THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

Privacy in Personal Electronic Devices at the Canadian Border

CANADIAN BAR ASSOCIATION
PRIVACY AND ACCESS LAW SECTION, IMMIGRATION LAW SECTION,
CRIMINAL JUSTICE SECTION, COMMODITY TAX, CUSTOMS AND TRADE SECTION AND
ETHICS AND PROFESSIONAL RESPONSIBILITY SUBCOMMITTEE

JUNE 2022

66 Slater St., Suite 1200, Ottawa, ON, Canada K1P 5H1
tel/tél. 613 237-2925 • **tf/sans frais** 1-800 267-8860 • **fax/téléc**. 613 237-0185 • cba.org • info@cba.org

PREFACE

The Canadian Bar Association is a national association representing 36,000 jurists, including lawyers, notaries, law teachers and students across Canada. The Association's primary objectives include improvement in the law and in the administration of justice.

This submission was prepared by the CBA Privacy and Access Law, Immigration Law, and Commodity Tax, Customs and Trade Law and the Criminal Justice Sections and the Ethics and Professional Responsibility Subcommittee with assistance from the Advocacy Department at the CBA office. The submission has been reviewed by the Law Reform Subcommittee and approved as a public statement of the CBA Privacy and Access Law, Immigration Law, Criminal Justice and Commodity Tax, Customs and Trade Law Sections and the Ethics and Professional Responsibility Subcommittee.

TABLE OF CONTENTS

Privacy in Personal Electronic Devices at the Canadian Border

Privacy in Personal Electronic Devices at the Canadian Border

EXECUTIVE SUMMARY

The Privacy and Access Law, Immigration Law, Commodity Tax, Customs and Trade Law, the Criminal Justice Sections and the Ethics and Professional Responsibility Subcommittee (the CBA Sections) appreciate the opportunity to appear before the Standing Senate Committee on National Security and Defence in its study of Bill S-7, *An Act to amend the Customs Act and the Preclearance Act, 2016*.

Information collection and sharing at the border is necessary to ensure the security of Canadians. However, collecting and sharing too much information or unreliable information can also lead to harmful consequences for Canadians. An appropriate balance must be achieved to protect our safety and preserve our individual privacy rights and freedoms. The CBA Sections comment on collection of information at the border on entry and exit, solicitor-client privilege at the border and disclosure of information collected at the border.

A. Collection of Information at the Border on Entry and Exit

Most travelers now carry mobile electronic devices like smartphones, with sensitive personal data. The powers of customs agents to inspect the contents of these devices should be re-examined. Information stored on an electronic device is not a "good" – and any interpretation of the *Customs Act* that would authorize a warrantless search of data stored on a device would likely be unconstitutional.

Bill S-7 amends the *Customs Act* to:

- clarify the circumstances in which border service officers may examine documents stored on personal digital devices;
- authorize the making of regulations in respect of those examinations; and
- update certain provisions respecting enforcement, offences and punishment.

It also amends the *Preclearance Act, 2016*, to clarify the circumstances in which preclearance officers may examine, search and detain documents stored on personal digital devices and

authorize the making of regulations and the giving of ministerial directions in respect of those examinations, searches and detentions.

The CBA Sections comment on the new, lower threshold of "reasonable general concern" for border searches of a traveler's Personal Electronic Devices (PEDs) and the new authority to examine created under Bill S-7. We also highlight relevant case law on the constitutionality of PED searches at the border as authorized by the *Customs Act*. In our view, the effect of Bill S-7 is not consistent with the existing caselaw regarding searches of electronic devices, given the very high privacy interests in their contents. The low threshold set out in S-7 does not offer any meaningful protection to the acute privacy interests of travelers.

B. Solicitor-Client Privilege

Solicitor-client privilege is fundamental to the proper functioning of the Canadian legal system. It must be respected at the Canadian border, at Canadian airports, and when Canadian lawyers and their clients travel to the US. The CBA Sections recommend the creation of a working group to collaborate on the development of a comprehensive, binding policy on solicitor-client privilege that is publicly available on the CBSA website. More detailed guidance should be available to CBSA officers and the public, including lawyers, to ensure safeguards are in place to avoid unauthorized access to documents protected by solicitor-client privilege.

Privacy in Personal Electronic Devices at the Canadian Border

I. INTRODUCTION

The Privacy and Access to Information Law, Criminal Justice, Immigration Law and Commodity Tax, Customs and Trade Law Sections and the Ethics and Professional Responsibility Subcommittee (the CBA Sections) have prepared this submission to the Senate Standing Committee on National Security and Defence, commenting on the proposed changes to the *Customs Act* and the *Preclearance Act* set out in Bill S-7.

The CBA is a national association of over 36,000 members, including lawyers, notaries, academics and law students, with a mandate to seek improvements in the law and the administration of justice. The CBA Sections comprise lawyers with an in-depth knowledge of privacy and access law, immigration law, criminal law and issues relevant to commodity tax, customs and trade law.

In September 2017, the CBA commented on proposed changes to the *Customs Act* in former Bill C-21, *An Act to Amend the Customs Act* and to proposed amendments to the *Preclearance Act* in former Bill C-23, *Preclearance Act, 2016.*[1] Many of the same privacy issues engaged by the proposed language of Bill S-7 were similarly engaged in those former Bills. We repeat 2017 submissions to the extent that they remain relevant and applicable to Bill S-7.

Dependence on technology has become even more entrenched in our personal lives since 2017, and reliance on digital tools to weather the challenges of the COVID-19 pandemic accelerated that process further. These digital technologies enable greatly enhanced collection, storage and sharing of personal information. In this context, legislation proposing to change the federal government's right to access and inspect information contained in personal electronic devices (PEDs) of people crossing the Canadian border requires striking a balance between the privacy rights of those persons and the imperative of the government to secure the country's borders and protect national security.

---

1 See Privacy of Canadians at Airports and Borders, CBA submission 2017: online.

With this balance in mind, the CBA Sections comment on collection of information at the border on entry and exit, solicitor-client privilege at the border, disclosure of information collected at the border, and collection of information at the border on entry and exit.

II. COLLECTION OF INFORMATION AT THE BORDER ON ENTRY AND EXIT

A. Legislative Changes Affecting Privacy Rights at the Border

Bill S-7 proposes changes to the *Customs Act* and the *Preclearance Act, 2016*.

With respect to the *Customs Act*, the Bill proposes to:

a) clarify the circumstances in which border service officers may examine documents stored on personal digital devices;

b) authorize the making of regulations in respect of those examinations; and

c) update certain provisions respecting enforcement, offences and punishment.

The main component of the Bill is to implement a new threshold that Canada Border Service Agency (CBSA) officers must establish before initiating an examination of PEDs. The Bill also establishes an authority to examine documents on PEDs pursuant to new regulations proposed in the changes to the two Acts.

Bill S-7 would also amend the *Preclearance Act, 2016* to clarify the circumstances in which preclearance officers may examine, search and detain documents stored on PEDs and authorize the making of regulations and the giving of ministerial directions in respect of those examinations, searches and detentions.

B. Searches of Electronic Devices

Most travelers now carry mobile electronic devices like smartphones tablets and laptops, with sensitive personal data. These devices have become increasingly indispensable in travel, including cross-border travel. More and more travelers are using their mobile devices for contactless payments, and the government requires that international travelers use the ArriveCan app to enter the country.

At one time, Canadians stored their most private information in physical records in their homes. When travelling, they might have had a bag or briefcase with documents necessary for their trip. Today, quantitatively and qualitatively more private information is in a single device than

used to be stored in briefcases, homes, offices or anywhere else.[2] The information storage capacity and the privacy concerns arising from them are completely different than those arising from physical storage vessels like luggage, which shaped the early principles of "briefcase law."[3]

The intimate personal information on the device can date back to the purchase of the phone, or even earlier. This includes current and historical data on a person's geo-location, call history, text messages, email, photos, contacts, calendar, physical activity, health, finances, shopping history, internet searches and more. This information can provide insight into a person's preferences, habits, interests and values. For many professionals –including doctors, lawyers, business executives, human rights activists and journalists – the devices may also contain highly sensitive information about others. Cloud services regularly synchronize significant data stores to one or more devices and may be difficult or impossible to fully delete.

This modern reality was unknown when the relevant provisions of the *Customs Act* were drafted. Since then, Supreme Court of Canada (SCC) decisions have modified the common law in response to technological change, and lead us to an understanding that there is a very high expectation of privacy in the contents of electronic devices.[4] For example, in *R v Fearon,*[5] the SCC modified the common law rule related to search incident to arrest for smartphones specifically due to the immense privacy implications in searching such devices.[6] The SCC has clearly established that the greater the intrusion on privacy, the greater the constitutional protections and a greater justification for the search is required. And while there may be a diminished expectation of privacy at the border, this expectation is not completely extinguished.[7] There is still an expectation of privacy, particularly when dealing with electronic devices that inherently attract significant privacy interests.[8]

---

2 *See for example,* Canadian Press, *Smartphone Use Way Up in Canada, Google Finds*, available online. This trend has attracted US judicial commentary, see for example, *Riley v. California*, 134 S. Ct. 2473 (2014), available online, where the US Supreme Court observed that saying a search of data on a smartphone is the same as the search of a person's physical items, "*is like saying a ride on horseback is materially indistinguishable from a flight to the moon."*

3 *See R. v Simmons,* [1988] 2 SCR 495, available online,where the Supreme Court referred to grounds for suspecting that a person has made a false declaration and is transporting prohibited goods in order to search a suitcase.

4 *R v Vu,* 2013 SCC 60, available online. *See also, R v Morelli*, 2010 SCC 8, available online.

5 2014 SCC 77.

6 *R v Fearon*, 2014 SCC 77, available online.

7 *Supra* note 9 (*Simmons*). *See also R v Nagle,* 2012 BCCA 373, available online.

8 *R v Cole,* 2012 SCC 53, available online. The search of an employee's company-issued laptop was found to be a violation of the employee's s. 8 *Charter* rights. While the employee had a lowered expectation of privacy in a work computer, he nonetheless had an expectation of privacy—particularly given the high stakes of a search of a computer.

In 2017, the Privacy Commissioner of Canada appeared before the House of Commons Standing Committee on Public Safety and National Security on the question of the privacy of electronic devices at the borders during its study of then-Bill C-23,[9] observing that the problem with groundless searches of electronic devices is that they do not recognize that they are extremely privacy intrusive because those devices contain the most personal and intimate information we hold. In his 2019 Report,[10] the Commissioner details the investigation of six complaints filed by individuals whose PEDs were searched by the CBSA. He concluded that the CBSA contravened the *Privacy Act* and identified significant failings in the CBSA's practices overall. In the 2020 Report,[11] the Commissioner held that CBSA could only retain traveler's digital device passcodes when necessary to do so.

C. Searches of Information Stored on Personal Electronic Devices Must Be Carefully Restricted to Respect Individual Privacy

Suspicionless searches of PEDs at the border are unconstitutional

Any warrantless search of the data stored on an electronic device (including any requirement that an individual disclose a device password) implicates sections 7 and 8 of the *Canadian Charter of Rights and Freedoms (Charter)* and would likely be found to be unconstitutional. In our view, the effect of Bill S-7 is not consistent with the existing caselaw regarding searches of electronic devices, given the very high privacy interests in their contents. The low threshold in Bill S-7 does not give any meaningful protection to the acute privacy interests of travelers.

The privacy interests in PEDs are so high that the lowered expectation of privacy rights at the border does not override those interests. In *R v Vu*, the SCC found that a warrant search excludes a computer found on those premises because of the acute privacy interests engaged by these devices.[12] While the information to obtain the warrant referenced computer generated documents, this was found to be insufficient to examine the contents of the computer without more specific authority.

---

9 Privacy Commissioner of Canada, *Follow-up letter to the Standing Committee on Public Safety and National Security regarding Bill C-23, An Act respecting the preclearance of persons and goods in Canada and the United States* (June 2017), available online

10 Crossing the Line? The CBSA's examination of digital devices at the border: available online

11 Privacy Commissioner of Canada, *CBSA should only retain traveler's digital passcodes when necessary,*

12 *Supra* note 4_ (*Vu*).

The Canfield decision

In 2020, the Alberta Court of Appeal ruled in *R v Canfield*[13] on the constitutionality of searches of PEDs at the border pursuant to the *Customs Act*. The definition of "goods" in s. 2 of the Act had been interpreted to encompass PEDs. CBSA agents used this definition to request access to both accuseds' devices after they observed several 'indicators' which they deemed required a 'secondary inspection.'[14]

The Court of Appeal found the authorization of routine, suspicionless searches of PEDs at the border to violate section 8 of the *Charter*.[15] Accordingly it declared the definition of "goods" in s. 2 of the Act to be "of no force or effect insofar as the definition includes the contents of personal electronic devices."[16] In its reasoning, the Court of Appeal noted that the low expectation of privacy at international border crossings must be balanced against the high expectation of privacy that individuals have in their PEDs.[17] Citing the finding in *Vu*, the *Canfield* decision emphasizes the high expectation of privacy individuals hold in their PEDs, and concludes that searches of PEDs at the border simply cannot be considered "routine."[18] Accordingly, any authorization to search PEDs "must have a threshold requirement" in order to be *Charter*-compliant.[19] The Court suspended the declaration of invalidity for a year in order to give Parliament time to amend the legislation and introduce a threshold.

The appropriate threshold of suspicion for searches of PEDs at the border

Bill S-7 proposes a novel standard of "reasonable general concern" for a border security officer to search a traveler's PED. The CBA Sections are concerned that "reasonable general concern" is too vague to be an appropriate threshold requirement and that the standard would not be *Charter*-compliant.

The standard of "reasonable general concern" has not been used to justify searches or employed by Canadian courts. Absent further clarification, it is difficult to know how it will be applied and whether its application by border security officers will be *Charter*-compliant. The concept of a "generalized suspicion," however, has been reviewed and compared to the

13 2020 ABCA 383 [Canfield].
14 Canfield at paras 4, 9-11.
15 Canfield at para 75.
16 Canfield at para 111.
17 Canfield at para 67.
18 Canfield at paras 71-75.
19 Canfield at para 75.

standard of "reasonable suspicion," with only the latter rendering warrantless searches compliant with section 8 of the *Charter*, in some circumstances.

In *R v Chehil*,[20] where a sniffer dog was used to detect drugs in a traveler's luggage, the SCC addressed the issue of what standard of suspicion is required to conduct a warrantless search at the border. It held the search was constitutional because the standard applied was that of reasonable suspicion, which is capable of being "subject to independent and rigorous judicial scrutiny".[21] The Court cautioned against the application of mere generalized suspicion which would have rendered the search unconstitutional. At paragraph 28 the SCC stated that:

> properly conducted sniff searches that are based on reasonable suspicion are Charter-compliant in light of their minimally intrusive, narrowly targeted, and highly accurate nature… However, the suspicion held by the police cannot be so broad that it descends to the level of generalized suspicion, which was described by Bastarache J … as suspicion "that attaches to a particular activity or location rather than to a specific person".

Chehil also positively cites American jurisprudence regarding the need for individualized suspicion at paragraph 30:

> A constellation of factors will not be sufficient to ground reasonable suspicion where it amounts merely to a "generalized" suspicion because it "would include such a number of presumably innocent persons as to approach a subjectively administered, random basis" for a search: United States v. Gooding, 695 F.2d 78 (4th Cir. 1982).

While in *Canfield* the Court of Appeal declined to specify a particular threshold and found that one lower than reasonable suspicion may be appropriate,[22] it also cited *Fearon* for the proposition that unlimited and suspicionless searches would not be compliant (at paras 78-79).[23] Also of note is paragraph 76 of *Canfield*:

> We hasten to add that not all searches of personal electronic devices are equal. As was noted in Vu at para 63, it is neither possible nor desirable "to create a regime that applies to all computers or cellular telephones that police come across in their investigations, regardless of context".

The Court of Appeal appropriately emphasizes the need for a specific standard that is tailored to the border context.

---

20 2013 SCC 49 [Chehil].

21 Chehil at paras 3-6.

22 Canfield at para 75.

23 Canfield at paras 78-79.

As *Canfield* is an appellate-level decision and *Chehil* from the SCC, differences in the analysis of the appropriate threshold standard of suspicion at the border must be settled by the latter case.

The proposed threshold of "reasonable general concern" in Bill S-7 is dangerously close to the standard of "generalized suspicion," which the SCC cited as an example of an unconstitutional threshold. The constitutionality of this threshold is further called into question because the term is a novel one in law and there are no guidelines in the Bill about how to apply it. Absent further qualification, as written it is at serious risk of not surviving *Charter* scrutiny.

Consistency with other Customs Act search powers

The powers of a customs officer to search "goods" that are being imported or exported is set out in subsection 99(1) of the *Customs Act*. In all cases where the issue leading to an examination is a potential contravention of a legal requirement in respect of the goods, such as errors in the declared tariff classification, valuation or origin of the goods, or a contravention of any other Act of Parliament administered or enforced by the CBSA, the officer must have "reasonable grounds" for the search. Bill S-7 proposes a new subs. 99.01(1) of the *Customs Act* to allow a search of information stored on a "personal digital device" for substantially the same reasons as are already in subs. 99(1) (i.e., potential contravention of any other Act of Parliament administered or enforced by the CBSA). It follows that a standard equivalent to or approaching "reasonable grounds" should be required for consistent application between subs. 99(1) and new subs. 99.01(1) searches; *a fortiori*, a "reasonable general concern" for searches of PEDs falls far short of an equivalent standard for contraventions that do not involve any privacy concerns (i.e., whether the tariff classification, origin or valuation of imported goods contravenes the *Customs Act*).

Reconciling "reasonable general concern" threshold with existing legislation permitting searches

Bill S-7 will create competing and inconsistent thresholds, both applicable to screening at ports of entry into Canada. By importing a "reasonable general concern" standard into the *Customs Act*, border officers will be caught between the threshold needed to examine PEDs for contravention of an Act of Parliament and the threshold for breaches of the *Immigration and Refugee Protection Act* (*IRPA*). This can lead to inconsistent application by officers at ports of entry, as violations of the *Customs Act* and *IRPA* are often interconnected. The CBA Sections recommend that the standards be consistent and that *IRPA* s.139(1) standard requiring "reasonable grounds," which has existed for over 30 years, be maintained.

Section 139(1) addresses examination at ports of entry to Canada, which requires that there be "reasonable grounds" before a border officer may search the luggage or personal effects of an individual entering Canada:

> **139 (1)** An officer may search any person seeking to come into Canada and may search their luggage and personal effects and the means of transportation that conveyed the person to Canada if the officer believes on reasonable grounds that the person.
>
> **(a)** has not revealed their identity or has hidden on or about their person documents that are relevant to their admissibility; or
>
> **(b)** has committed, or possesses documents that may be used in the commission of, an offence referred to in section 117, 118 or 122.

To conduct a search, there must be reasonable grounds to believe a person (1) has not revealed their identity, (2) may be inadmissible to Canada, which includes Canadian and overseas criminality, security concerns, medical or financial grounds, misrepresentation, and non-compliance with *IRPA*,[24] or (3) is involved with human smuggling or trafficking, or the creation, possession, or use of fraudulent or improperly obtained identity documents.

The proposed s. 99.01(1)(c) in Bill S-7 permits searches where there is a "reasonable general concern" that documents stored on a PED will provide evidence of a contravention of an Act of Parliament. This would include *IRPA*, yet a search of luggage and personal effects – less intrusive that a search of a PED – for contraventions of *IRPA*, requires reasonable grounds.

To offer an example, a border officer would need reasonable grounds to believe that a person has worked without authorization in Canada (non-compliance with *IRPA*, under s.41), yet would require a lower standard of reasonable general concern to search for obscene materials. This becomes problematic when the discovery of obscene materials is pursued before a court or tribunal. By committing this crime on entry to Canada, the individual is also anticipated to be inadmissible to Canada under ss.36(1)(c), 36(2)(c), and/or 36(2)(d) of *IRPA*[25], yet this search and discovery would only require "reasonable general concern" which is an insufficient threshold for the search of PED under *IRPA.* Evidence acquired by such means could not be used to support an admissibility hearing under *IRPA* yet could be used for a more serious criminal prosecution.

---

24 Grounds of admissibility are captured under Part 1, Division 4: Inadmissibility of the *IRPA*, ss. 34 to 42.

25 Sections 36(1)(c) and 36(2)(c) capture the commission of offences outside Canada, such as possession of obscene materials. Section 36(2)(d) captures those who commit and offence on entry to Canada, which could capture the importation of obscene materials.

Section 16 of *IRPA* requires individuals seeking entry to Canada (through application or at the port of entry) to answer truthfully and present the documents required for the assessment of their eligibility to enter Canada. This is a broader search concerned with eligibility to enter Canada (identity and compliance with the Act), and therefore has limited application for Canadian citizens who must only establish citizenship to be eligible for entry.

Since the Alberta Court of Appeal's decision in *Canfield*, that Court looked at port of entry searches in *Al Askari*.[26] The Crown agreed that the search of Mr. Al Askari's PED could not be supported under s.139(1), as the border officer did not have reasonable grounds to complete the search but argued that the search was instead permitted under s.16 of *IRPA*. The Court of Appeal concluded that searches under s.16 required "reasonable suspicion:"[27]

> [63] Prof Robert Currie argues for a careful treatment of electronic devices at the border, and proposes a framework similar to that adopted in *Canfield*: see "Electronic Devices at the Border: The Next Frontier of Canadian Search and Seizure Law?" (2016) 14:2 Can J L & Tech 289. His proposal adapts the traditional s 8 methodology with a view to balancing the heightened privacy interests in electronic devices with lower expectations at the border and the state's legitimate security objectives: 307. Prof Currie advocates departing from *Simmons* by beginning with the premise that s 8 applies during the screening process: 307-308.
>
> [64] Prof Currie suggests that the critical issue is measuring the reasonably reduced expectation of privacy at the border and the extent of permissible state intrusion into it. In his view, this is best achieved through the established test in *R v Collins*, 1987 CanLII 84 (SCC), [1987] 1 SCR 265, 308, 38 DLR (4th) 508. Was the search authorized by law? Is the law itself reasonable? Is the search carried out in a reasonable manner?
>
> [65] When assessing whether the law itself is reasonable, Prof Currie proposes a standard of reasonable suspicion because it is tailor-made to the border context. It must amount to more than a generalized suspicion and be based on objectively reasonable facts within the totality of the circumstances: 311. On the reasonableness of the search, he advocates for an inquiry into whether the search was limited in scope and duration: 312-314.
>
> [66] We endorse this approach but it must be tailored to the purposes of *IRPA*; identity and admissibility. Refugee claimants might carry all of their documents on an electronic device and in this circumstance the display of those documents would be part of the routine examination under the Act. Other claimants carry hard copy documents, as did Mr. Al Askari. In either scenario, a reasonable suspicion that would ground a further search of the electronic device might arise.

Both thresholds for searches under *IRPA* are higher than the proposed "reasonable general concern" in Bill S-7. The creation of a "reasonable general concern" standard is not only novel

---

26 *R v Al Askari*, 2021 ABCA 204

27 Ibid, at paras. 44, 55, 66.

and without definition, but also inconsistent with existing legislation governing port of entry searches. Given the jurisprudence confirming that PEDs contain inherently private information, the creation of this lower threshold is unreasonable, inconsistent with other search standards, and anticipated to run afoul of the *Charter*.

In the impaired driving context, the *Criminal Code* authorizes warrantless searches for breath samples to be given into approved screening devices and approved instruments, saliva samples to be given into approved drug screening equipment, and blood samples for analysis into approved containers. However, these searches are not an adequate comparator to the searches conducted at the border.[28]

For example, most searches conducted in the driving context are based on a higher standard than contemplated in Bill S-7 if the fruits of the searches are to be used for an evidentiary purpose. There is a common law prohibition on the use of the results of any search conducted on a reasonable suspicion or lower standard (such as roadside breath testing, saliva testing, or standardized field sobriety tests) as evidence at trial.[29] The results are only admissible for the limited purpose of permitting an officer ground to make a further evidentiary demand.

Further, while the right to counsel is suspended in the context of these searches, that suspension is also directly connected to constitutional safeguards in the testing process, including the limited-use-immunity doctrine and the requirement that the search be conducted forthwith, or immediately.[30] This requirement is subject only to the exigencies of the equipment in obtaining a reliable result.[31] There are no such procedural safeguards in the context of Bill S-7 with respect to the searches of PED at a point of entry.

Similarly, the *Criminal Code* prohibits the use of any breath, blood, or bodily testing results obtained for any purpose other than the prosecution of a criminal impaired driving offence.[32]

In December 2018, *Criminal Code* amendments came into force to permit breath sample searches absent any grounds. In finding such legislation constitutional, courts have routinely pointed to the fact that driving is a highly regulated activity that is a privilege and not a right.

---

28 *Criminal Code of Canada,* Part VIII.1.

29 *R. v. Orbanski; R. v. Elias,* [2005] 2 SCR 3.

30 *R. v. Thomsen,* [1988] 1 SCR 640; *R. v. Grant,* [1991] 3 S.C.R. 139; *R. v. Orbanski; R. v. Elias,* [2005] 2 SCR 3; *R. v. Woods,* [2005] 2 SCR 205.

31 *R. v. Bernshaw* [1995] 1 S.C.R. 254.

32 *Criminal Code of Canada,* Section 320.36(1).

This was confirmed in *R. v. Ladouceur,*[33] a constitutional challenge to the ability of police to randomly stop motorists to check sobriety. The SCC determined that s. 8 of the *Charter* is not engaged.

By contrast, entering Canada is a constitutionally protected right for any citizen of Canada. And searches of PEDs clearly engage s. 8. While crossing the border is a highly regulated activity, it is not analogous to driving which itself comes with a well-recognized reduced expectation of privacy and where arbitrary stops are permissible.

In *R v Hufsky*,[34] the appellant was stopped at a checkpoint for mechanical fitness and sobriety, among other things. The SCC found that the "overriding importance of the effective enforcement of the motor vehicle laws and regulations in the interest of highway safety" justified the limitation on the s. 9 right. This was grounded not only in the increased ability to detect impaired drivers but also the increased perception of the risk. Few other enforcement methods were available as mere observation of driving could not be relied on. The Court noted that driving is a "licensed activity subject to regulation and control in the interests of safety" and therefore the limitation on the right was proportionate.

It is also not accurate to say that the mandatory breath testing scheme sets the foundation for baseless searches. There are still limitations on mandatory testing: The officer must be in possession of the approved screening device (ASD). The officer must have conducted a lawful stop or be in the lawful execution of their duty. The demand and test must be immediate. These procedural safeguards distinguish this from what is proposed in Bill S-7.

Further, in *Goodwin v British Columbia (Superintendent of Motor Vehicles)*[35], the SCC emphasized that breath sample searches were not invasive and did not reveal core biographical data about the person. The results of the search could not be preserved. Again, *Goodwin* is relevant to this analysis. There, the SCC noted:

> The first is the degree of intrusiveness of the ASD test on a driver's bodily integrity and privacy interests. More intrusive than a demand for documents, a breath demand clearly amounts to what La Forest J. described as "the use of a person's body without his consent to obtain information about him" by which the state "invades an area of personal privacy essential to the maintenance of his human dignity": *R. v. Dyment*, 1988 CanLII 10 (SCC), [1988] 2 S.C.R. 417, at pp. 431-32. However, a roadside ASD test is far less intrusive than many other searches or seizures that may be performed

33 [1990] 1 SCR 1257

34 [1988] 1 SCR 621

35 2015 SCC 46

> for law enforcement purposes, such as the blood sample at issue in *Dyment*, or a DNA swab, which contains deeply personal information: *R. v. S.A.B.*, 2003 SCC 60, [2003] 2 S.C.R. 678, at para. 48. The roadside breath demand authorized by the *Criminal Code* has a much less significant impact on an individual's bodily integrity and privacy interests: *R. v. Stillman*, 1997 CanLII 384 (SCC), [1997] 1 S.C.R. 607, at para. 90. This minimally intrusive character supports the reasonableness of the ASD seizure.

At paragraph 67, the court also emphasized the reliability of the search in its specificity and accuracy at quickly detecting impaired drivers:

> [67] The reliability of a search or seizure mechanism is directly relevant to the reasonableness of the search or seizure itself: *R. v. Chehil*, 2013 SCC 49, [2013] 3 S.C.R. 220, at para. 48. As noted in *Chehil*, "[a] method of searching that captures an inordinate number of innocent individuals cannot be reasonable": para. 51. By contrast, a high degree of accuracy has been crucial to endorsing sniffer-dog searches on a lower standard of reasonable suspicion: *R. v. A.M.*, 2008 SCC 19, [2008] 1 S.C.R. 569, at para. 11; see also *R. v. Kang-Brown*, 2008 SCC 18, [2008] 1 S.C.R. 456.

The same cannot be said for PED searches, which could well involve a high number of innocent individuals and where there is no guarantee that the results yielded in the search will advance the interests of the legislation.

RECOMMENDATION

1. **The CBA Sections recommend that Bill S-7 specify a threshold of "reasonable grounds" or in the alternative "reasonable suspicion" or similarly individualized standard of suspicion, prior to the search of personal electronic devices at international borders. Or, in the alternative, that Bill S-7 be amended to articulate guardrails around "reasonable general concern", such that it can withstand Charter-scrutiny.**

III. SOLICITOR-CLIENT PRIVILEGE AT THE BORDER

Solicitor-client privilege is fundamental to the proper functioning of the Canadian legal system.[36] It must be respected at the Canadian border, at Canadian airports, and when Canadian lawyers and their clients travel to the US.

Solicitor-client privilege is the quasi-constitutional right to communicate in confidence with a lawyer. The privilege belongs to the client, not the lawyer.[37] Information protected by

---

36 *Blood Tribe Department of Health v. Attorney General of Canada et. al.*, [2008] 2 S.C.R. 574, online. *See also* Canadian Bar Association, *Solicitor-Client Privilege at the Canada-US Border* (June 19, 2014), online

37 *Andrews v. Law Society of British Columbia*, [1989] 1 S.C.R. 143, available online

solicitor-client privilege cannot be disclosed without the client's consent or a court order. The SCC has repeatedly emphasized that the privilege must remain "as close to absolute as possible and should not be interfered with unless absolutely necessary."[38] In the rare case of necessity, there must be explicit statutory authorization accompanied by legislated safeguards to ensure that disclosure does not compromise the substantive right.[39]

A lawyer or client may travel with documents (physical or electronic) that are protected by solicitor-client privilege. It is essential that the CBSA and US Customs and Border Protection (US CBP) in Canada maintain a transparent and expedited process to address solicitor-client privilege. Access to a PED (and the privileged information it contains) under examination may be necessary to meet important filing deadlines or for a client to seek time-sensitive legal advice, and loss of access over an extended period could have serious consequences.

No specific provision in the *Customs Act*, regulations or Bill S-7 deals with solicitor-client privilege, and there is some concern that CBSA might apply s. 153 of the *Customs Act* if a lawyer or client does not permit the examination of solicitor-client documents. Section 153 gives CBSA authority to charge an individual (or corporation) with avoiding compliance with the *Customs Act*. CBSA has used s. 153 of the *Customs Act* in similar circumstances – for example, in the case of Alain Philippon, who was charged after refusing to give CBSA his mobile phone password and later accepted a plea deal.[40] Lawyers in this situation are bound by their obligations to their clients and would find themselves in a very difficult situation.

CBSA wields limited public powers – it must obey relevant legislation and case law, and is subject to court orders.[41] CBSA decision-makers must also act fairly, especially when the impact of their decisions is substantial, such as handling documents and PEDs where solicitor-client privilege is claimed.[42] The US CBP is also permitted to undertake certain administrative and enforcement activities, including limited powers to examine goods, in approved preclearance areas at airports and border crossings through the *Preclearance Act.* Neither CBSA nor the US CBP should determine whether solicitor-client privilege applies to documents. This adjudication should be made only by a Canadian court.

---

38 *See most recently, Alberta (Information and Privacy Commissioner) v. University of Calgary,* 2016 SCC 53, available online.

39 *Canada (Attorney General) v. Chambre des notaires du Québec,* 2016 SCC 20, available online

40 *See* Mark Gollom, CBC News, *Alain Philippon phone password case: Powers of border agents and police differ* (March 6, 2015), available online

41 *Attorney General of Canada v. Bri-Chem Supply Ltd.*, 2016 FCA 257, available online

42 *Luking v. Minister of Public Safety an Emergency Preparedness, 2013 FC 222,* available online

The CBSA website reveals no published policy on solicitor-client privilege at the border that is readily available to lawyers and the public. In August 2013, the CBA urged the Ministers of Justice and Public Safety and the CBSA President to adopt a policy to recognize claims of solicitor-client privilege over documents and electronic documents at the border. The CBA also recommended the establishment of a working group and a collaborative approach to developing the CBSA policy.[43]

On September 27, 2016, Minister Goodale wrote to the President of the Canadian Bar Association, informing her that the CBSA had adopted policy guidance for CBSA officers in 2014.[44] This policy guidance was developed without input from or notification to the CBA. Since then, the Minister's Office has assisted in obtaining copies of Operational Bulletin (OB) PRG-2014-07, Examination of Solicitor-Client Privilege Materials, as well as Chapter 12 of the CBSA Enforcement Manual, which contains a short section on solicitor-client privilege.

OB PRG-2014-07 provides insufficient guidance to CBSA officers on solicitor-client privilege and contains misleading and conflicting information. The CBA Sections continue to recommend the development of a comprehensive, binding policy on solicitor-client privilege that is publicly available on the CBSA website.

The OB instructs CBSA officers to treat documents protected by solicitor-client privilege, electronic or otherwise, with sensitivity. This includes printed documents in a lawyer's or client's possession, printed documents sent by mail or courier, or documents on an electronic device. The CBSA limits the policy to documents clearly marked 'solicitor-client privilege,' addressed to or from a law firm or lawyer's office, or in the possession of a lawyer and the lawyer claims the privilege during the examination process. However, as a matter of law, solicitor-client privilege is applied based on the nature of a document. It must be respected whether or not a document is labelled as such, and whether claimed by a lawyer or their client.

The OB also states that CBSA officers will 'not normally' open materials that meet the criteria for solicitor-client privilege. However, if a CBSA officer has reasonable grounds to believe that a letter, package or electronic device contains more than solicitor-client privileged documents, the CBSA officer may open it to determine admissibility, tariff treatment or the presence of contraband, unreported or falsely reported goods – notwithstanding a claim of

---

43 Canadian Bar Association, *Resolution 13-06-A, Solicitor-Client Privilege Claims at the Canadian Border* (August 17, 2013), available online

44 *See* Canadian Bar Association, Welcome to the Public Safety Portfolio (February 1, 2017), available online

privilege – and documents that the CBSA officer determines are clearly not subject to solicitor-client privilege (such as invoices for purchases) may be seized. This guidance erroneously suggests that the examining CBSA officer can make a determination of privilege. It could also be used to justify a 'fishing expedition' if, for example, the CBSA officer were looking for failure to report a specific good that was being imported.

The OB states that where solicitor-client privilege has been asserted – and the CBSA officer is unable to clearly determine the nature of documents but has reason to believe that the documents contain contraband or evidence of wrongdoing – the CBSA officer should seal the documents in an evidence bag without examining them and set them aside for review by a court to determine privilege. However, the OB fails to outline the process to follow after the documents are placed in the evidence bag.

The CBSA Enforcement Manual gives some additional detail, recommending that the CBSA officer contact Legal Services (or another appropriate section of the CBSA) where privilege is claimed or potentially applicable. CBSA officers are instructed to:

- ensure another officer is available to witness and sign the appropriate form IMM 5242B;
- ensure the client understands and observes the process;
- have the client sign the appropriate form;
- ensure that notification is given to the lawful owner of the documents;
- limit the contamination factor by sealing the item and not allowing others to view or handle the seized items; and
- report procedures on file and/or update the CBSA's Field Operations Support System (FOSS).

The Manual also notes that there are exceptions to solicitor-client privilege, such as when the client seeks guidance from a lawyer in order to facilitate a commission of a fraud or crime. These exceptions could be misinterpreted by CBSA officers. They should be removed from the manual and addressed by a Canadian Court.

Subsection 99(1) of the *Customs Act* allows CBSA to open mailed and couriered packages. Chapter 12 of the Customs Enforcement Manual states that CBSA should 'not normally' open mail and couriered documents (packages that clearly contain only documents) from a law firm or lawyer or being sent to a law firm or lawyer. However, mailed or couriered packages containing solicitor-client privileged documents will be more likely to be subject to examination when the new provisions come into force. More detailed guidance should be

available to CBSA officers and the public, including lawyers, to ensure safeguards are in place to avoid unauthorized access to documents protected by solicitor-client privilege.

RECOMMENDATIONS

2. **The CBA Sections recommend the creation of a working group with representatives from the CBA, Justice Canada and CBSA to collaborate in the development of a defined policy for searches at the Canadian border that involve information protected by solicitor-client privilege.**
3. **The CBA Sections recommend that the CBSA policy clarify that:**
   a. **Information protected by solicitor-client privilege cannot be disclosed without the client's consent or by court order;**
   b. **CBSA officers must respect all claims of solicitor-client privilege, whether made by a lawyer or their client;**
   c. **CBSA officers must follow an expedited procedure to address claims of solicitor-client privilege;**
   d. **Determinations about the applicability of solicitor-client privilege must be made by a Canadian court.**
4. **The CBA Sections recommend that CBSA policy and procedures for claims of solicitor-client privilege be publicly available on the CBSA website.**

IV. CONCLUSION

The CBA Sections appreciate the opportunity to share our views on the privacy of Canadians at airports and borders. While information collection and sharing at the border is necessary to ensure the security of Canadians, collecting and sharing too much information – or information that is incomplete or unreliable – can also lead to harmful consequences for Canadians. An appropriate balance must be achieved to protect our safety and preserve individual privacy rights.

V. SUMMARY OF RECOMMENDATIONS

1. **The CBA Sections recommend that Bill S-7 specify a threshold of "reasonable suspicion", or similarly individualized standard of suspicion, prior to the search of personal electronic devices at international borders. Or, in the alternative, that S-7 be amended to articulate guardrails around "reasonable general concern", such that it can withstand Charter-scrutiny.**

2. **The CBA Sections recommend the creation of a working group with representatives from the CBA, Justice Canada and CBSA to collaborate in the development of a defined policy for searches at the Canadian border that involve information protected by solicitor-client privilege.**

3. **The CBA Sections recommend that the CBSA policy clarify that:**

   a. **Information protected by solicitor-client privilege cannot be disclosed without the client's consent or by court order;**

   b. **CBSA officers must respect all claims of solicitor-client privilege, whether made by a lawyer or their client;**

   c. **CBSA officers must follow an expedited procedure to address claims of solicitor-client privilege;**

   d. **Determinations about the applicability of solicitor-client privilege must be made by a Canadian court.**

4. **The CBA Sections recommend that CBSA policy and procedures for claims of solicitor-client privilege be publicly available on the CBSA website.**