THE CANADIAN BAR ASSOCIATION
L'ASSOCIATION DU BARREAU CANADIEN

Privacy of Canadians at Airports and Borders

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

September 2017

500–865 Carling Avenue, Ottawa, ON, Canada K1S 5S8
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 Canadian Bar Association Privacy and Access Law, Immigration Law, and Commodity Tax, Customs and Trade Law Sections, the Canadian Corporate Counsel Association, and the Ethics and Professional Responsibility Subcommittee with assistance from the Legislation and Law Reform Directorate at the CBA office. The submission has been reviewed by the Legislation and Law Reform Committee and approved as a public statement of the Canadian Bar Association.

TABLE OF CONTENTS

Privacy of Canadians at Airports and Borders

Privacy of Canadians at Airports and Borders

EXECUTIVE SUMMARY

The Privacy and Access Law, Immigration Law, and Commodity Tax, Customs and Trade Law Sections the Canadian Corporate Counsel Association, and the Ethics and Professional Responsibility Subcommittee (the CBA Sections) appreciate the opportunity to appear before the Access to Information, Privacy and Ethics Committee in its study of Privacy at Airports, Borders and Travelling in the United States.

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, disclosure of information collected at the border, and the importance of effective Canada Border Services Agency (CBSA) oversight and accountability mechanisms.

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

Most travellers 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.

The impact of technological advances are magnified through two recent bills – Bill C-21, *An Act to Amend the Customs Act*, and Bill C-23, *Preclearance Act, 2016*, that would increase powers of examination, collection and disclosure at the border. Bill C-21 requires international carriers to collect and hand over detailed biometric information on all travellers departing Canada. The Bill would also significantly expand the role of the CBSA in controlling the exit of goods and people from Canada. Bill C-23 will significantly enhance the powers to foreign officers operating on Canadian soil, reducing the privacy rights of Canadians without adequate safeguards. We recommend full consultations and an extensive review before enacting Bill C-23.

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 continue to recommend the creation of a working group to collaborate on the development of a comprehensive 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.

C. Disclosure of Information Collected at the Border

Information sharing is a significant aspect of privacy protection for Canadians whose information is collected at the border. Even if personal information is collected legally, by appropriate means, and observing relevant privacy protections, significant harm may result if that information is disclosed to, or shared with persons or for purposes that were not contemplated at the time of collection.

The CBA Sections are concerned with increased information sharing, not only between national security and law enforcement agencies, but also between the public and private sectors. We recommend a principled approach to information sharing. Any sharing of personal information collected at the border should be subject to all applicable privacy rules under Canadian law, and effective steps should be taken to ensure application of those rules when information is shared with foreign entities.

D. Effective CBSA Oversight

The CBA Sections continue to urge the federal government to put effective CBSA oversight and complaints mechanisms in place to ensure that national security is balanced with meaningful protection of privacy rights for Canadians at the border.

I. INTRODUCTION

The Privacy and Access Law, Immigration Law, and Commodity Tax, Customs and Trade Law Sections the Canadian Corporate Counsel Association, and the Ethics and Professional Responsibility Subcommittee of the CBA Board (the CBA Sections) appreciate the opportunity to appear before the Access to Information, Privacy and Ethics Committee in its study of Privacy at Airports, Borders and Travelling in the United States.

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, commodity tax, customs and trade law, and of issues relevant to in-house counsel.

The Committee's examination of privacy rights at the border is timely, given rapid advances in technology that enable greatly enhanced gathering and sharing of information about cross-border travellers. The impact of these advances is likely magnified through recent bills that would increase powers of examination, collection and disclosure at the border.

Information collection and sharing at the border is necessary to ensure the security of Canadians. However, 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 between national security and preserving our individual privacy rights and freedoms.

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 the importance of effective oversight and accountability mechanisms.

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

E. Legislative Changes Affecting Privacy Rights at the Border

Parliament is currently considering two Bills – Bill C-21, *An Act to Amend the Customs Act*, and Bill C-23, *Preclearance Act, 2016* – which would significantly expand the powers of Canadian and US Customs and Immigration authorities to examine travellers and to gather, store and share their personal information[1].

Bill C-21 – An Act to Amend the Customs Act

Bill C-21 amends the *Customs Act*, to implement the Beyond the Border (BTB) initiative between Canada and the US.[2]

The BTB agreement includes a commitment to implement a biographic entry and exit information exchange. It compels international carriers to collect and hand over detailed biometric information on all travellers departing Canada. Section 92 of the Bill will allow the collection of information on persons leaving Canada or who have left Canada – including biographical information, passport and other travel document information, and date and place of entry. Even though this change flows from the BTB initiative, with the exception of arrival information, it will not be limited to persons entering the US – it will apply to all persons leaving Canada, no matter where to or by what means. The Bill will enable regulations (as yet undisclosed) to specify the sources, timing and nature of information required.

The Bill would also massively expand the role of the Canada Border Services Agency (CBSA) in controlling the exit of goods and people from Canada. The current *Customs Act* does not require travellers leaving Canada to submit to examination by CBSA officers, except for the limited purpose of controlling export of funds.[3] Proposed section 94 of the Act, set out in section 2 of the Bill will require every person leaving Canada to present themselves to an officer if requested to do so, and, "*to answer truthfully any questions asked of them by an officer in the performance of their duties under this or any other Act of Parliament.*" This will give officers the same powers to examine goods and persons leaving Canada as they do on entry. While this section was apparently intended to give officers powers to search shipping containers to catch illegal exports, it has no limitations, and would therefore permit examination and searches of all goods and persons leaving Canada.

The Bill also raises concerns about how collected information will be shared with other government agencies in Canada, foreign governments and the private sector. Although this information sharing will be primarily for customs, immigration and national security purposes, it will be tempting for other government agencies to access and mine the stored data for other purposes.

---

1 Bill C-21, *An Act to amend the Customs Act,* 42nd Parliament, 1st Session, available online (http://ow.ly/DeIC30fkLOBg). Bill C-23, *Preclearance Act, 2016,* 42nd Parliament, 1st Session, available online (http://ow.ly/UmAu30fkLPB). *Customs Act, R.S.C., 1985, c. 1 (2nd Supp.),* available online (http://ow.ly/ddhB30fkLQB).

2 *Declaration on a Shared Vision for Perimeter Security and Economic Competitiveness,* available online (http://ow.ly/S05P30fkLS3).

3 *See Proceeds of Crime (Money Laundering) and Terrorist Financing Act,* R.S.C. 2000, c. 17 (at section 12), available online (http://laws-lois.justice.gc.ca/eng/acts/p-24.501/).

Information exchanged with the US through amendments to the *Customs Act* set out in this Bill will have serious privacy implications for travellers. Shared information may affect the future ability of Canadians to travel, work or study in the US. Canadians who travel abroad may also encounter tax or immigration problems in the US. Past experience has also shown that information sharing by the Canadian government can have devastating consequences, particularly where the information is inaccurate or unreliable, as illustrated through the experience of Maher Arar.[4]

RECOMMENDATION

1. **The CBA Sections recommend that, once Bill C-21 is enacted, Parliament subject the legislation to regular review to ensure the letter and the spirit of Canada's *Privacy Act* are respected.**

Bill C-23 – Preclearance Act, 2016

Bill C-23 implements the *Agreement on Land, Rail, Marine, and Air Transport Preclearance* between Canada and the US (the Preclearance Agreement). It will grant significantly enhanced powers to foreign officers operating on Canadian soil, reducing the privacy rights of Canadians and other travellers on Canadian soil who will be subject to these powers, without adequate safeguards. The CBA Immigration Law Section's March 2017 submission on Bill C-23 to the Standing Committee on Public Safety and National Security is attached as Appendix A, and endorsed by the CBA Sections.[5] We repeat the recommendations for your ease of reference.

This agreement was negotiated when both Canada and the US were represented by different leaders and governments, with substantially different approaches and agendas. Those differences warrant a re-examination of the scope and content of the agreement and this draft legislation that flows from it. Several recent developments give rise to serious concerns about how the significantly expanded powers of US officers operating on Canadian soil could be exercised.

Withdrawing from Preclearance

Sections 18 and 30 of Bill C-23 set out a traveller's obligations and ability to withdraw from US or Canadian preclearance. They represent a substantial change from the current *Preclearance Act*, which gives travellers an unqualified right to choose to withdraw from a US preclearance area, terminating their examination.[6] A traveller's ability to withdraw from a US preclearance area is an essential right that should be subject only to the restriction that there is no allegation of an offence. This approach recognizes that the traveller is on Canadian soil, and entitled to minimal restrictions on freedom of movement.

While it is recognized that US authorities are entitled to pose reasonable enquiries to travellers seeking entry to the United States, the intrusiveness of the examination is certainly of concern –

---

4 Commissioner Dennis O'Connor, *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar* (September, 2006), available online (http://ow.ly/oywQ30fkLUf) 1.

5 Canadian Bar Association, *Bill C-23 - Preclearance Act 2016* (March 27, 2017), available online (http://ow.ly/VVgT30fkLWu).

6 *Pre-Clearance Act, S.C. 1999, c. 20*, available online (http://ow.ly/3fYA30fkLZL).

particularly when the traveller is compelled to remain in an examination to provide and be questioned about their reasons for wishing to withdraw.

Any law conferring discretion to detain without express or implied criteria governing its exercise is an arbitrary law.[7] The right to withdraw is meaningless without restrictions on the questions a traveller may be asked, and the length of time the traveller may be subjected to questioning. The proposed wording would allow US preclearance officers to engage in 'fishing expeditions', asking intrusive questions about the person's political or religious views, past behavior and associations - all in the name of questioning them about their reasons for withdrawing.

The manner in which a traveller meets his or her obligation to provide the reasons for withdrawal should be addressed specifically. For example, a traveller withdrawing an application for entry to the United States could satisfy this obligation by providing their reasons for withdrawal in a written statement.

The vague obligation under subsection 31(3) to avoid unreasonable delay for withdrawal provides insufficient protection. Travellers who believe their questioning is overly intrusive, lengthy or unjustified would have no remedy except to refuse to answer questions or walk away. At that point, they would face arrest, detention, and a possible charge under this Act, for not complying with section 30 (answering truthfully any question asked by a US preclearance officer) or section 38 (obstructing or resisting a US preclearance officer).

Travellers might also face US immigration consequences for withdrawing when directed not to do so by a preclearance officer. They would also have no recourse under Canadian law to challenge a US preclearance officer who exceeded powers granted by Canadian law. US preclearance officers would be virtually unaccountable, as section 40 of the bill exempts their decisions from judicial review in Canada, section 39 makes them exempt from civil liability, and section 42 permits the US to bar their extradition to Canada.

Strip Searches

A US preclearance officer's authority to conduct a strip search under section 22 of Bill C-23 is a dramatic departure from the current Preclearance Act, which requires that all strip searches in preclearance areas be conducted by Canadian officers. While the Bill seemingly includes this requirement, subsection 22(4) undermines the intent of section 22 by allowing US preclearance officers to conduct invasive strip searches where a CBSA officer is unavailable, unwilling or does not appear in time.

If a Canadian officer applying Canadian standards on Canadian soil concludes that a strip search is not justified, a US officer would legally be permitted to ignore that determination and conduct a strip search anyway. It is unacceptable that a strip search by a US preclearance officer could be conducted in a preclearance process without the involvement of a Canadian border services officer. The CBA Sections recommend that a strip search should only occur upon mutual agreement of the US and Canadian officers as to its need, and should be conducted by or under the direction of the Canadian officer.

Even though Bill C-23 would require US preclearance officers to exercise their powers and perform their duties and functions – including executing searches – in accordance with Canadian law (including the *Canadian Charter of Rights and Freedoms*), it is problematic to authorize US

---

7 *Regina v. Hufsky*, [1988] 1 S.C.R. 621, available online (http://ow.ly/bsZi30fkM1k).

preclearance officers to perform invasive searches on Canadian soil.[8] US preclearance officers are unfamiliar with Canadian law enforcement methods, and poorly positioned to apply Canadian law. They are more likely to inadvertently breach constitutional rights of Canadian citizens, and are virtually unaccountable for violating Canadian law. Ensuring that these searches, which constitute detentions, are conducted under the protection of Canadian law is particularly important for vulnerable groups, such as minors, and lesbian, gay, bisexual, transgender and two-spirited individuals.

Section 25 of the Bill gives a traveller the right to be taken before a CBSA officer or US preclearance officer's senior officer before a strip search is conducted; however it is unclear what role the senior officer plays in this process. In subsection 25(2), a search is only permitted if the senior officer agrees that, "*the preclearance officer or border services officer, as the case may be, is authorized under the applicable section to conduct the search*." The senior officer is not required or entitled to undertake a substantive review of the merits of the search, including the reasonable grounds on which the decision was made by the preclearance officer or border services officer. The section affords no additional rights to travellers, and legal advice would be difficult to obtain in the context of these searches.

RECOMMENDATIONS

2. **The CBA Sections recommend that the government engage in full consultations and an extensive review before enacting Bill C-23, which is so highly intrusive on privacy rights and personal liberties.**

3. **The CBA Sections recommend that Bill C-23 be amended to impose strict limits on questioning a traveller for the purposes of Section 30, to ensure Charter compliance. This could be achieved by replacing the power to question the traveller on the reasons for withdrawal with a requirement that they provide a brief written explanation of their reasons for withdrawal, which would fully satisfy the obligation.**

4. **The CBA Sections recommend that Bill C-23 be amended to include a requirement that strip searches in preclearance areas be conducted only by Canadian officers.**

5. **The CBA Sections recommend that subsection 22(4) of Bill C-23, which would allow preclearance officers to conduct invasive strip searches where a CBSA officer is unavailable, unwilling or does not appear in time, be deleted.**

6. **The CBA Sections recommend that senior officers be given discretion under Section 25 to direct that a strip search not be conducted where the senior**

---

8 *Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, Schedule B to the Canada Act, 1082 (UK)*, 1982, c 11, available online (http://ow.ly/FCkV30fkM2K).

officer determines that that there are insufficient circumstances to warrant such an invasive act.

F. Searches of Electronic Devices

Most travellers now carry mobile electronic devices like smartphones tablets and laptops, with sensitive personal data. As airlines have moved to electronic ticketing and boarding passes – along with electronic notices about delayed flights – the devices have become increasingly indispensable in travel. This calls for a reexamination of the powers of customs agents to inspect the contents of these devices.

At one time, Canadians stored their most private information in physical records in their homes. When travelling, they might have filled 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.[9] 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".[10]

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 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.[11] For example, in *R v Fearon*, 2014 SCC 77, the Supreme Court modified the common law rule related to search incident to arrest for smartphones specifically due to the immense privacy implications in searching the device.[12] The Supreme Court has clearly established that the greater the intrusion on privacy, the greater the constitutional protections and a greater justification is required. And while there may be a diminished expectation of privacy at the border, this expectation is not completely

---

9 *See for example,* Canadian Press, *Smartphone Use Way Up in Canada, Google Finds*, available online (http://ow.ly/157330fkM4y). This trend has attracted US judicial commentary, see for example, *Riley v. California*, 134 S. Ct. 2473 (2014), available online (http://ow.ly/lYje30fkM5k), 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."*

10 *See R. v Simmons,* [1988] 2 SCR 495, available online (http://ow.ly/kNqt30fkM6C), 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.

11 *R v Vu*, 2013 SCC 60, available online (http://ow.ly/4xeb30fkM9G). *See also, R v Morelli*, 2010 SCC 8, available online (https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/7847/index.do).

12 *R v Fearon*, 2014 SCC 77, available online (http://ow.ly/Gr7Y30fkMbr).

extinguished.[13] There is still an expectation of privacy, particularly when dealing with electronic devices that inherently attract significant privacy interests.[14]

Taken together, these point for a need to re-examine any rule or law that would permit warrantless searches of these devices. These devices may provide access to information that is in no meaningful sense 'at' the location of a search. The *Customs Act* has not been updated to reflect modern Canadian views on our advancing technologies, and it is now up to Parliament to weigh in.

Recently, the Privacy Commissioner of Canada announced an investigation of CBSA practices of searching electronic devices.[15] CBSA policies and practices related to suspicionless searches have also come under increasing scrutiny by the media, reflecting the concerns of Canadians.[16] Commissioner Therrien 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 Bill C-23,[17] making the following important observations:

> The fundamental problem with groundless searches of electronic devices is that these searches do not recognize that they are extremely privacy intrusive. Yet Bill C-23 recognizes the sensitivity of other searches, namely searches of persons, from the relatively un-intrusive frisk or pat-down searches to the more intrusive strip and body cavity searches. These searches legally cannot be performed unless an officer has reasonable grounds to suspect some legal contravention, notably the concealment of goods. In my view, it is extremely clear that searches of electronic devices can generally be much more intrusive than frisk searches, for electronic devices can contain the most personal and intimate information we hold… The idea that electronic devices should be considered as mere goods and therefore subject to border searches without legal grounds is clearly outdated and does not reflect the realities of modern technology. Border controls are important and legitimate for reasons of sovereignty and public safety, but they should not be exercised arbitrarily.

G. Information Stored on an Electronic Device is not a 'Good'

The *Customs Act* is an analog statute. When Parliament considered the Act in the 1980s, digital smartphones were unlikely imagined. The Act has no provisions applying specifically to electronic storage or devices.

---

13 *Supra* note 9 (*Simmons*). *See also R v Nagle,* 2012 BCCA 373, available online (http://canlii.ca/t/fss1c).

14 *R v Cole,* 2012 SCC 53, available online (http://canlii.ca/t/ft969). 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.

15 Marie-Danielle Smith, *Privacy commissioner investigating Canada Border Services Agency over electronic media searches, National Post* (15 March 2017), available online (http://ow.ly/tYhg30fkMcP).

16 *See, for example*, Matthew Braga, Canadian Broadcasting Corporation, *What happens when a Canadian border agent asks to search your phone*? (March 2017), available online (http://ow.ly/KTfg30fkMf2). See also, Sue Bailey, *Border phone search raises privacy, charter issues, say lawyers*, *The Canadian Press* (17 August 2016), available online (http://ow.ly/N1hS30fkMgI).

17 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 (http://ow.ly/CqVT30fkMio).

When a traveller carries an electronic device across the Canadian border, the physical phone is obviously a 'good' that is 'imported' into Canada. The word 'good' is defined in the Customs Act to include luggage and 'any document in any form'. The CBSA interprets the word 'document' to include an electronic document, which can be examined with grounds or a warrant. However, the Act has no application to electronic information in or accessible through an electronic device.

Parliament clearly intended to treat mail differently from 'goods.' The *Customs Act* drew a clear distinction between *goods* crossing the border, and the *content* of private correspondence (which attracts heightened privacy protection) crossing the border. Subsection 99(1)(a) permits a customs official to examine any goods and open and examine any package or container of goods imported into Canada without grounds or a warrant. Subsection 99(1)(b) creates different rules for mail imported into Canada. While customs officers may examine a *physical envelope* without grounds or a warrant, they are prohibited from *opening* the envelope absent reasonable grounds to believe the envelope contains a regulated, controlled or prohibited substance. There is no authority in the *Customs Act* to review the information itself.

The mail provisions of the Act were enacted following the Royal Commission of Inquiry into Certain Activities of the RCMP (the McDonald Commission), which looked at (among other things), the police practice of opening Canadians' mail. The McDonald Commission Report concluded that, "*no customs personnel should be allowed to read or divulge any correspondence contained in sealed mail.*"[18] Crossing the border with an electronic device is akin to crossing the border with every piece of mail a traveller has ever sent or received. It would not be unreasonable to expect the information stored in an electronic device to attract even greater protection than a single physical envelope containing a single written letter.

If Parliament had intended the *Customs Act* to capture searches of these communications, it would have done so. To illustrate this point, it recently amended the *Customs Act* to extend customs agents' right to search mail 30 g or less for contraband by repealing subsections 99(2) and (3), but explicitly did not alter the language in subsection 99(1) that creates this distinction between mail and other goods.[19]

Applying the Customs Act to electronic data is unconstitutional

Any interpretation of the *Customs Act* that would authorize a warrantless search of the data stored on an electronic device (or require an individual to disclose a password) would implicate sections 7and 8 of the *Charter*, and would likely be found to be unconstitutional.

The privacy interests in electronic devices are so high that the lowered expectation of privacy rights at the border does not sufficiently counterbalance those interests. A number of cases on electronic device searches at border crossings have improperly focused on the quantity of information these devices possess in drawing comparisons with other storage containers like briefcases or luggage. It is equally important to consider that these devices contain a wide variety of *types* of information in any analysis.

---

18 Royal Commission of Inquiry into Certain Activities of the RCMP, *Report of the Royal Commission of Inquiry into Certain Activities of the RCMP*, available online (http://ow.ly/gKBS30fkO8X). The Commission also relates an interesting history of Canada Customs stretching the then-existing laws to the limit in order to inspect correspondence (at p.140).

19 *An Act to amend the Controlled Drugs and Substances Act and to make related amendments to other Acts,* R.S.C. 2017, c. 7. (formerly Bill C-37), available online (http://ow.ly/rtFP30fkObh).

In *R v Vu*, the Supreme Court found that a search with a warrant had to exclude a computer found on those premises because of the acute privacy interests engaged by these devices.[20] 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. Given this decision, it would be illogical to suggest that customs agents could rely on the general provisions of the *Customs Act* (which refer only to 'goods') to do exactly that.

Immeasurable amounts of electronic information stream in and out of Canada through fiber optic cables without any degree of scrutiny by CBSA. Any review of this information without a warrant would be unconstitutional under the *Charter*, and no court would issue a warrant for wholesale fishing expeditions of it. How can information stored on an electronic device carried by a traveller be any different? The inevitable conclusion is that a warrant or other judicial approval must be obtained prior to examining the information contained in or accessed through an electronic device at the border.

RECOMMENDATIONS

7. **The CBA Sections recommend that the *Customs Act* be updated to clarify that information stored on or accessed through electronic devices and cloud storage services does not constitute a 'good' as defined in the Act. Any interpretation of the Customs Act that would authorize a warrantless search of the data stored on an electronic device (or require an individual to disclose a password) would implicate sections 7and 8 of the Charter, and would likely be found to be unconstitutional.**

III. SOLICITOR-CLIENT PRIVILEGE AT THE BORDER

Solicitor-client privilege is fundamental to the proper functioning of the Canadian legal system.[21] 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.[22] Information protected by solicitor-client privilege cannot be disclosed without the client's consent or a court order. The Supreme Court of Canada has repeatedly emphasized that the privilege must remain "as close to absolute as possible and should not be interfered with unless absolutely necessary."[23] In the rare case of

---

20 *Supra* note 10 (*Vu*).

21 *Blood Tribe Department of Health v. Attorney General of Canada et. al., [2008] 2 S.C.R. 574,* available online (http://ow.ly/iYYi30fkMwp). *See also* Canadian Bar Association, *Solicitor-Client Privilege at the Canada-US Border (June 19, 2014), available online* (http://ow.ly/kGlc30fkMxu).

22 *Andrews v. Law Society of British Columbia*, [1989] 1 S.C.R. 143, available online (http://ow.ly/fktH30fkMAt).

23 *See most recently, Alberta (Information and Privacy Commissioner) v. University of Calgary,* 2016 SCC 53, available online (http://ow.ly/6bNl30fkMCg).

necessity, there must be explicit statutory authorization accompanied by legislated safeguards to ensure that disclosure does not compromise the substantive right.[24]

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 device (and the client information it contains) under examination may be necessary to meet important filing deadlines, and loss of access over an extended period could have serious consequences.

No specific provision in the *Customs Act* or regulations deals with solicitor-client privilege, and there is some concern that CBSA might apply section 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 section 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.[25] Lawyers in this situation are bound by their obligations to their client(s) 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.[26] CBSA decision-makers must also act fairly, especially when the impact of their decisions is substantial, such as handling documents and electronic devices where solicitor-client privilege is claimed.[27] 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* (which would be amended by Bill C-23). 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.

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.[28]

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.[29] This policy guidance was developed without input from or notification to the CBA. Since then, the Minister's

---

24 *Canada (Attorney General) v. Chambre des notaires du Québec,* 2016 SCC 20, available online (http://ow.ly/3asH30fkMDq).

25 *See* Mark Gollom, CBC News, *Alain Philippon phone password case: Powers of border agents and police differ* (March 6, 2015), available online (http://ow.ly/UnSd30frEPj).

26 *Attorney General of Canada v. Bri-Chem Supply Ltd.*, 2016 FCA 257, available online (http://ow.ly/dAQK30fkMGn).

27 *Luking v. Minister of Public Safety an Emergency Preparedness, 2013 FC 222,* available online (http://ow.ly/9zUz30fkMHt).

28 Canadian Bar Association, *Resolution 13-06-A, Solicitor-Client Privilege Claims at the Canadian Border* (August 17, 2013), available online (http://ow.ly/eoaj30fkMIW).

29 *See* Canadian Bar Association, Welcome to the Public Safety Portfolio (February 1, 2017), available online (http://ow.ly/UeYa30fkMKX).

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 also 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 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 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 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 provides 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 more appropriately on a case-by-case basis through advice from CBSA Legal Services.

Subsection 99(1) of the *Customs Act* allows CBSA to open mailed and couriered package, but subsections 99(2) and (3) currently exempt packages or letters that weigh less than 30 grams. These sections will be repealed when amendments in R.S.C. 2017, c. 7 (formerly Bill C-37) come into force.[30] 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

8. **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.**
9. **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.**
10. **The CBA Sections recommend that CBSA policy and procedures for claims of solicitor-client privilege be publicly available on the CBSA website.**
11. **The CBA Sections recommend that the federal government require the US Department of Homeland Security (and US CBP) to have a policy on**

30 *An Act to amend the Controlled Drugs and Substances Act and to make related amendments to other Acts,* R.S.C. 2017, c. 7, Royal Assent May 18, 2017, available online (http://ow.ly/3rDB30fkMN9).

solicitor-client privilege that is applicable to preclearance examinations on Canadian territory.

IV. DISCLOSURE OF INFORMATION COLLECTED AT THE BORDER

Information sharing is a significant aspect of privacy protection for Canadians whose information is collected at the border. Even if personal information is collected legally, by appropriate means, and observing relevant privacy protections, significant harm may result if that information is disclosed to, or shared with persons or for purposes that were not contemplated at the time of collection.

The CBA Sections are concerned with increased information sharing, not only between national security and law enforcement agencies, but also between the public and private sectors. Information sharing by government institutions should be designed to fulfil specific, narrow purposes, one of which includes the protection of Canada from activities that undermine its security as contemplated in the *Security of Canada Information Sharing Act* (SCISA).[31]

A. A Principled Approach to Information Sharing

The CBA comments to the Committee in its study of SCISA addressed balanced information sharing, restrictions on subsequent use and disclosure of shared information, and additional checks and balances.[32] We supported the guiding principles in section 4 of SCISA, which should apply to sharing information collected at the border, whether domestically or with foreign entities:

(i) effective and responsible information sharing protects Canada and Canadians;

(ii) respect for caveats on and originator control over shared information is consistent with effective and responsible information sharing;

(iii) entry into information sharing arrangements where Government of Canada institutions share information regularly;

(iv) the provision of feedback as to how shared information is used and as to whether it is useful in protecting against activities that undermine the security of Canada facilitates effective and responsible information sharing;

(v) only those within an institution who exercise its jurisdiction or carry out its responsibilities in respect of activities directly related to the purpose of the sharing ought to receive information that is disclosed under the relevant legislation.

In 2008, the CBA also commented to the government on cross-border law enforcement initiatives, with particular reference to Canada-US arrangements.[33] These initiatives have

---

31 *Security of Canadians Information Sharing Act,* R.S.C. 2015, c. 20, s. 2, available online (http://ow.ly/RgRF30fkMQ1).

32 *Canadian Bar Association, Security of Canadians Information Sharing Act (SCISA) (*January 2017), available online (http://ow.ly/PiwJ30fkMSj).

33 *See for example,* Canadian Bar Association, *Framework for Integrated Cross-Border Law Enforcement Initiatives* (September 2008), available online (http://ow.ly/dCff30fkMWj).

received heightened focus since the events of 9/11, and in particular, have taken the form of the BTB law enforcement initiative entered into by Canada and the US in December 2012.

We recommended a principled framework, which has advantages over what was then recognized as an *ad hoc* approach. We continue to support the application of this type of framework to any sharing of information with foreign entities, and specifically to personal information collected at the border.

This framework would provide a vehicle to ensure that fundamental principles are respected, adherence to Canadian laws and values are enshrined and consequences are required for any breach. It would need to stress the exceptional nature of any such transnational enforcement efforts, and be founded on certain core principles including:

(i) adherence to the Canadian Charter of Rights and Freedoms;

(ii) adherence to all applicable customary and conventional international law, rules of accountability, transparency, oversight and solicitor/client privilege, and respect for Canadian autonomy;

(iii) ensuring that privacy protection afforded in Canada continues to apply when Canada shares information to a foreign government; and

(iv) transparency when breaches of the framework agreement that are contrary to the values of Canadians occur and those responsible must be held to account.

The framework should also describe the nature and scope of information-sharing, with precise definitions and clear limitations on the scope and purposes for sharing, as well as effective safeguards to ensure that shared information is reliable. It should also set clear lines of accountability for handling and security of information shared between agencies, such as clear and enforceable restrictions on subsequent use and disclosure of information by the recipient agency to third parties (including other law enforcement agencies).

The parties to the framework should agree to respect all domestic and applicable international customary and conventional law in arrangements made and activities carried out under the framework agreement. Specifically, any proposal related to cross-border law enforcement must be very carefully scrutinized to ensure that it accords with the letter and spirit of Canadian privacy legislation, including the *Privacy Act* and the *Access to Information Act*.[34] Any records created under the framework – regardless of where they are located – should be subject to these acts, along with the comparable US legislation. Finally, all information systems, filing systems registries, and the like, should be subject to a comprehensive privacy impact assessment.

B. Privacy Principles for Information Sharing by Government Entities

Information sharing between government institutions must be done in accordance with applicable Canadian laws. The basic privacy principles applicable to disclosure of personal information by federal government institutions are in the *Charter, Privacy Act* and SCISA (which has significantly expanded intra-governmental information sharing for national security purposes in Canada).

---

34 *Privacy Act,* R.S.C., 1985, c. P-21, available online (http://laws.justice.gc.ca/eng/acts/p-21/). *See also, Access to Information Act,* R.S.C., available online (http://laws.justice.gc.ca/eng/acts/A-1/).

Generally, information may be disclosed by an institution for the purpose for which it was collected by the institution, or for a use consistent with that purpose, or for any other purpose in accordance with an act of Parliament or regulation that authorizes its disclosure. This means that if disclosure of personal information to another Canadian institution or to a foreign entity was contemplated as one of the purposes for collection at the time of initial collection, then disclosure would be permitted, absent any other restrictions or rules that may apply. Sharing information for purposes not contemplated at the initial collection stage requires specific statutory authorization, unless consent is obtained from the individual to whom it relates. SCISA is an example of a statute that addresses such a requirement.

This rule subsumes the premise that the disclosing institution was authorized to collect the personal information in the first place because: it related directly to an operating program or activity of the institution; and the individual from whom it is collected has been informed of the purpose for which the information is collected. Likewise, the information disclosed must be directly relevant to the recipient institution's mandate.

The *Privacy Act* stipulates other specific permitted purposes for disclosure, such as complying with a subpoena or court order, use in legal proceedings or to a prescribed investigative body. Disclosure may also be permitted through a patchwork of other sector-specific legislation and inter-agency information sharing arrangements. If none of these permissions or exceptions apply, the collecting institution must obtain the consent of an individual to share their personal information prior to its disclosure to another government entity.

C. Specific Applications of Information Sharing

Information sharing by CBSA with other federal departments is governed by the *Customs Act,* which specifies limits for the use and disclosure of information collected by the agency. Information sharing by Citizenship and Immigration Canada (CIC) is governed by several inter-agency agreements and arrangements that permit sharing a wide range of personal information by officials administering and enforcing Canada's citizenship and immigration programs. The personal information that can be shared varies under the terms of each arrangement and agreement, but is restricted to the information needed to advance specified program objectives.

The BTB initiative focused on enhancing security of the North American perimeter. It provides for the exchange of biographical data collected for all third country nationals (including landed immigrants) on entry or exit from either Canada or the US. This arrangement is subject to the *Beyond the Border Action Plan Statement of Privacy Principles by the United States and Canada.*[35] Initiatives are underway to extend the scope of cross-border law enforcement initiatives to apply to citizens of both countries, but to date these have not been put in place.

In 2013, CIC undertook a privacy impact assessment (PIA) to ensure that the BTB arrangements complied with Canadian privacy requirements, including the *Privacy Act*. This PIA concluded that the BTB arrangements contained obligations consistent with the *Charter,* the *Privacy Act* and the *Statement of Privacy Principles*. It identified certain privacy risks to be mitigated or eliminated prior to implementation, focusing primarily on completing procedural documentation – including information threat and risk analyses, security procedures and access to information procedures. CIC and CBSA indicated their intent to implement all the recommendations identified in the PIA prior to the commencement of information-sharing.

---

35 *Beyond the Border Action Plan Statement of Privacy Principles by the United States and Canada* (May 30, 2012), available online (http://ow.ly/Nz3330fkN0g).

D. End-to-end Privacy Protection for Information Collected at the Border

The CBA Sections recommend a comprehensive, principled approach to address sharing of all personal information collected at the border, encompassing the guiding principles in SCISA, as well as the recommendations in the CBA's 2008 submission on cross-border law enforcement initiatives. This approach would ensure end-to-end protection for this information, including built-in safeguards for sharing with third parties, restrictions of subsequent use and disclosure, appropriate penalty or remedial provisions, and an effective oversight mechanism.

RECOMMENDATIONS

12. The CBA Sections recommend that any sharing of personal information at the border be subject to all applicable privacy rules under Canadian law and that steps be taken to ensure application of those rules when information is shared with foreign entities.

13. The CBA Sections recommend that appropriate oversight mechanisms be adopted to ensure compliance with privacy rules and full accountability when breaches occur.

E. Private Sector Information Shared with Law Enforcement

While there is little public discussion of this phenomenon, criminal law lawyers are aware that law enforcement routinely obtain access to flight manifest information for routine policing purposes without a warrant or a production order.

These practices were described in a 2008 Nova Scotia case, *R. v. Chehil*, in which a police officer reviewed the manifest for a domestic Westjet flight from Vancouver to Halifax with the airline's permission, but without a warrant or the permission of any passengers.[36] Based on the officer's evidence, these practices appeared to have become routine over time. The court noted that private sector entities are subject to privacy laws that limit what information they can voluntarily provide to law enforcement.

The CBA Sections recommend that any systemic sharing of information between private sector operators and government agencies be subject to strict tests of necessity, and preferably rooted in statute and regulation, such as in the *Secure Air Travel Act*.[37] In our recent submission on SCISA, we recommended that subsequent disclosures to the private sector (and foreign governments) under the Act be prohibited.

---

36 *R. v. Chehil*, 2008 NSSC 357, available online (http://canlii.ca/t/224d2), overturned in *R. v. Chehil*, 2009 NSCA 111, available online (http://canlii.ca/t/224d2). The subsequent Supreme Court decision in *R. v. Spencer*, [2014] 2 SCR 212, 2014 SCC 43, available online (http://ow.ly/dTda30fkN34) may limit the precedential value of the Nova Scotia Court of Appeal's decision.

37 *Secure Air Travel Act*, SC 2015, c 20, s 11, available online, (http://ow.ly/NhFX30fkN6h).

RECOMMENDATION

14. The CBA Sections recommend that any systemic sharing of information between private sector operators and government agencies be subject to strict tests of necessity, authorized by statute and regulation and, if not authorized by statute, require a warrant or court order.

V. EFFECTIVE OVERSIGHT OF CBSA

Accountability and transparency have been recurring themes in studies and commissions, as well as in past CBA submissions on national security issues in Canada.[38] Robust accountability mechanisms are crucial to the legitimacy and efficacy of our national security agencies, as well as to public confidence in them. They help to ensure that problematic issues are eventually exposed and appropriately addressed.

The CBA Sections continue to urge the federal government to put effective CBSA oversight and complaints mechanisms in place to ensure that security is balanced with meaningful protection of privacy rights for Canadians at the border. This oversight –particularly important in the search and information sharing context – could be achieved through a number of models in the national security framework, as noted in our past submissions.

Given the current realities of broad information-sharing and coordinated action by several agencies, certain elements are essential for these models to be effective. There must be robust expert review at the agency level – by an independent agency with a mandate at least as broad as the CBSA itself, with the appropriate resources and level of expertise necessary to review any CBSA's activities. There should also be effective cooperation between the national security review bodies, particularly where agencies work jointly or share information, and a higher level review of the national security infrastructure as a whole to address systemic issues in a coherent and consistent way.

Finally, there are limits as to when improperly obtained information derived from an unauthorized or unlawful examination at the border can be retained. Any information obtained through an illegal or unauthorized practice should not be retained by a government authority. It would be prudent for CBSA to develop a transparent process for travellers to challenge the appropriateness of methodology for collecting information about them at the border. When it is determined that a traveller's information has been improperly obtained, this information should be expunged from all government databases.

RECOMMENDATIONS

15. The CBA Sections recommend that the federal government put effective CBSA oversight and complaints mechanisms in place to ensure that national

---

38 Canadian Bar Association, *Our Security our Rights: National Security Green Paper, 2016* (December 20, 2016), available online (http://ow.ly/WJvH30cqK6W). *See also,* Canadian Bar Association, *Welcome to the Public Safety Portfolio* (February 01, 2016), available online (http://ow.ly/MF7E30fkN8v). *See also,* Canadian Bar Association, *New National Immigration Detention Framework* (June 2017), available online (http://ow.ly/lOKa30fkNah).

security is balanced with meaningful protection of privacy rights for Canadians at the border.

16. **The CBA Sections recommend that the CBSA oversight model incorporate essential elements including robust review at an agency level, effective cooperation between the national review bodies, and a higher level review of the national security infrastructure as a whole.**

17. **The CBA Sections recommend that CBSA develop a transparent process for travellers to challenge the appropriateness of methodology for collecting information about them at the border. Improperly obtained information should be expunged from all government databases.**

VI. 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.

VII. SUMMARY OF RECOMMENDATIONS

The CBA Sections recommend that:

1. **once Bill C-21 is enacted, Parliament subject the legislation to regular review to ensure the letter and the spirit of Canada's *Privacy Act* are respected.**

2. **the government engage in full consultations and an extensive review before enacting Bill C-23, which is so highly intrusive on privacy rights and personal liberties.**

3. **Bill C-23 be amended to impose strict limits on questioning a traveller for the purposes of Section 30, to ensure Charter compliance. This could be achieved by replacing the power to question the traveller on the reasons for withdrawal with a requirement that they provide a brief written explanation of their reasons for withdrawal, which would fully satisfy the obligation.**

4. **Bill C-23 be amended to include a requirement that strip searches in preclearance areas be conducted only by Canadian officers.**
5. **subsection 22(4) of Bill C-23, which would allow preclearance officers to conduct invasive strip searches where a CBSA officer is unavailable, unwilling or does not appear in time, be deleted.**
6. **senior officers be given discretion under Section 25 to direct that a strip search not be conducted where the senior officer determines that that there are insufficient circumstances to warrant such an invasive act.**
7. **the *Customs Act* be updated to clarify that information stored on or accessed through electronic devices and cloud storage services does not constitute a 'good' as defined in the Act. Any interpretation of the Customs Act that would authorize a warrantless search of the data stored on an electronic device (or require an individual to disclose a password) would implicate sections 7and 8 of the Charter, and would likely be found to be unconstitutional.**
8. **a working group with representatives from the CBA, Justice Canada and CBSA be created to collaborate in the development of a defined policy for searches at the Canadian border that involve information protected by solicitor-client privilege.**
9. **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.**
10. **CBSA policy and procedures for claims of solicitor-client privilege be publicly available on the CBSA website.**

11. **the federal government require the US Department of Homeland Security (and US CBP) to have a policy on solicitor-client privilege that is applicable to preclearance examinations on Canadian territory.**
12. **any sharing of personal information at the border be subject to all applicable privacy rules under Canadian law and that steps be taken to ensure application of those rules when information is shared with foreign entities.**
13. **appropriate oversight mechanisms be adopted to ensure compliance with privacy rules and full accountability when breaches occur.**
14. **any systemic sharing of information between private sector operators and government agencies be subject to strict tests of necessity, authorized by statute and regulation and, if not authorized by statute, require a warrant or court order.**
15. **the federal government put effective CBSA oversight and complaints mechanisms in place to ensure that national security is balanced with meaningful protection of privacy rights for Canadians at the border.**
16. **the CBSA oversight model incorporate essential elements including robust review at an agency level, effective cooperation between the national review bodies, and a higher level review of the national security infrastructure as a whole.**
17. **CBSA develop a transparent process for travellers to challenge the appropriateness of methodology for collecting information about them at the border. Improperly obtained information should be expunged from all government databases.**