

| What is Bill C-2?

Bill C-2, known as “Strong Borders Act”, is a wide-ranging proposal that imposes severe limitations on access to refugee claims while expanding surveillance and information-sharing capabilities.

Presented as one component of a broader “strong borders” response to trade pressures and discredited claims of criminals and drugs flowing across the U.S. border, the Bill poses a significant threat to privacy rights, while doing nothing to address Canada’s outdated and inadequate framework for privacy protection.

This explainer outlines how Bill C-2 will expand information sharing between Canada and the U.S. and some of the implications of this expansion. Additional resources on Bill C-2’s privacy implications and its erosion of refugee rights can be found below.

| How is information currently shared with the United States

Canada already shares significant volumes of information with the United States through shared databases, in agency-to-agency exchanges, by automated querying, on a per request basis, and by other means. In some contexts, what information is shared will be based on political priorities set by the Canadian government or our international partners including the United States.

The United States constitutional right to privacy does not apply to Canadians and other foreigners who are outside the United States. Other key protections such as the Privacy Act have limited application, and Canada has been excluded from efforts to extend privacy rights to foreigners. As a result, once Canada shares information with the United States, people in Canada have limited ability to challenge or seek redress for privacy violations.

| Consequences of information-sharing with the United States

Aggressive information-sharing with the United States can have severe consequences for Canadians.

The historical inclusion of sensitive mental health information in shared Canadian police databases, for example, has led to denial of entry at the U.S. border. Visitors to the U.S. are now subjected to vetting by foreign intelligence agencies that receive information from their Canadian counterparts while the list of reasons for turning people away—or even detaining them—at the border has grown to include political dissent, political views or any criticism of the U.S. government.

Information-sharing with the United States can also lead to placement on TIDE, a U.S. database of over 2.5 million people designated as alleged terrorists that is shared widely within the U.S. and Canada. Inclusion in TIDE and the array of watchlists and screening mechanisms it populates has been fraught with errors that are racially and ethnically disproportionate, includes large numbers of people with no suspected terrorist affiliation, and has been used to coerce innocent people into cooperating with U.S. security agencies. Inclusion in TIDE and its subsidiary lists can lead to travel restrictions (including placement on the infamous no-fly list), academic or professional consequences, and enhanced surveillance.

Two separate independent inquiries have concluded that unrestrained information sharing with the United States contributed to, and even caused, the illegal detention and torture of Canadians based on inaccurate information. Over a decade later, the government has yet to fully address the failings that resulted in these miscarriages of justice for Maher Arar, Abdullah Almalki, and others, making expanded information-sharing a cause for ongoing concern.

| Bill C-2 paves the way for expanded information-sharing with the United States

Once Bill C-2 becomes law, Canada will be able to adopt international agreements that expand information-sharing with the United States.

Under one of these agreements (the Second Additional Protocol to the Budapest Convention or “2AP”), U.S. demands for sensitive identification data and metadata could become binding if approved by a Canadian court. The information demands would need to meet some Canadian standards, but not all, and key safeguards intended to protect against self-incrimination under Canadian law are excluded. Canada and the United States have both signed but not yet adopted the 2AP. Canadian government officials have stated that part of Bill C-2 is intended to meet Canada’s obligations under the 2AP so that it can be adopted.

Canada has also been negotiating a second information-sharing agreement with the United States since 2022 under a U.S. legislative framework called the CLOUD Act. The contents of this agreement are not known, but Canadian government officials have indicated that elements of Bill C-2 are designed to align Canadian surveillance practices with U.S. practice, despite fundamental differences in our constitutional privacy protections and standards. CLOUD Act agreements with other countries have expanded information-sharing while failing to provide any enforceable privacy rights to impacted people.

Both of these agreements allow Canada to share information with the United States even if the conduct being investigated is not criminalized in Canada. While Canada can still refuse to cooperate in some contexts, the risk that Canada will become complicit in problematic U.S. investigations is growing as the human rights gap between Canada and the United States widens and the U.S. criminalizes conduct such as exercising one’s right to reproductive health or generally disagreeing with the government.

| Information-sharing grows while safeguards lag

Canada has expanded its information-sharing with the United States and other countries multiple times in recent years, while its cross-border safeguards and privacy protections remain significantly outdated.

Since late 2024, when border control-related trade concerns were first raised by the United States, Canada has significantly increased information-sharing already by expanding a surveillance, profiling and automated information sharing program to include permanent residents and by granting the Communications Security Establishment (Canada’s global intelligence agency) an expanded cross-border drug enforcement mandate.

Canada’s framework for privacy protection was first introduced in 1974 and has not been meaningfully updated since. It does not offer an adequate level of privacy protection, and by extension undermines the ability of people in Canada to ensure that personal information is only shared with the United States if appropriate protections are in place.

A Canadian legislative framework for processing international information-sharing agreements is equally outdated. It fails to prohibit information sharing for investigations that are politically motivated or where the conduct being investigated by the foreign government in question is not criminalized in Canada. Canada has also failed to take adequate steps to fully ensure that its information-sharing with foreign governments does not facilitate torture or mistreatment.

| What can I do?

You can call on your MP to withdraw Bill C-2 using the following tools:

<https://action.openmedia.org/page/173242/action/1>

<https://iclmg.ca/stop-bill-c-2/>

<https://ccrweb.ca/en/take-action-write-mp-bill-c-2>

<https://migrantrights.ca/actionslist/stopc2/>

<https://www.ourcommons.ca/petitions/en/Petition/Details?Petition=e-6838>

| Learn More

Other information resources: <https://ccla.org/privacy/bill-c-2-information-resources/>

Canadian Council of Refugees, Bill C-2 Advocacy Messaging Guide, https://ccrweb.ca/sites/ccrweb.ca/files/2025-08/Bill-C2-Key-Concerns_0.pdf

Coalition of Coalitions call for withdrawal of Bill C-2, July 11, 2025, CCLA, <https://ccla.org/privacy/ccla-joins-calls-for-withdrawal-of-bill-c-2/>

Kate Robertson, Unspoken Implications, June 16, 2025, *The Citizen Lab*, <https://citizenlab.ca/2025/06/a-preliminary-analysis-of-bill-c-2/>

Cynthia Khoo & Kate Robertson, “Canada-US Cross-Border Surveillance Negotiations Raise Constitutional and Human Rights Whirlwind under US CLOUD Act”, February 24, 2025, *The Citizen Lab*, <https://citizenlab.ca/2025/02/canada-us-cross-border-surveillance-cloud-act/>

Open Letter: Canada Must Not Adopt UN Cybercrime Convention, December 12, 2024, <https://openmedia.org/press/item/canada-must-not-adopt-un-cybersecurity-convention>

International Civil Liberties Monitoring Group, Brief on Bill C-59, May 2019, <https://iclmg.ca/wp-content/uploads/2019/05/C-59-brief-May-2019-update.pdf>

Library of Parliament, Legislative Summary – Preliminary Version, Bill C-2, June 19, 2025, https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/LegislativeSummaries/PDF/45-1/PV_45-1-C2-E.pdf

Bill Robinson, “A Look at CSE’s Annual Report 2024-2025”, *Lux Ex Umbra*, July 30, 2025, https://luxexumbra.blogspot.com/2025/07/#Canadian_SIGINT_clients_up_41%

LawBytes Podcast, “Bill C-2’s Cross-Border Data Sharing Privacy Risks”, October 6, 2025, <https://www.michaelgeist.ca/podcast/episode-245-kate-robertson-on-bill-c-2s-cross-border-data-sharing-privacy-risks/>

Secure Line Podcast, “Backdoors, Borders, and Bill C-2”, September 22, 2025, <https://podcasts.apple.com/us/podcast/backdoors-borders-and-bill-c-2/id1791171013?i=1000727886529>

Robert Diab, Bill C-2 Background: New Search Powers and Their Charter Compliance, (2025) 73(3) *Crim Law Q* forthcoming, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5363319

Jenna Fung, Bill C-2 FAQ, August 12, 2025, *OpenMedia*, <https://openmedia.org/article/item/bill-c-2-faq-explaining-canadas-dangerous-new-surveillance-law>

Recommendations Arising from the Iacobucci and O’Connor Inquiries, June 2009, <https://www.ourcommons.ca/Content/Committee/402/SECU/Reports/RP4004074/securp03/securp03-e.pdf>