Federation of Law Societies of Canada

Fédération des ordres professionnels de juristes du Canada

Crossing the Border with Electronic Devices: What Canadian Legal Professionals Should Know

Prepared by the

Policy Counsel Counterpart Group

December 14, 2018

World Exchange Plaza 1810 - 45 O'Connor Street Ottawa Ontario K1P 1A4
Tel: 613.236.7272 Fax: 613.236.7233 www.flsc.ca

Crossing the Border with Electronic Devices: What Canadian Legal Professionals Should Know

With travellers at Canadian airports and border crossings subject to increasing scrutiny,[1] it is important for lawyers and Quebec notaries to have an understanding of how the privacy interests of their clients may be impacted by legislation and policies developed to address public safety issues. Legal counsel should also understand that their profession does not make them immune to policies and processes that could impact information otherwise subject to solicitor-client privilege.

Canadian lawyers and Quebec notaries travelling internationally with electronic devices face increasing uncertainty about how those electronic devices will be treated by border agents on apprehension by Canadian Border Security Agency ("CBSA") officers on return to Canada, by border agents in the U.S., or by border agents in other international destinations. Searching the electronic device (including smart phones, laptops, and USB sticks) of a legal professional may infringe solicitor-client privilege when that legal professional crosses borders.

This advisory, developed by the Policy Counterpart Group of the Federation of Law Societies of Canada (the "Federation") with the assistance of law society practice advice counsel, describes the risks of travelling with an electronic device when returning to Canada, going through pre-clearance with U.S. border officials on Canadian soil, and when travelling to the U.S. and beyond. This advisory also identifies relevant professional responsibilities, and concludes with suggestions and advice for Canadian lawyers and Quebec notaries on minimizing those risks.

Returning to Canada

When returning to Canada, a lawyer or Quebec notary may be unable to rely on a claim of privilege to adequately protect clients' confidential information due to the CBSA's broad interpretation of "goods."[2]

Section 99(1)(a) of the *Customs Act* provides border service officers with the authority to examine "any goods that have been imported and open or cause to be opened any package or container of imported goods and take samples from imported goods in reasonable amounts" without a warrant. Goods are defined within the legislation as including "conveyances, animals and any document in any form."[3] The CBSA further interprets section 99(1)(a) to extend to electronic devices and the documents contained on them.[4] The courts are amenable to this

---

[1] Office of the Privacy Commissioner, "Your privacy at airports and borders," (October 2018), online: https://www.priv.gc.ca/en/privacy-topics/public-safety-and-law-enforcement/your-privacy-at-airports-and-borders/

[2] *Customs Act*, RSC 1985, c 1 (2nd Supp), s 99(1)(a) [*CCA*].

[3] *Ibid*, s 2(1).

[4] The Honourable Ralph Goodale PC, MP, Response to the Tenth Report of the Standing Committee on Access to Information, Privacy and Ethics entitled: *Protecting Canadians' Privacy at the US Border*, (Letter to The Honourable Bob Zimmer, MP, Chair of the Standing Committee on Access to Information, Privacy, and Ethics) (April 16, 2018), online: House of Commons <http://www.ourcommons.ca/>.

interpretation; recent BC and Saskatchewan decisions have affirmed that section 99(1)(a) authorizes a CBSA officer to examine the data stored on any electronic device in the actual possession of, or in the accompanying baggage of, a traveller.[5] The CBSA further asserts that officers can request passwords for the devices. The BC Civil Liberties Association estimates that CBSA examines a daily average of 40 electronic devices at borders crossings across the country; from those 40 electronic devices, an average of 13 are searched each day.[6]

While CBSA policy currently is not publicly available on the CBSA's website, a copy of an operational bulletin for digital devices and media may be found appended to a recent House of Commons Committee report on privacy at the border.[7] A review of information available through other sources[8] and correspondence from Minister Goodale[9] suggests that solicitor-client privileged information is subject to special rules. However, the policy does not completely exempt a legal professional's electronic device from a border search and there are concerns that adequate protections are not in place.

Both the Federation[10] and the Law Society of British Columbia[11] have expressed concerns about the Canadian government's interpretation of "goods" under the Act, as well as the CBSA policy guiding examination of electronic device by its officers. To date, Minister Goodale has responded affirming the CBSA's interpretation of "goods," and asserting that there are procedures in place for documents subject to solicitor-client privilege.[12]

The Supreme Court of Canada has held that section 8 *Charter* protections against unreasonable search and seizure include a heightened expectation of privacy in electronic devices.[13] Further, the Supreme Court has stated that solicitor-client privilege is near absolute, and can only be set aside with legislative language that is clear, explicit, and unequivocal.[14] In a non-border context, search provisions found in legislation must provide the constitutionally required protection for solicitor-client privilege, or they will be found to infringe the s. 8 *Charter*

---

[5] See *R v. Gibson*, 2017 BCPC 237, and *R v. Bielski*, 2018 SKCA 71, and the authorities canvassed within.
[6] BCCLA and Canadian Internet Policy and Public Interest Clinic, "Electronic Devices Privacy Handbook: A Guide to your Rights at the Border," (2018) online: <https://bccla.org/wp-content/uploads/2018/07/Electronic-Devices-Privacy-Handbook-BCCLA_2018.pdf>
[7] Canadian Border Services Agency, Operational Bulletin: PRG -2015 -31, Examination of Digital Devices and Media at the Port of Entry – Interim Guidelines, 30 June 2015, at Appendix A of the Standing Committee on Access to Information, Privacy and Ethics report "Protecting Canadians' Privacy at the U.S. Border," (December 2017), online: http://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9264624/ethirp10/ethirp10-e.pdf
[8] Federation of Law Societies of Canada, *RE Border Searches of Electronic Devices and the Preservation of Solicitor Client-Privilege,* (Letter to The Honourable Ralph Goodale, Minister of Public Safety) (April 20, 2018), online: FLSC <https://flsc.ca/> [*FLSC*]. For further discussion on the CBSA's policy see online: House of Commons ETHI minutes (September 27, 2017) <http://www.ourcommons.ca/>.
[9] The Honourable Ralph Goodale PC, MP, (Letter to Herman Van Ommen, QC, President of the Law Society of British Columbia) (June 28, 2017), online: The Law Society of British Columbia <https://www.lawsociety.bc.ca/> [*Goodale*].
[10] *FLSC, supra* note 8.
[11] Herman Van Ommen QC, *Re: Search of Lawyers' Electronic Devices by Border Agents,* (Letter to The Honourable Jody Wilson-Raybould, Minister of Justice and Attorney General of Canada, and The Honourable Ralph Goodale, Minister of Public Safety) (May 1, 2017), online: The Law Society of British Columbia <https://www.lawsociety.bc.ca/>.
[12] *Goodale*, supra note 6. The Honourable Ralph Goodale PC, MP (Letter to Sheila MacPherson, President of the Federation of Law Societies of Canada) (June 21, 2018).
[13] *R v Fearon*, 2014 SCC 77, [2014] 3 SCR 621; *R v Vu*, 2013 SCC 60, [2013] 3 SCR 657.
[14] *Canada (Privacy Commissioner) v Blood Tribe Department of Health*, 2008 SCC 44, [2008] 2 SCR 574; *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, 2010 SCC 23, 1 SCR 815 at 54.

right to be free of unreasonable search and seizure.[15] The *Customs Act* does not contain the required language for CBSA officers to access privileged information. The Supreme Court of Canada has continuously reaffirmed solicitor-client privilege as a civil right and a fundamental principle of justice of supreme importance in Canadian law that must be as close to absolute as possible.[16] Therefore any incursions to privilege must be absolutely necessary and minimally impairing.[17]

In *Lavallee*, the Supreme Court of Canada set out guidelines for law office searches to protect solicitor-client privilege.[18] These guidelines were extended in *Festing*, where the BC Court of Appeal stated "the legal protection afforded solicitor-client privilege does not begin and end at the door of a law office."[19] In this case, the Court of Appeal broadly defined "law office" as extending to "any place where privileged documents may reasonably be expected to be located."[20] Accordingly, an electronic device used to practice law, such as a laptop or smartphone, should be considered a "law office" subject to the *Lavallee* guidelines. Further, the Supreme Court has held that the expectation of privacy in communications subject to solicitor-client privilege is invariably high. The Court has specifically rejected the argument that there is a reduced expectation of privacy for privileged communication during a search of a law office by a FINTRAC official rather than a police officer investigating a criminal complaint.[21] There has been no case law to suggest there is a reduced expectation of privacy for solicitor-client privileged information at the border.

Respecting body searches at the border, courts have concluded that the State's sovereignty and security interests grant a lower expectation of privacy at the border than in other situations.[22] In *Simmons,* warrantless border searches were "justified by the national interests of sovereign states in preventing the entry of undesirable persons and prohibited goods, and in protecting tariff revenue."[23] While solicitor-client privilege is nearly absolute, there are limited exemptions. One exemption is the narrowly defined "protection of public safety." This is not a broad public safety exemption; it requires that (1) the client poses a clear risk to an identifiable person or group of persons; (2) the risk is of serious bodily harm or death; and (3) the risk is imminent.[24] There is nothing to indicate the CBSA could rely on the public safety exemption in a broader context.

Because the legality of a potential CBSA search of a lawyer or notary's electronic device containing privileged information has not been tested in court, legal professionals should be wary when crossing the border into Canada.

---

[15] *Canada (Attorney General) v Federation of Law Societies of Canada*, 2015 SCC 7, [2015] 1 SCR at 6 [*AG v FLSC*].
[16] *Alberta (Information and Privacy Commissioner) v University of Calgary*, 2016 SCC 53, [2016] 2 SCR 555.
[17] *Ibid.*
[18] *Lavallee, Rackel & Heintz v Canada (Attorney General); White, Ottenheimer & Baker* v *Canada (Attorney General); R* v *Fink,* [2002] 3 SCR 209, 2002 SCC 61 (CanLII).
[19] *Festing v Attorney General (Canada),* 2003 BCCA 112 at para 27, 223 DLR (4th) 448.
[20] *Ibid* at para 24.
[21] *AG v FLSC*, *supra* note 15 at para 38.
[22] *R v Simmons*, [1988] 2 SCR 495 at para 49, 55 DLR (4th) 673.
[23] *Ibid*, at para 48.
[24] *Smith v Jones*, [1999] SCJ No 15 at para 77, [1999] 1 SCR 455 (SCC).

Lawyers and notaries should also consider whether, in certain situations, they ought to take steps to protect solicitor-client privilege as between themselves and their clients with respect to communications that may be in the possession of their clients on their own laptops or cellphones.[25] Legal professionals could include information in their retainer letter about protecting privileged information during travel, and should discuss this issue with their clients, providing guidance as appropriate to the circumstances.

U.S. Border Officials on Canadian Soil: Pre-Clearance

Lawyers and notaries should also know that travellers to the U.S. could encounter U.S. border officials while still on Canadian soil. At a growing number of preclearance points across Canada, U.S. border officials have the authority to examine passengers and their goods, including electronic devices, ahead of travel. As set out on the Privacy Commissioner of Canada's website

> "While preclearance legislation states U.S. officers must, while in Canada, also comply with Canadian law, including the *Charter*, a Canadian who believes a U.S. customs official has broken Canadian law has little recourse in the courts due to the principle of state immunity."[26]

Of course, Canadian travellers may also choose to walk away from a proposed search and forego their wish to enter the U.S., although that decision may be noted and affect future travel. If you are concerned that a U.S. border official operating in a preclearance facility has violated Canadian law, you could contact Public Safety Canada's Preclearance Unit (Public Safety Canada International Affairs Division – Preclearance, 269 Laurier Avenue West, Ottawa, Ontario K1A 0P8).

Travelling to the United States and Beyond

On January 4, 2018, U.S. Customs and Border Protection ("CBP") issued a new Directive on the border search of electronic devices.[27] It sets out procedures for CBP officers to follow when they encounter information on an electronic device over which solicitor-client privilege is asserted: they need to seek clarification from the owner as to specific files, attorney or client names, or other particulars that may assist CBP officers in identifying privileged information; any privileged material must be segregated following a mandatory consultation with CBP counsel; and unless any of those materials indicate an imminent threat to homeland security, copies of the privileged materials must be destroyed. The American Civil Liberties Association has criticized the Directive for failing to require a search warrant in advance of a CBP's search and

---

[25] See, i.e., *R. v Simpore*, 2017 NBQB 162 (CanLII), which revolved around the propriety of a search undertaken by CBSA agents on an individual's laptop and cell phone, resulting in the discovery of communications between the client and an articling student.
[26] "Your privacy at airports and borders," *supra* note 1.
[27] U.S. Customs and Border Protection, CBP Directive No. 3340-049A, online: https://www.cbp.gov/sites/default/files/assets/documents/2018-Jan/CBP-Directive-3340-049A-Border-Search-of-Electronic-Media-Compliant.pdf.

copy of a traveler's electronic device.[28] It is notable as well that the Directive exempts actions taken to determine if physical contraband is concealed within the device itself, and does not limit CBP's authority to conduct lawful searches of electronic devices in response to exigent circumstances.[29]

Other jurisdictions may or may not have laws and policies addressing border searches of electronic devices. While it is outside of the scope of this advisory to canvas legislative authorities in other countries, we advise lawyers and Quebec notaries to undertake due diligence about applicable laws and policies when travelling internationally with electronic devices.

Model Code of Professional Conduct obligations and other responsibilities

"Lawyers must keep their clients' confidences and act with commitment to serving and protecting their clients' legitimate interests."[30] Solicitor-client privilege is a principle of fundamental justice, and one of the obligations that lawyers have a professional duty to uphold. The *Model Code of Professional Conduct* Rule 3.3-1 sets out the following requirements:

> "A lawyer at all times must hold in strict confidence all information concerning the business and affairs of a client acquired in the course of the professional relationship and must not divulge any such information unless:
>
> (a) expressly or impliedly authorized by the client;
> (b) required by law or a court to do so;
> (c) required to deliver the information to the Law Society; or,
> (d) otherwise permitted by this rule."[31]

Rule 3.4-23 extends obligations to protect the confidential information of clients to law firm staff. Subrule (b) requires that a lawyer or law firm must exercise due diligence in ensuring that each member and employee of the law firm, and each other person whose services the lawyer or the firm has retained, does not disclose confidential information of clients of the firm, or any other law firm in which the person has worked.[32] A potential electronic device search at the border also engages Rule 3.3-2, which requires that a lawyer not "disclose a client's or former client's confidential information to the disadvantage of the client or former client, or for the benefit of the lawyer or a third person without the consent of the client or former client."[33]

---

[28] ACLU Comment on Trump Administration Directive on Border Searches, January 5, 2018, available online: https://www.aclu.org/news/aclu-comment-trump-administration-directive-border-searches.
[29] *Ibid* at para. 2.3.
[30] *AG v FLSC*, *supra* note 15 at para 1.
[31] Federation of Law Societies of Canada, *Model Code of Professional Conduct* (14 March 2017), r 3.3-1, online: FLSC <https://flsc.ca/>. As of the date of writing every province and territory, with the exceptions of Quebec and the Yukon, has either adopted or agreed to adopt the *Code*.
[32] *Ibid*, r 3.4-23.
[33] *Ibid*, r 3.3-2.

In addition to Code obligations regarding confidential client information, legal counsel may also have obligations under rules of their respective law societies and applicable privacy legislation. These obligations may require legal professionals to report to their law society or to the privacy commissioner or both in circumstances where their electronic device containing confidential client information has been examined by a border official. Legal counsel may contact a law society practice advisor or the equivalent at their law society for guidance as to their reporting obligations.

Suggestions for Canadian Lawyers and Notaries Travelling with Electronic Devices

Lawyers and Quebec notaries should assess the risks of carrying confidential client information across borders and take steps to ameliorate the risk of a client's information being exposed.

Below are some suggestions to consider for travelling with electronic devices.

1. Establish a policy about cross-border travel by legal counsel and staff carrying smartphones, laptops and other electronic devices that may contain confidential information of their clients. Lawyers and notaries have an obligation to maintain the confidentiality of their clients' information and this obligation extends to ensuring that non-lawyer staff and each other person whose services the lawyer, notary, or law firm has retained[34] also maintain clients' confidentiality.

2. Get help from information technology professionals regarding the security of your devices and alternatives to carrying potentially privileged information across the border. The safest way to travel is without any confidential client information. Some firms have separate clean laptops and phones available for cross-border travel.[35] It may be advisable to forensically clean confidential information from your device before travelling (including cookies, cache and browsing history).

3. If you do not maintain separate devices for work and personal matters, separate your work and personal accounts on your laptop or smartphone, if possible, so that privileged information in one user account can be easily identified during any prospective searches.[36] Characterize sensitive information, clearly marking privileged documents as solicitor-client privileged. If documents are not clearly marked, the information may be at heightened risk of being examined by the CBSA or other border agencies. Whether or not privileged documents are clearly marked, it is important to speak up early during the examination process and claim privilege when appropriate.

---

[34] Paralegals, accountants, bookkeepers, information technology professionals, etc., may have privileged information on their devices.
[35] Barbara Buchanan QC, *Client Confidentiality-Think Twice Before Taking Your Laptop or Smart Phone Across Border* (Benchers' Bulletin, Spring 2017) online: Law Society of British Columbia <https://www.lawsociety.bc.ca/> at 11.
[36] BC Civil Liberties Association, *supra* note 5 at 49.

4. Carry identification that shows that you are a legal professional, such as your law society member identification card and a business card.

5. Understand that certain characteristics of your travel and your behavior make you more susceptible to closer examination by border agents. Based on research done by the B.C. Civil Liberties Association, you are more likely to be chosen to have your devices searched by the CBSA if, amongst other indicators, you have travelled to and from "high risk" destinations, are a single man traveling alone, exhibit nervousness or agitation, have multiple electronic devices (including hard drives), purchase a ticket to travel at the last minute, or have "unusual" travel routes.[37]

6. Put your device on airplane mode to stop information from transmitting[38] and turn it off before approaching the border. When you turn your device on again, it will still be in airplane mode and no new information will have been transmitted. CBSA and CBP officers are supposed to look at only information that is on your device, not use the device to access information that is in the cloud.[39]

7. If asked by a border officer to hand over your electronic device, explain that you are a lawyer or Quebec notary and claim privilege (if the device may contain privileged information). If the officer is a CBSA officer, tell him or her about Minister Goodale's letter assuring that there are CBSA policies in place for solicitor-client privileged information (or even carry a copy with you and provide it to the officer).[40]

8. If the CBSA demands your electronic device containing privileged information, request to see the senior customs officer at the place in which the search is to be conducted.[41] If the senior officer sees no reasonable grounds for a search, you may be discharged.[42]

9. Do not be intentionally vague to border officers. Legal counsel should be prepared to explain the purpose of their travel, and if appropriate, their connection to a Canadian law practice, without divulging confidential client information. Do not rely on your electronic device to answer travel questions. Instead, have a printed itinerary to show to border officers.

10. Communicate with your clients about what information, if any, they are comfortable having you travelling with across borders. Also consider that some clients may not

---

[37] *Ibid* at 24-25.
[38] This will prevent any new incoming texts, emails, calls, and other incoming communications from your applications.
[39] Canadian Border Services Agency, Operational Bulletin: PRG – 2015 -31, Examination of Digital Devices and Media at the Port of Entry – Interim Guidelines, 30 June 2015, *supra* note 7; U.S. Customs and Border Protection, CBP Directive No. 3340-049A, *supra* note 27.
[40] *Goodale*, *supra* note 7.
[41] *CCA*, *supra* note 2 s 99.2(3).
[42] *Ibid*, s 99.2(4).

permit their confidential information to be accessed on an electronic device outside of Canada or the disclosure of any information without their consent or a court order.[43]

11. Bring less data with you.[44] If you use a cloud-based storage provider[45], you may wish to delete cloud-based applications before crossing the border and reinstall afterwards. Similarly, client contact and calendar information can be deleted from smartphones and subsequently restored through internet services. Contact your IT professionals about how to securely re-install deleted applications.

12. Use encryption and secure passwords. Use two-factor authentication to control access to your accounts. It will not deter initial access to your electronic device during a border search, but in the event that your electronic device is seized for further examination, protected accounts may not be accessible.[46]

13. If a CBSA officer retains or accesses your device, get a receipt and make sure that you have a detailed description of the device including make, model and serial number.

14. If you refuse to provide your device's password to allow examination or if there are technical difficulties preventing a CBSA officer from examining the device, the CBSA officer may detain the device for examination by an expert trained in forensic examinations.[47] Under the 2015 operational bulletin, until further instructions are issued, CBSA officers have been advised not to arrest a traveler for hindering solely for refusing to provide a password; a restrained approach is to be adopted until the matter is settled in ongoing court proceedings.[48] It may be advisable to seek legal advice if you anticipate refusing to provide the password to your device to a CBSA officer.

15. Consider applying for a Nexus pass. Nexus is run jointly by the CBSA and U.S. Customs and Border Protection. While having a pass does not mean that you will not be searched, low-risk, pre-approved travelers into Canada and the U.S. enjoy expedited clearance and participating U.S. and Canadian airports, land and marine border crossings.

---

[43] A client's needs and expectations are ideally explored at the beginning of the solicitor-client relationship and dealt with in the retainer agreement. Consider asking simple questions such as whether it is acceptable to share the name of the client and to disclose the purpose of the retainer.
[44] BC Civil Liberties Association, *supra* note 6 at 42-44.
[45] The Law Society of BC has a Cloud Computing Checklist (May 2017) and Law Society Rules 10-3 and 10-4 regarding cloud storage providers, standards and security.
[46] *Supra* note 6 at 46.
[47] *Customs Act*, RSC 1985, c 1 (2nd Supp), s 101.
[48] *Supra* note 7 and *Customs Act*, s. 153.1.