

---

---

**BRIEF ON BILL C-21:  
AN ACT TO AMEND THE CUSTOMS ACT**

---

---

**By:**  
International Civil Liberties Monitoring Group (ICLMG)

**Presented to:**  
The House Standing Committee on Public Safety and National Security  
October 18, 2017

## About the authors

---

### **The International Civil Liberties Monitoring Group (ICLMG)**

The ICLMG is a national coalition of Canadian civil society organizations that was established in the aftermath of the September 2001 terrorist attacks in the United States. The coalition brings together some 43 NGOs, unions, professional associations, faith groups, environmental organizations, human rights and civil liberties advocates, as well as groups representing immigrant and refugee communities in Canada.

In the context of the so-called ‘war on terror’, the mandate of the ICLMG is to defend the civil liberties and human rights set out in the Canadian Charter of Rights and Freedoms, federal and provincial laws (such as the Canadian Bill of Rights, the Canadian Human Rights Act, provincial charters of human rights or privacy legislation), and international human rights instruments (such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment).

Since its inception, ICLMG has served as a round-table for strategic exchange – including international and North/South exchange – among organizations and communities affected by the application, internationally, of new national security (“anti-terrorist”) laws. ICLMG has provided a forum for reflection, joint analysis and cooperative action in response to Canada’s own anti-terrorist measures and their effects, and the risk to persons and groups flowing from the burgeoning national security state and its obsession with the control and movement of people.

Finally, further to its mandate, the ICLMG has intervened in individual cases where there have been allegations of serious violation of civil liberties and human rights. The ICLMG has also intervened to contest proposed legislation, regulations and practices that contravene the Canadian Constitution, other Canadian laws and international human rights standards.

## **Introduction**

Since our founding, the International Civil Liberties Monitoring Group (ICLMG) has paid particular attention to the impacts that increasing border security can have on Canadians' rights and freedoms, including around privacy rights and the right to movement.

We therefore welcome the opportunity to submit our comments to the House Standing Committee on Public Safety and National Security for your study of Bill C-21, *An Act to amend the Customs Act*.

Over the past 15 years, the ICLMG has been critical of proposals that further integrate Canadian border security with United States border security, which has been a near constant project since Sept. 11, 2001, regardless of changes in government in the United States and Canada.

While we are not opposed to cooperation on security, we remain concerned over the harmonization of Canadian border and security regulations with the United States. In particular, we believe that such harmonization undermines Canada's ability to set security policies according to Canadians' priorities and concerns, and to adequately protect Canadians' civil liberties as set out by the Charter of Rights and Freedoms.

We expressed such concerns as new agreements were proposed and developed post-Sept. 11, 2001, including the 2001 "smart border" agreement, the proposed 2008 Security and Prosperity Partnership, and the 2011 Beyond the Border agreement.

The concerns have not been unfounded, as we have seen instances of security and border agreements that either follow the US' lead and/or are negotiated with little public input or debate. This includes, for example, the US-Canada preclearance agreement currently being implemented through the proposed Bill C-23, and the ill-fated Security and Prosperity Partnership.

Bill C-21, while also responding to some domestic concerns, flows directly from the Beyond the Border agreement and must be seen in that context.

The bill must also be considered in the context of Canada's ever growing information collecting and sharing regimes, both domestically and internationally. The Canadian government now collects more data on its residents than ever before, both for social policy and for security purposes, and participates in unprecedented international intelligence sharing partnerships, such as the Five Eyes alliance. Without even making passing a judgement on the effectiveness and integrity of these programs, such expansions automatically bring greater concerns about ensuring stronger privacy protections.

Therefore, while Bill C-21 is at first glance a straightforward bill, the issues involved becomes more complex when examined in the context of increasing surveillance, data retention and sharing, and the use of this data to analyse and identify security threats.

## **1. Type of data collected**

The government has stated on multiple occasions that the data to be collected will consist of the information on the second page of a person's passport: name, date of birth, nationality, sex, kind of document, issuing country and travel document number. However, the data collected will go further to include the location and date of departure, and for those travelling on a "prescribed conveyance" any identifying number issued to that passenger.

This kind of data, tying a person and their personal identifying documents to their movement across borders, can paint a very specific and revealing portrait, especially if and when it is combined with other information collected by government agencies (employment records, health records, government benefits, etc). While it is important to not be alarmist, it is also important to point out that the information collected is potentially significant, necessitating strong safeguards and clear regulations on its collection, sharing/disclosure, retention and eventual use.

We would also underline the necessity to consider how exit data collection, once enacted in law, could eventually be expanded. We have seen how, over time, data collection regimes that start as limited gradually grow, either through "operational creep" outside the law or through additional legislation that simply "expands" on rules already there. An example would be CSIS expanding its data retention to include "uncollected" or "incidental" data not directly related to a particular national security threat, found illegal by the courts and which will possibly be legalized through Bill C-59.

If we begin collecting exit data, it will be incredibly important to ensure that the information collected, and how it is used, remains strictly controlled and that any change in kind or amount of data collected is scrutinized and only authorized through legislation. This warning is not to guard against a mysterious, unpredictable future. Rather, since there is the real possibility that as both Canada and the United States use more biometric technology – including facial recognition and fingerprinting – in border and travel controls, that there will be a push to include such information in the exit data collected and retained by the government. The collection, retention and sharing of biometric information obviously pose significant challenges and concerns from a privacy and civil liberties stand-point, and we believe it is important to look not just at the immediate use and purpose of laws, but at trends that are developing that will raise future concerns.

As it stands, we are reassured by the fact that any change in the type and amount of data collected upon exit from Canada can solely be modified through future

amendments to the legislation, but remain wary of the path that we are heading along.

## **2. Collection process and regulations**

Discussions on C-21, including at committee, have pointed to a lack of clarity around how exit data collection will actually operate. However, from our understanding there will be two methods.

First, for individuals leaving the country by land, data would be collected by US border agents, who will then share the information with the Canadian Border Services Agency (CBSA). In that sense, CBSA will in fact be “collecting” the data from the US border service, and not directly from individuals. This raises questions of ensuring accuracy of the information gathered by US officers, as well as privacy protections for the information as it is being sent to the CBSA. (We are aware that this system has been tested with data on foreign nationals and permanent residents, and that privacy impact assessments – PIAs – have been undertaken as well.)

Second, for individuals traveling by other means of transport in a “prescribed conveyance” – by plane, for example – it will be up to a “prescribed person” to provide the information directly to the CBSA. However, it is not clear in the legislation what will be included as a prescribed conveyance: will trains be included? Water transport? Buses? This is not an insignificant question, as it raises concerns regarding who will be handling this sensitive information, and how it will be transmitted to the CBSA.

This confusion comes from what we perceive as a flaw in the bill: As others have also pointed out, both sections 92 and 93 leave much to be decided by regulations that will be prescribed by the Governor in Council. The resulting vagueness of the bill makes it difficult to judge the processes that will take place and the information that will be dealt with, as well as the appropriate safeguards that may be necessary.

Our preference would be that the committee and/or the government bring greater precision to the bill before it is passed. However, at a minimum we would request that a statute be included stating that any regulation set by the Governor in Council regarding data collection, sharing/disclosure or retention, must undergo a PIA, which would allow for vetting and reporting by the Privacy Commissioner.

## **3. Privacy and National Security**

The government has stated that its objectives for collecting exit data are national security, law enforcement and fraud prevention. While we recognize that there are valid concerns regarding the latter issue, we will focus on the first two.

We are concerned that there are no explicit protections in the law regarding how the information collected may be used or the amount of time that such information may be retained.

As the Privacy Commissioner has already pointed out in annual reports, Canadians expect that information collected by the government be used for the specific purpose for which it was collected. Along with that, we would add that Canadians have a reasonable expectation that once the information is used for that purpose, it would be destroyed.

We would therefore suggest that two clauses be added:

- a) Detailing how the information collected will be used and/or shared
- b) Setting a time limit on the CBSA's retention of all non-actionable data

On the latter, there have been media reports that CBSA has agreed to a retention period of 15 years. While this has not been officially confirmed, it does appear from committee testimony that this limit was agreed upon through consultation with the Privacy Commissioner. For clarity and scrutiny, the reasoning for the 15 year limit should be shared publicly, and the limit explicitly included in the legislation.

On the former, clear delineations on the use and/or sharing of the exit data collected would be important to prevent national security over-reach. For example, there are ongoing and legitimate concerns that this type of data could be added in bulk to CSIS datasets. The result would be a massive archive of the travels of innocent Canadians who should have a reasonable expectation that such information is not being retained by the government unless it is related to an actual national security investigation.

This also raises questions under Security of Canada Information Sharing Act and the newly proposed Security of Canada Information Disclosure Act: an individual suspected of the vague and overly-broad status of "undermining national security" could see their information share by the CBSA with CSIS, the RCMP or other agencies without having been suspected of (or having committed) a crime.

It is also well known that the Canadian government shares intelligence with other jurisdictions, including its Five Eyes partners. We are concerned that Canadians' travel information – either individually or in bulk – will be shared with foreign intelligence agencies who can then use the information as they wish. This includes (despite attempts to seek assurances) the potential further sharing of this information with other governments or agencies. Such information sharing is at the heart of the cases of people like Mr. Almalki, Mr. Elmaati and Mr. Nurreddin, who suffered unjust imprisonment and torture abroad.

Finally, while we will address redress later, we would also recommend that the bill should explicitly state that the CBSA is responsible for the accuracy of exit data collected. If this information will be used for sensitive national security activities, it

is important that a centralized, Canadian agency take responsibility for its accuracy, and the CBSA would be most clearly suited to play that role.

#### **4. Law Enforcement**

While law enforcement is not limited to national security concerns, it is closely related. After reading the bill and consulting testimony to the committee from other witnesses, we would encourage the Committee to seek out more details on how exit data would be used in urgent law enforcement cases, for two reasons.

First, the government has stated that exit data collection will aid in real-time law enforcement, for example in the case of an Amber Alert or in stopping a person suspected of posing a national security threat from leaving the country. However, experts have testified that the data collection does not occur in real-time: there is a minimum delay of 15 minutes between the information being shared at the border with US officials and it being transmitted to CBSA. This would make it impossible for CBSA or Canadian law enforcement to take action, or even share the information back to US border agents, before a suspected individual crosses the border and, potentially, disappears. We are therefore curious as to how real-time law enforcement would prove a strong justification for exit data collection (especially since it has been central to government arguments in support of C-21).

Second, we are concerned about the possible over-emphasis of the need to monitor Canadians crossing into the United States for national security purposes. While there have been foiled attempts at cross-border terrorism, current laws have been effective in preventing them. Using the spectre of stopping terrorists from crossing from Canada into the United States to justify greater border security has rightly been criticized in the past, and we are dismayed that the government would continue to perpetuate it.

#### **5. Redress**

Currently, the bill provides no option for redress should exit data about an individual be incorrect. We would make two recommendations that should be added to Bill C-21:

- a) That a system be put in place allowing individuals to request from CBSA any information about their travels that the agency may currently hold (similar to the system that currently exists for air travel passengers)
- b) That a redress system be created within CBSA to request the correction of any inaccurate personal information being held, and that CBSA be responsible for ensuring that any agencies with whom that information has been shared be provided the updated, corrected information

This is particularly important, given that there is currently no independent review or complaints body for the CBSA.

## **Conclusion**

The collection of exit data has become the norm in the international community, including among Canada's security partners. We recognize that this means it is likely that Canada will adopt the same practice. At the same time, we remain concerned that the Canadian government's national security priorities continue to focus primarily on perceived threats and imposing greater and more restrictive security laws.

While Bill C-21 is not the most menacing or far-reaching piece of legislation, it is an integral part of a larger trend in Canadian national security policy to collect more and more Canadians' private information in order to analyse and predict national security threats, a practice that has been widely criticized as flawed. It also continues the trend of greater border and security integration with the United States, once again raising concerns of privacy, but also of accountability and, where necessary, redress.

As a coalition, we continue to urge the Canadian government to take a rights-based approach to all national security policies. We strongly believe that the protection and strengthening of our rights and freedoms (including for Canadians, permanent residents and foreign nationals) does more to increase our collective security than does the gradual creep of national security and surveillance laws.

We hope the Committee reviews Bill C-21 with these issues in mind and takes our recommendations into consideration. Should you have more questions, please contact our national coordinator, Tim McSorley, at either [national.coordination@iclmg.ca](mailto:national.coordination@iclmg.ca) or at (613) 241-3298. We thank you for your time.