Senate Standing Committee on National Security and Defence, Study on

Bill S-7: Digital Devices at Our Borders

Legislative Brief

June 9, 2022

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC)
Tamir Israel, Staff Lawyer

The Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) is a legal clinic based at the Centre for Law, Technology & Society at the University of Ottawa, Faculty of Law.

An electronic version of this document can be obtained at:
https://cippic.ca/uploads/20220609-BillS7-Testimony.pdf

Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic

University of Ottawa, Faculty of Law, Common Law Section
57 Louis Pasteur Street
Ottawa, ON K1N 6N5
Website: https://cippic.ca
Email: admin@cippic.ca
Twitter: @cippic

Introduction

The Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC) is pleased to provide its input the Senate Standing Committee on National Security and Defence's study of Bill S-7, which would create a framework for searches of digital devices at ports of entry.

CIPPIC is a legal clinic based at the Centre for Law, Technology and Society at the University of Ottawa, Faculty of Law. CIPPIC's mandate is to advocate in the public interest on matters arising at the intersection of law and technology.

Bill S-7 represents the government's response to the Alberta Court of Appeal's decision in *R v Canfield*, which held that border control officials could not rely on a generalized search power and non-binding policies as a basis for examining digital devices at border crossings. While there are a number of issues with the Bill, our written comments focus on what we view as its central problem—the adoption of a novel and, in our view, constitutionally indefensible standard for digital device searches that will subject thousands of Canadians' deeply private digital devices to scrutiny by border officials.

The *Canfield* decision adopted an incremental approach to its constitutional ruling—while noting that reasonable suspicion appears to be the most appropriate standard for device searches, the Alberta Court of Appeal did not foreclose the government an opportunity to attempt to justify a more rigorous standard.[1] However, the *Canfield* court also noted that it is difficult to justify how reliance on a lower threshold can be minimally impairing as constitutionally required when the reasonable suspicion standard is employed for border searches of less intrusive searches.[2] In the context of immigration-related border searches, the Alberta Court of Appeal has since held that reasonable suspicion is the constitutional minimum.[3]

[1] *R v Canfield*, 2021 ABCA 383, para 75; *R v Pike*, 2022 ONSC 2297, paras 102-104.

[2] *R v Canfield*, 2021 ABCA 383, paras 91-102; *R v Pike*, 2022 ONSC 2297, para 108.

[3] *R v Al Askari*, 2021 ABCA 204, para 75.

Unfortunately, Bill S-7 represents the most intrusive option available to the government in light of the *Canfield* decision and fails to adopt a solution that respects the important privacy interests threatened by expansive searches of digital devices.

When we bring our phones and laptops along with us in our international travels, a fastidious record of our lives comes with us. While the act of packing a suitcase is a selective process, we do not—and should not need to—audit our devices for revealing health documents, politically unpopular conversations or embarrassing photos each time we travel abroad. Empowering border officials to subject our devices to this type of scrutiny in the absence of reasonably grounded suspicion can have chilling effects that reverberate into our lives.

The novel standard proposed by Bill S-7 is problematic for a number of reasons. It is, as noted, simply not commensurate with the intrusiveness of the searches it would authorize. By definition, a lower standard will impact more innocent people and this is not acceptable given the high countervailing privacy interests engaged. Second, the more latitude that is granted to border officials the more their conscious and subconscious biases will play a significant role in their target selection. Even under more restrictive standards, racial profiling and targeting of marginalized LGBTQ content has been a problem at the border.[4] Third, CBSA's device search initiative is predominantly operating as a domestic law enforcement program. While the content that is the primary object of this program is insidious, it possess no security threat and in the majority of instances its possession has minimal connection to border crossings but is rather a reflection of an individual's general use of their devices. Finally, the more permissive standard adopted by Bill S-7 will also harm lawyers, journalists, human rights defenders, and others who take their sensitive work on their personal devices when they travel.

Additional concerns arise from the novelty of the standard. If the standard is not struck down as unconstitutional, courts will, in time, provide guidance on the substantive requirements of Bill S-7's "reasonable general concern". We further note that most other jurisdictions around the world

[4] *Little Sisters Book and Art Emporium v Canada (Minister of Justice)*, 2000 SCC 69.

operate under a two-tiered system for articulated grounds of search creating further confusion regarding where this new standard could fit into a system oHowever, until that occurs, CBSA will have relatively free reign to apply its codified policies in a fluid manner. Tens if not hundreds of thousands of Canadians may be unfairly subjected to device searches in the interim.

Bill S-7 is not driven by critical border security objectives

We grant our border officials wide latitude to interfere search travellers as they cross our borders. This is out of recognition that travellers recognize that "that sovereign states have the right to control who and what enters their borders" and so expect lower levels of privacy when seeking to enter a country.[5]

While mobile devices can also contain receipts or identification documents, travellers can be compelled to show these documents to border officials at ports of entry and the presence of these documents provides no justification for a reduced standard with respect to sensitive mobile devices.[6] The primary target of the intrusive digital device searches CBSA would authorize though this Bill is digital contraband.

Individual border crossings play a significant role in facilitating the global dissemination of some forms of contraband, such as narcotics or counterfeit goods. This is not the case with respect to the circulation of unlawful digital content such as copyright infringing or child exploitation materials, which are predominantly circulated through the Internet.

CBSA's digital contraband initiative is predominantly operating as a domestic law enforcement program and its operation is far removed from the pressing objectives that justify extraordinary intrusions by border officials.[7] While the content that is the primary target of this program is insidious, it does not rely on individual border crossings as a means of dissemination and possess no security threat and in the majority of instances its possession

[5] *R v Al Askari*, 2021 ABCA 204, para 31.

[6] *R v Al Askari*, 2021 ABCA 204, paras 44 and 66; *R v Pike*, 2022 ONSC 2297, paras 95-96.

[7] *R v Singh*, 2019 ONCJ, 453, paras 78, 83-84 and 87-90.

has minimal connection to border crossings but is rather a reflection of an individual's general use of their devices.

Additionally, while it is unfair to require all Canadians to audit their digital devices for embarrassing content prior to each international trip, it is likely that criminals will become aware over time that traversing the border with contraband is risky and will begin taking steps to transfer contraband over the Internet instead of on their devices.[8]

The conduct that Bill S-7 would authorize is therefore far removed from the pressing objectives that justify extraordinary search at our borders.

Reasonable General Concern allows racial & other subjective biases to prevail in identifying who to search

To survive constitutional scrutiny, grounds for intrusive search must be objective and individualized. The Reasonable General Concern standard requires a 'concern' that certain indicia are in place before a search of a device can occur. The term "concern" is intended to signal something less than a "suspicion" which, in turn, signals something less than a "belief" in the hierarchy of legal standards that govern when government officials can interfere with privacy.

Where the *Charter* requires that a search be premised on articulated grounds, these grounds must be objective and individualized to meet the constitutional minimum. [9] In terms of its intended statutory scope, the new standard is objective in that it only applies to "reasonable" concerns. We do not, however, accept that the new standard is individualized as it embraces "general" rather than individualized concerns.

Putting aside the specific language of the proposed standard, we have serious doubts that there is room for objectiveness or individualization below the reasonable suspicion threshold. While border control officers will be required to point to objective and perhaps individualized criteria in

[8] Testimony of Lex Gill, Research Fellow, Citizen Lab, Standing Senate Committee on National Security and Defence, Study on Bill S-7, 44th Parl, 1st SESS, June 8, 2022.

[9] *R v Kang-Brown*, 2008 SCC 18; *R v Chehil*, 2013 SCC 49; *R v MacKenzie*, 2013 SCC 50.

justification of a device search, the lower the threshold the less objective criteria must be in place before a search can occur.

Regardless of how that standard is currently being applied or what indicia are encoded into supporting regulations once Bill S-7 becomes law, the standard being advanced is intrusive and will interfere with the privacy of thousands of Canadians. The reasonable suspicion standard itself is demarcated by its capacity to interfere with the privacy of more innocent Canadians than the robust reasonable grounds to believe standard.[10]

The threshold proposed by Bill S-7 is by definition so low that thousands of travellers will meet the objective criteria necessary to justify a search. Decisions on which of these thousands of travellers will, in fact, be searched are therefore ultimately guided by subjective hunches and biases that require no documentation or articulation, because the legally required threshold is already met.

As noted above, the reasonable general concern standard adopted by Bill S-7 intends to encode without alternation an existing CBSA method for identifying which devices to search. Those policies require that border officials identify a "multiplicity of indicators" before searching a device. Many indicators are general in nature and others require subjective observations by the officer. CBSA has testified before the courts and before this committee that the presence of as many as two indicators is sufficient to justify an initial search of a device.[11] For example, CBSA

[10] *R v Chehil*, 2013 SCC 49, para 28: "The fact that reasonable suspicion deals with possibilities, rather than probabilities, necessarily means that in some cases the police will reasonably suspect that innocent people are involved in crime."

[11] Testimony of the Honourable Marco EL Mendicino, Minister of Public Safety, Standing Senate Committee on National Security and Defence, Study on Bill S-7, 44th Parl, 1st Sess, May 30, 2022, https://sencanada.ca/en/Content/Sen/Committee/441/SECD/55555-E:

> Let me walk you through some examples of how this will work. You have a single traveller returning from a lengthy stay in a country known for sex trafficking without a reasonable explanation for the journey. The traveller then becomes increasingly agitated and nervous as the exam progresses, demonstrating continued avoidance of eye contact, shifting weight back and forth, stuttering and sweating. Multiple digital devices are found during the baggage exam without a rationale as to why they are necessary for the journey. An examination of the devices uncovers multiple images of child pornography. In this case, we believe a threshold of reasonable, general concern would have been met thus authorizing the officer's search of the personal digital devices. However, it is doubtful that the higher "reasonable grounds to suspect" threshold would have been met, thus allowing the harmful content to pass through the border and enter the country.

R v Pike, 2022 ONSC 2297, para 88:

> The policy directives incumbent on customs officials are in my view insufficient to provide the necessary assurance that a digital device search is being conducted with the appropriate respect for personal privacy. The directives do not have the force of law. Examinations of digital devices are not to be conducted "as a matter of course [and]... should only occur where there is a multiplicity of indicators suggesting evidence of a contravention ..." This policy is inherently vague and gives great latitude to the officer. An "indicator" is "a single piece of information,

officials consider the United States to be a "renowned as a source country for child pornography",[12] while over a hundred thousand travellers cross into Canada from the United States *daily* in non-pandemic times.[13]

While training and statistical tracking are helpful steps that can help reduce implicit racial and other biases, studies have shown that there is an upper limit in the mitigating effect that these types of interventions can have in reducing deeply embedded and implicit biases.[14] Providing officers with broad discretion to search individual devices absent an obligation to rely on rigorous objective criteria as justification invites the ongoing reliance on implicit racial and other biases as a guiding force in deciding who's devices will get searched.

The CBSA search criteria that Bill S-7 would encode has been characterized by the Ontario Superior Court of Justice "grant[ing] to BSOs a virtually unfettered discretion to search digital devices"[15] while the Alberta Court of Appeal in *Al Askari* described CBSA device searches under this policy as "fishing expeditions".[16] The reasonable concern standard Bill S-7 would adopt codifies this open-ended discretion and would embrace the implicit racial and other bias that guide discretionary searches.

---

trend, abnormality, or inconsistency that when added to other information or data raises a concern to an officer about the threat presented by a traveller or shipment." An indicator can be as minor as the observation that the subject is nervous. In Mr. Pike's case, he was tapping his fingers on the desk at one point. Furthermore, for digital devices, a multiplicity of indicators is required but in cross-examination Mr. Vinette appeared to say that this could mean as few as two. The policy in this regard, Mr. Vinette was at pains to make clear, is not meant to impose a legal threshold. The result, in my view, is to grant to BSOs a virtually unfettered discretion to search digital devices.

R v AM, 2008 SCC 19, per Bastarache, J, para 151; *R v Chehil*, 2013 SCC 49, paras 28 and 31 (reasonable suspicion cannot attach to a "particular activity or location rather than a specific person" and "characteristics that apply broadly to innocent people are insufficient, as they are markers only of generalized suspicion. The same is true of factors that may "go both ways", such as an individual's making or failing to make eye contact. On their own, such factors cannot support reasonable suspicion."

[12] *R v Canfield*, 2020 ABCA 383, para 57.

[13] Statistics Canada, "Travel Between Canada and Other Countries, December 2021", February 23, 2022, https://www150.statcan.gc.ca/n1/daily-quotidien/220223/dq220223b-eng.htm: "In December, US residents took 550,300 trips to Canada, almost five times as many as in December 2020 (113,900), but less than one-third (32.4%) of the 1.7 million such trips taken in December 2019. … Canadian residents returned from 1.1 million trips to the United States in December 2021, more than four times December 2020 (271,100), but far below the 3.4 million such trips in December 2019."

[14] Testimony of Lex Gill, Research Fellow, Citizen Lab, Standing Senate Committee on National Security and Defence, Study on Bill S-7, 44th Parl, 1st SESS, June 8, 2022; Testimony of Pantea Jafari, Member, Canadian Muslin Lawyers Association, Standing Senate Committee on National Security and Defence, Study on Bill S-7, 44th Parl, 1st Sess, June 6, 2022; Colleen Walsh, "Solving Racial Disparities in Policing", February 23, 2021, *The Harvard Gazette*, https://news.harvard.edu/gazette/story/2021/02/solving-racial-disparities-in-policing/.

[15] *R v Pike*, 2022 ONSC 2297, para 88.

[16] *R v Al Askari*, 2021 ABCA 204, para 39; contrast paras 67-74.

Reasonable Suspicion is the constitutional minimum

In our view, reasonable suspicion is the constitutional minimum for border device searches and, indeed, reasonable and probable grounds may be the most appropriate standard and ultimately required by the courts.[17]

The reasonable suspicion standard is already highly permissive and was initially adopted specifically to address the context of border searches. Compounding the problem is the nature of the search—border officials need only formulate reasonable suspicion that some evidence of *any* border-related wrongdoing might be found on a given device.[18] As a result, even the reasonable suspicion standard will capture more digital devices than when applied to other border searches such as strip or cavity searches, where suspicion must establish the possibility of contraband.[19]

Despite our concern regarding the permissiveness of the reasonable suspicion standard, we accept that reasonable suspicion is an acceptable standard for parliament to advance in terms of border device searches. It is a well established standard with substantial guidance from the courts and with familiar equivalents in other jurisdictions.

By contrast, Bill S-7's Reasonable General Concern standard has no known counterpart in law, and establishes a threshold so low that it invites racially biased and subjectively driven interference with the significant privacy interests inherent in our digital devices. We ask that you amend Bill S-7 and insert reasonable suspicion as the basis for search.

FIN.

[17] *R v Al Askari*, 2021 ABCA 204, para 52.

[18] *R v Pike*, 2022 ONSC 2297, paras 97-100; proposed 99 … (c).

[19] *R v Chehil*, 2013 SCC 49, para 36: "A nexus must exist between the criminal conduct that is suspected and the investigative technique employed: see *Mann*, at para. 34. In the context of drug detection dogs, this nexus arises by way of a constellation of facts that reasonably supports the suspicion of drug-related activity that the dog deployed is trained to detect."