

and provincial governments with private sector players led by Visa, Mastercard, Interac,[29] the major banks, and Canada's credit unions. Most DIACC members are Canadian, but membership does include non-Canadian entities, such as the Chinese-owned technology group Lenovo.

Since then, both federal and provincial governments have pursued interoperable credentialling systems designed to allow seamless authentication across government departments and private platforms. This health infrastructure already allows (on a voluntary basis) users in Alberta and BC to sign into federal services such as CRA and Service Canada, and provides a model for further cross-silo integration of other government databases through a single access framework and a unique identifier code.

In short, the concern is not the convenience of showing identification on a phone that such a system makes possible. It is the *centralized, interoperable network of personal information* that such a system enables: granting government agents access to linked data across departments and ultimately to private entities.

For now, laws still impose strict limits on how much information government departments may share internally or obtain from the private sector; warrants or other rigorous conditions are generally required to access individual tax records or internet user data. But recent legislative efforts show a clear appetite on the part of politicians and other government officials to widen that access.

Bills such as C-2 and C-8 are indicative. They would expand the government's ability to obtain private information wherever that information resides – often with lowered thresholds or no judicial oversight – particularly in areas touching border security, money laundering, telecommunications, and online activity.

When combined with algorithmic risk scoring, the possibilities grow darker still. Institutions with access to aggregated datasets – governments, banks, credit agencies – can classify individuals as "safe" or "risky" (which amounts to "compliant" or "non-compliant") based on patterns of behaviour. The 2022 invocation of the *Emergencies Act* provided a vivid demonstration: financial surveillance enabled authorities to identify and freeze the accounts of persons of interest with remarkable speed and without traditional judicial process.

---

policy initiative, and it is enthusiastically driven by an alliance of business, government and public advocacy organizations.

[29] In a curious piece of promotion, Interac – a commercial enterprise whose primary purpose is efficient payments between buyer and seller – enthusiastically touts the government uses of digital ID along with its commercial uses.

In short, the government's assurance that no mandatory national digital ID is planned may be technically accurate but deeply disingenuous. The infrastructure for persistent identity tracking is already being assembled, piece by piece, under the banner of interoperability, convenience, and security.

Is a centralized framework coming that allows broad access to linked personal data across government silos and private providers?

The precedents are in place. The technology is capable. The legislative momentum points toward fewer rather than more safeguards. The result, if this trend continues unchecked, is not merely greater administrative efficiency. Rather, it is the steady construction of an architecture of surveillance and control over how Canadians live, work, and speak online.

Bills C-2 and C-8: An authoritarian surveillance combo

Bill C-2 – Warrantless data demands

Ostensibly, Bill C-2 (the *Strong Borders Act*) is to address US-Canada border issues.[30] It does that, especially regarding asylum issues.[31] But it also enlarges the domestic powers of police, intelligence agencies and government to access personal data that may have little relevance to border issues. Law professor Robert Diab[32] observes that Bill C-2 contains "a raft of new search powers completely unrelated to the border. They do more to expand the state's power to access private data in Canada than any law in the past decade."[33]

---

[30] Government of Canada. "Charter Statement: Bill C-2." Department of Justice Canada. June 19, 2025. https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c2_2.html

[31] Borders Law Firm. "Understanding the Strong Borders Act Bill C-2 and Its Implications for Canadian Immigration." June 03, 2025. https://borderslawfirm.com/understanding-the-strong-borders-act-bill-c-2-and-its-implications-for-canadian-immigration/

[32] Robert Diab is a law professor at Thompson Rivers University in Kamloops, B.C.

[33] Diab, Robert. "Buried in a Border Bill, Canada Creates Major New Search Powers Over Private Data." June 13, 2025. https://www.techpolicy.press/buried-in-a-border-bill-canada-creates-major-new-search-powers-over-private-data/

Most importantly, C-2 reduces judicial oversight over government access to personal information, allowing law enforcement to make warrantless data demands from service providers and other government agencies.

Of concern:

- **Warrantless data demands**: Government agencies may demand personal and subscriber data (including data about whom you messaged, when, for how long, and your approximate location) from online service providers and other individuals and organizations that "provide a service to the public." Providers would be required to organise their information for the convenience of law enforcement and may also be gagged from notifying affected individuals.
- **Warrantless postal searches**: Canada Post will have expanded authority to open mail if there is "reasonable suspicion" of contraband or dangerous goods, rather than the higher privacy-protecting standard of "reasonable and probable" grounds.
- **Warrantless data-sharing:** Bill C-2 expands data-sharing between Canadian government agencies and with the U.S. and other countries, potentially undermining established rights under the *Charter* and federal privacy laws.[34]
- **Cash limits:** Bill C-2 limits cash transactions to $10,000, ensuring all transactions above that limit are traceable.

In his reading of the bill, internet lawyer Michael Geist adds,[35]

> *"…the providers who can be targeted with this demand extends far beyond telecom and Internet providers. The information demand power applies literally to anyone who provides services to the public. There is no definition or obvious limitation on the services in question or the person who provides them – it could be a telecom provider, physician, hospital, library, educational institution, or financial institution. It is critical to emphasize that this is not limited to communications services."*

To invoke this power, law enforcement needs only "reasonable grounds to suspect" that an offence has or will be committed. "Offence" is not limited to the *Criminal Code* but covers any Act of Parliament; this extends far beyond criminal investigation.

At the time of writing, Bill C-2 remains at Second Reading in the House of Commons.[36]

---

[34] The Canadian Civil Liberties Association shares our concerns: https://ccla.org/privacy/ccla-joins-calls-for-withdrawal-of-bill-c-2/

[35] Geist, Michael. "Government Doubles Down on Bill C-2's Information Demand Powers." Michael Geist Blog. September 17, 2025. https://www.michaelgeist.ca/2025/09/government-doubles-down-in-defending-bill-c-2s-information-demand-powers-that-open-the-door-to-warrantless-access-of-personal-information/

[36] Government of Canada. Bill C-2: Strong Borders Act. Parliament of Canada. 45th Parliament, 1st session. https://www.parl.ca/LegisInfo/en/bill/45-1/c-2

Bill C-8 – Government-forced "deplatforming"

Bill C-8 (*An Act respecting cyber* security…) complements Bill C-2 by allowing secret government orders to telecoms and critical infrastructure providers. Supposedly, it is about securing critical infrastructure against foreign attacks. Nevertheless, privacy advocates say the Bill's lack of robust safeguards and transparency creates significant risks for Canadians' digital privacy and trust.

Of concern:

- **Government-forced "deplatforming":** Bill C-8 empowers the Minister of Industry to "direct a telecommunications service provider to remove all products provided by a specified person from its telecommunications networks or telecommunications facilities, or any part of those networks or facilities." In other words, to "kick Canadians off the Internet."[37] Those affected would never know why.
- **Secret government directives:** The Government of Canada could issue confidential orders to telecoms and other critical service providers without prior consultation, independent review, or transparency. Such secrecy undermines accountability and could be used to limit personal privacy and digital rights.
- **Warrantless access to personal data:** Bill C-8 would allow governments to compel service providers to allow access to personal data, metadata, and encrypted environments.[38] The Bill could be used to compel operators to weaken or bypass encryption, creating "backdoors" that expose private communications and other sensitive data to government surveillance and cyberattacks.[39]

At the time of writing, Bill C-8 is in Committee, having passed Second Reading in the House of Commons.[40]

---

[37] Hannaford, Nigel. "Death by a thousand clicks: The rise of internet censorship and control in Canada." Justice Centre for Constitutional Freedoms. December 15, 2025. https://www.jccf.ca/wp-content/uploads/2025/12/Death-by-a-thousand-clicks_Final.pdf

[38] Encryption is the process of transforming readable plain text into unreadable ciphertext to mask sensitive information from unauthorized users. Organizations regularly use encryption in data security to protect sensitive data from unauthorized access and data breaches.

[39] Privacy expert Sharon Polsky comments that "Section 20(6) of the CCSP (Critical Cyber Systems Protection) prohibits a designated operator or class of operators from intercepting communications, but third parties that support critical services aren't included. That could easily be operationalized as encryption-busting back doors." Private communications. January 2026.

[40] Government of Canada. Bill C-8: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts. Parliament of Canada. 45th Parliament, 1st session. https://www.parl.ca/LegisInfo/en/bill/45-1/c-8

The resulting dragnet: total surveillance

As detailed above, Bills C-2 and C-8 would result in increased state surveillance powers, including enhanced financial surveillance, and real-time data-sharing obligations imposed on service providers.

The government claims Bill C-8 serves to "modernize" Canada's cybersecurity framework and protect it against threats of "interference, manipulation, disruption or degradation."[41] Yet the contents of Bill C-8, taken together, will create a surveillance web in which:

- Financial activity may be continuously monitored and attributable.
- Communications metadata and online identifiers are readily accessible.
- Private companies are deputized (used) as data collection and compliance agents.
- Judicial oversight is fragmented, delayed, or conducted after the fact.

Combined, then, C-2 and C-8 significantly empower the increasing centralised identity infrastructure discussed above, creating the capacity for a total surveillance. Such a surveillance web would not require the state to engage in constant active surveillance of every Canadian. However, it allows the government at its discretion to see, observe and know more things about our private lives than ever before, and then to selectively exercise this power to target "individuals of interest."

Deterring bad actors: existing tools are sufficient

We are not indifferent to the need to discourage bad actors from using the internet to "interfere with, manipulate, disrupt or degrade" public discourse. Crime prevention, border security, and cybersecurity are important objectives that Canadians should support.

However, the Government of Canada has not shown that current targeted, judicially overseen tools – such as warrants issued under existing laws – fail to effectively address these risks. Nor has it provided evidence to show that the actual benefits of Bills C-2 and C-8 would outweigh the significant harms of mass surveillance.

Instead, together with the halted Bill C-9, these bills signal a nudge[42] toward normalizing surveillance, and the erosion of privacy expectations. The illegal use in 2022 of the *Emergencies Act* illustrates how extraordinary surveillance powers can be deployed swiftly

[41] Government of Canada. "Charter Statement: Bill C-8." Department of Justice Canada. September 23, 2025. https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c8_2.html

[42] Justice Centre for Constitutional Freedoms. "New report warns Ottawa's 'nudge' unit erodes democracy and public trust." News Release. November 17, 2025. https://www.jccf.ca/new-report-warns-ottawas-nudge-unit-erodes-democracy-and-public-trust/

and broadly. Bills C-2 and C-8, as written, simply expand and make government surveillance powers permanent.

In her remarks to the Standing House Committee on Public Safety and National Security during its study of Bill C-8,[43] Sharon Polsky, President of the Privacy and Access Council of Canada, emphasized how the government's strategy reduced protections in Canada:

> *"The preamble says that this bill is to protect telco providers and critical systems, and provides the Minister with sweeping powers to order them to 'do anything, or refrain from doing anything' to protect the Canadian telco system. [s15.2(2)] But it lacks safeguards to prevent abuse or ideological attack."*

The intent seems clear: encourage citizen compliance and acceptance of a persistent state presence, while eroding traditional expectations of privacy.

The precedents are worrying: the Government of Canada's use of the *Emergencies Act* in 2022 showed how the state can and will use extraordinary powers immediately and with little warning, even without necessity. Bills C-2 and C-8 would now extend authority far beyond border integrity or cyber defence, to create a general-purpose surveillance capacity.

Will Canadians retain any privacy?

Bills C-2 and C-8 are not isolated statutes. Alongside digital ID frameworks, limits on cash, financial surveillance, and cyber-security authorities, they form an integrated architecture of visibility and control. Indeed, working together, they become force multipliers: C-2 broadens who can be compelled to provide personal data and for what purposes, while C-8 enlarges the government's ability to reach deeply into the technical systems that hold and transmit that data.

Should these two bills pass, privacy for Canadians would persist only at the margins: thoughts, beliefs and offline interactions not translated into digital form; cash transactions under $10,000 (for as long as cash lasts); and those activities conducted outside regulated platforms and networks, which have become increasingly rare over the last ten years.[44]

That is, if C-2 and C-8 pass, actual privacy on a practical level – the ability to live digitally,

---

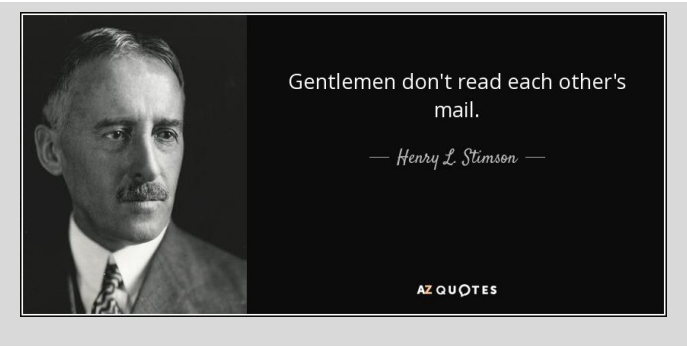
[43] Polsky, Sharon. "Evidence," Standing Committee on Public Safety and National Security, Number 010, 1st Session, 45th Parliament, House of Commons. https://www.ourcommons.ca/DocumentViewer/en/45-1/SECU/meeting-10/evidence

[44] Even trying to rent a car or a hotel room is all but impossible without a credit card. For practical purposes, Canada's economy is fully digitized.

transact economically, and communicate socially without creating a permanent, linkable record accessible to the state – would be a thing of the past.

The core problem is not a single law or intention, but the design of an entire system. Notwithstanding the Government of Canada's repudiation of any designs upon a digital ID, the work that has already been done on integrating identity, financial data, and communications under interoperable legal and technical frameworks has produced an infrastructure of total visibility and control, where restraint depends less on hard limits than on trust in future governments.

To this, the Government of Canada would now add the examination of Canadians' emails.



Of course, if privacy were left to statesmen like U.S. Secretary of State Henry L. Stimson — who famously closed the U.S. Cipher Bureau (which read secret correspondence between officials) in 1929 with the remark, "Gentlemen don't read each other's mail"[45] — perhaps confidence would be warranted.

But there is little evidence of Stimsonian restraint in the Government of Canada or its bureaucratic enablers.

Whether this network is ultimately used sparingly or expansively, the capacity itself marks a fundamental shift in the relationship between Canadians and the state. In regard to the technological capacity enabled by Bills C-2 and C-8, the relationship between Canadians and their government will differ little from the relationship between the People's Republic of China and its citizens, except that Ottawa might be less ruthless and aggressive than Beijing.[46]

[45] Zablocki, Peter. "The Spy Who Exposed the Secrets of the Black Chamber, One of America's First Code-Breaking Organizations." Smithsonian Magazine. February 4, 2025. https://www.smithsonianmag.com/history/the-spy-who-exposed-the-secrets-of-the-black-chamber-one-of-americas-first-code-breaking-organizations-180985947/

[46] Justice Centre for Constitutional Freedoms. "Canada's Road to Beijing: The digital threat to the Charter rights and freedoms of Canadians." A Justice Centre Report. August 10, 2022. https://www.jccf.ca/wp-content/uploads/2022/08/Canadas-Road-to-Beijing_FINAL.pdf

Conclusion

Privacy must be protected, and state surveillance power strictly limited

To the government official, information is power, as information is power for corporations and individuals. For politicians and bureaucrats, the relentless accumulation of data – regardless of need — becomes both a professional imperative and, too often, an end in itself. Yet unchecked surveillance carries grave dangers: it tempts abuse, is vulnerable to catastrophic breaches,[47] and chills dissent before it even forms. Tools introduced for one crisis rarely vanish; they metastasize, creeping from terrorism to protest monitoring, from border security to keeping Canadians "safe" from the "wrong" opinions.

Bills C-2 and C-8 are not mere technical improvements to the status quo. Together with financial tracking, cash limits, paused-but-ready digital ID frameworks, and cybersecurity pretexts, they reveal a deliberate architecture for governments to see, monitor and control what Canadians think and say; how and where they spend their money; with whom they connect online and in person; and how they live their lives.

Neither Bill has been justified by compelling evidence as to what, specifically, is lacking in current laws. Neither Bill provides meaningful safeguards against retaliation, coercion, or mission creep. Neither demands transparent review, robust judicial oversight, or strict proportionality. Both invite executive overreach. Both erode the anonymity that makes true liberty possible.

Surveillance capacity, once constructed, almost never shrinks. The question is not *if* these powers will be misused, but *when*.

Privacy, free expression, and freedom in all its dimensions are inseparable. They are the very foundations of a self-governing people. Yet today, they are under sustained assault by an expanding surveillance web that Bills C-2 and C-8 seek to entrench and accelerate.

In the face of such serious threats, Canadians must choose: submission to a state that knows all, or resolute defence of the private sphere where dignity, autonomy, and dissent can breathe. Functional privacy – the ability to live, transact, and speak digitally without forging a permanent, state-accessible chain of records – hangs by a thread. If we allow it to snap, what remains will be the illusion of freedom in a glass house - every move observed, every thought potentially criminalized.

---

[47] Amishav, Josh. "Data Breach Examples: The Biggest Security Incidents." Breach Sense. February 02, 2026. https://www.breachsense.com/blog/data-breach-examples/

This is no time for complacency. The Justice Centre has fought – and will continue to fight – through litigation, research, and unyielding advocacy to expose and halt this drift toward control.

But the battle can only be won through the active engagement of every Canadian. Canadians should:

- Take notice and inform themselves about how their data is harvested, stored, and weaponized.
- Resist the seductive pressure to adopt digital ID, central bank digital currencies, or any system that trades anonymity for convenience.
- Use emails, phone calls, and petitions to demand that their Members of Parliament vote against Bills C-2 and C-8.
- Inform their friends, family, neighbours, and colleagues about the dangers of Bills C-2 and C-8.
- Donate to the Justice Centre and other civil liberties groups that oppose the surveillance state.

Canada was built on the promise that the state serves the citizen, not the reverse — that liberty is not granted by government but that it must be fiercely defended against government. Our forebears rejected tyranny in the name of self-determination. Today, the tyranny wears subtler clothes: the promises of safety, security and convenience. We must reject it with the same unyielding spirit.

It is not too late. Canadians have awakened before to threats against their freedoms. We can – and we must – do so again. For our children, for our dignity, for the Canada in which we still believe: let this generation draw the line. Privacy is not a relic, but the shield of a free people.

Bibliography

Authier, Philip. “Quebec wants to give each citizen a digital profile to fight identity theft.” Montreal Gazette. December 11, 2019. https://montrealgazette.com/news/quebec/quebec-wants-to-give-citizens-a-digital-identity-to-block-identity-theft

Blake, Austin. “‘Not Implementing’: Ottawa Shuts Down Mandatory National Digital ID Rumours.” iPhone in Canada. https://www.iphoneincanada.ca/2026/01/29/not-implementing-ottawa-shuts-down-mandatory-national-digital-id-rumours/. (Accessed February 07, 2026.)

Borders Law Firm. “Understanding the Strong Borders Act Bill C-2 and Its Implications for Canadian Immigration.” June 03, 2025. https://borderslawfirm.com/understanding-the-strong-borders-act-bill-c-2-and-its-implications-for-canadian-immigration/

Canada. Sessional Paper Response to Question 537: No Plans for National Digital ID. House of Commons. January 26, 2026. https://www.ourcommons.ca/written-questions/45-1/q-537/13856577?showQuestion=true&section=all

Canadian Bankers Association. “White Paper: Canada’s Digital ID Future - A Federated Approach.” Research and Advocacy. May 30, 2018. https://web.archive.org/web/20220301171152/https://cba.ca/embracing-digital-id-in-canada

Curry, Bill. “Ottawa turns to consulting firm McKinsey to fix Phoenix pay system, doubling spending on outsourcing.” The Globe and Mail. January 18, 2022. https://www.theglobeandmail.com/politics/article-ottawa-turns-to-mckinsey-to-fix-phoenix-doubling-spending/

Davidson, Sean. “Ontario government won't comment on progress of digital ID program.” CTV News. April 07, 2022. https://toronto.ctvnews.ca/ontario-government-won-t-comment-on-progress-of-digital-id-program-1.5852732

Diab, Robert. “Buried in a Border Bill, Canada Creates Major New Search Powers Over Private Data.” June 13, 2025. https://www.techpolicy.press/buried-in-a-border-bill-canada-creates-major-new-search-powers-over-private-data/

Digital ID and Authentication Council of Canada (DIACC). “Digital Trust for the Economy.” https://diacc.ca/the-diacc/

Digital ID and Authentication Council of Canada (DIACC). “Trust Framework.” https://diacc.ca/trust-framework/

Geist, Michael. “Government Doubles Down on Bill C-2's Information Demand Powers.” Michael Geist Blog. September 17, 2025. https://www.michaelgeist.ca/2025/09/government-doubles-down-in-defending-bill-c-2s-information-demand-powers-that-open-the-door-to-warrantless-access-of-personal-information/

Goodreads. “Edward Snowden > Quotes > Quotable Quote.” https://www.goodreads.com/quotes/7308507-ultimately-arguing-that-you-don-t-care-about-the-right-to. (Accessed February 07, 2026).

Government of Canada. “Algorithmic Impact Assessment tool.” Government of Canada. https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html (Accessed, February 07, 2026)

Government of Canada. “Charter Statement: Bill C-2.” Department of Justice Canada. June 19, 2025. https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c2_2.html

Government of Canada. “Charter Statement: Bill C-8.” Department of Justice Canada. September 23, 2025. https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c8_2.html

Government of Canada. “Directive on Automated Decision-Making.” Government of Canada. https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592 (Accessed February 07, 2026)

Government of Canada. “Evaluation of the Canadian Digital Service.” The Treasury Board of Canada Secretariat (TBS). https://www.canada.ca/en/treasury-board-secretariat/corporate/reports/evaluation-canadian-digital-service.html

Government of Canada. “Government of Canada Digital Identity (ID).” The Treasury Board of Canada Secretariat (TBS). August 08, 2020. https://canada-ca.github.io/PCTF-CCP/docs/2020-08-08%20Digital-ID-General-with-CIOSC-Standard-Draft%20(EN).pdf

Government of Canada. “Section 8 – Search and seizure.” Department of Justice Canada. https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art8.html (Accessed February 07, 2026)

Government of Canada. “The Personal Information Protection and Electronic Documents Act (PIPEDA).” Office of the Privacy Commissioner Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Government of Canada. “The Privacy Act.” Office of the Privacy Commissioner Canada. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-privacy-act/

Government of Canada. Bill C-2: Strong Borders Act. Parliament of Canada. 45th Parliament, 1st session. https://www.parl.ca/LegisInfo/en/bill/45-1/c-2

Government of Canada. Bill C-8: An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts. Parliament of Canada. 45th Parliament, 1st session. https://www.parl.ca/LegisInfo/en/bill/45-1/c-8

Hannaford, Nigel. “Death by a thousand clicks: The rise of internet censorship and control in Canada.” Justice Centre for Constitutional Freedoms. December 15, 2025. Death-by-a-thousand-clicks_Final.pdf

Interac Canada. “How will my digital ID shape the future of digital government in Canada?.” May 30, 2025. https://www.interac.ca/en/content/ideas/how-will-digital-identity-will-shape-the-future-of-canada/

Investopedia. “Open Banking: Definition, How It Works, and Risks.” The Investopedia Team. August 02, 2025. https://www.investopedia.com/terms/o/open-banking.asp (Accessed February 01, 2026)

Justice Centre for Constitutional Freedoms. “Canada’s Road to Beijing: The digital threat to the Charter rights and freedoms of Canadians.” A Justice Centre Report. August 10, 2022.https://www.jccf.ca/wp-content/uploads/2022/08/Canadas-Road-to-Beijing_FINAL.pdf

Justice Centre for Constitutional Freedoms. “New report warns Ottawa’s ‘nudge’ unit erodes democracy and public trust.” News Release. November 17, 2025. https://www.jccf.ca/new-report-warns-ottawas-nudge-unit-erodes-democracy-and-public-trust/

Karadeglija, Anja. “Privacy watchdogs call for laws limiting police use of facial recognition.” National Post. May 02, 2022. https://nationalpost.com/news/politics/privacy-watchdogs-call-for-laws-limiting-police-

use-of-facial-recognition

Legislative Assembly of Ontario. “Section 4.09, 2015 Annual Report of the Auditor General of Ontario.” Standing Committee on Public Accounts. Service Ontario. 1st Session, 41st Parliament. https://www.ola.org/sites/default/files/node-files/committee/report/pdf/2016/2016-06/report-1-EN-41_1_PAC_ServiceOntario_07062016_en.pdf

Mantyka, Wayne. “Plan to introduce digital identification system in Sask. put on hold.” CTV News. April 04, 2022. https://regina.ctvnews.ca/plan-to-introduce-digital-identification-system-in-sask-put-on-hold-1.5846948

Neilson, Luke. “Digital ID, Surveillance, and the Value of Privacy.” Justice Centre for Constitutional Freedoms. August 09, 2023. https://www.jccf.ca/wp-content/uploads/2023/04/Digital-ID-Surveillance-and-the-Value-of-Privacy_Justice-Centre-for-Constitutional-Freedoms.pdf

Nick. “Understanding the Reasonable Expectation of Privacy in Canadian Criminal Law.” Canadian Criminal Lawyer. July 02, 2025. https://canadacriminallawyer.ca/understanding-the-reasonable-expectation-of-privacy/

Pilon, Marilyn. “Search, Seizure, Arrest and Detention Under the Charter.” Government of Canada. February 15, 2000. https://publications.gc.ca/Collection-R/LoPBdP/CIR/917-e.htm

Polsky, Sharon. “Evidence,” Standing Committee on Public Safety and National Security, Number 010, 1st Session, 45th Parliament, House of Commons. https://www.ourcommons.ca/DocumentViewer/en/45-1/SECU/meeting-10/evidence

Postmedia News. “Feds admit tracking 33 million mobile phone devices during lockdowns.” Toronto Sun. December 21, 2021. https://torontosun.com/news/national/feds-admit-tracking-33-million-mobile-phone-devices-during-lockdowns

R. v. Duarte, 1990 CanLII 150 (SCC), [1990] 1 SCR 30, https://canlii.ca/t/1fszz, Retrieved on 2026-02-07

Statista. “Number of licensed drivers in Canada from 1994 to 2018.” https://www.statista.com/statistics/448557/number-of-licensed-drivers-in-canada/ (Accessed February 07, 2026)

Tasker, John Paul. “Banks are moving to freeze accounts linked to convoy protests. Here's what you need to know.” CBC News. February 16, 2022. https://www.cbc.ca/news/politics/emergencies-act-banks-ottawa-protests-1.6353968

United Nations. “Transforming our world: the 2030 Agenda for Sustainable Development.” Department of Economic and Social Affairs. Sustainable Development. https://sdgs.un.org/2030agenda (16.9)

United Nations. United Nations Legal Identity Agenda. SDG Goal 16.9. https://unstats.un.org/legal-identity-agenda/

White, Olivia; Anu Madgavkar, James Manyika, et al. “Digital identification: A key to inclusive growth.” McKinsey & Company. Report. April 17, 2019. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.

Wikipedia. “Edward Snowden.” https://en.wikipedia.org/wiki/Edward_Snowden (Accessed February 01, 2026)

World Economic Forum. Digital Identity Agenda. 2021. https://www.weforum.org/agenda/archive/digital-identity; https://www.weforum.org/impact/tackling-digital-deserts-the-first-cross-sector-alliance-to-close-the-digital-gap-launches-at-the-davos-agenda. *Inter alia*.

Zablocki, Peter. "The Spy Who Exposed the Secrets of the Black Chamber, One of America's First Code-Breaking Organizations." Smithsonian Magazine. February 4, 2025. https://www.smithsonianmag.com/history/the-spy-who-exposed-the-secrets-of-the-black-chamber-one-of-americas-first-code-breaking-organizations-180985947/