STOCKWOODS
barristers

Flying With Your Cell Phone?
Here's What You Need to Know

by Nader R. Hasan & Gerald Chan[1]

As lawyers, we are inseparable from our cell phones and digital devices. Understandably so. Without those "smart" phones, many of us would feel moored to our desks. Portable e-mail and phone capability allow us to provide prompt service to our clients, while also allowing us a modicum of freedom.

But when we travel — particularly when we travel internationally — that convenience raises a host of legal and ethical concerns. The Canadian Border Services Agency ("CBSA") and its international counterparts, including U.S. Customs and Border Protection ("CBP"), take very aggressive positions on their authority to search your cell phone and laptop when you travel. Those aggressive positions have (so far) withstood court challenge. As a result, you need to be ready for the foreseeable event that a border agent should say, "*Ma'am/sir, I'm going to look at your I-Phone*."

The purpose of this paper is not to provide a detailed analysis and critique on the law of digital privacy at the border (although such papers are available.[2]) Rather, the purpose of this paper is to provide a set of practical tips (though not legal advice) for your consideration when you travel.[3]

The Expansive Search Powers of the Border Services Officers

The CBSA takes the position that it can search *your* cell phone when you return to Canada.[4] According to the CBSA, Border Services Officers ("BSOs") do not require a warrant. They do not require a reasonable and probable grounds. They do not require even reasonable suspicion. While that position is vulnerable to court challenge, so far no such court challenge has been successful and the Ontario Court of Appeal recently declined to address the issue.[5]

---

[1] Nader Hasan and Gerald Chan are partners at Stockwoods LLP in Toronto where they practise criminal, constitutional, and regulatory litigation. Together, they have been counsel in five major digital privacy cases at the Supreme Court of Canada (*R v Cole*, 2012 SCC 53; *R v Vu*, 2013 SCC 60; *R v Fearon*, 2014 SCC 77; *R v Marakah*, 2017 SCC 59; *R v Jones*, 2017 SCC 60). You can reach them at NaderH@stockwoods.ca and GeraldC@stockwoods.ca.

[2] See Nader Hasan & Stephen Aylward, "Cell Phone Searches at the Border: Privilege and the Portal Problem" (February, 2017), *For the Defence*.

[3] We assume that, to the extent you avail yourself of these suggestions, you are doing so to protect the confidentiality and privilege in client-related materials or acting for some other bona fide legal purpose.

[4] CBSA relies on s. 99(1)(a) of the *Customs Act*. That provision states in relevant part: "An officer may, …(a) at any time up to the time of release, examine any goods that have been imported and open or cause to be opened any package or container of imported goods and take samples of imported goods in reasonable amounts."

[5] *R. v. Saikaley*, 2013 ONSC 1854, aff'd 2017 ONCA 374.

The U.S. government takes a similarly expansive approach to CBP's powers. The closest any U.S. court has come to reining in CBP was the Ninth Circuit's decision in *U.S. v. Cotterman.* In *Cotterman,* the Court held that BSOs need reasonable suspicion of illegal activity before they can conduct a *forensic* search of an electronic device, but that a *manual* search of a digital device is "routine" and so a warrantless and suspicionless search passes muster under the Fourth Amendment.[6]

While both the U.S. and Canadian approaches are vulnerable to constitutional challenge, at present the law permits BSOs to conduct groundless, warrantless searches of your digital device at the border.

The Lawyer's Dilemma

Until the constitutional right to privacy catches up to changing technologies, lawyers will have to be especially careful when they travel. Lawyers traffic in confidential and privileged information. On one hand, lawyers have an ethical obligation to provide "prompt service to clients"[7] in a "cost-effective manner."[8] Lawyers are expected to promptly respond to communications from, and report developments to, their clients.[9] In the Digital Age, many clients will expect their lawyer to carry devices such as cell phones when travelling, so that she or he will be able to promptly respond to telephone calls and emails.

On the other hand, lawyers must take "all reasonable steps to ensure the privacy and safekeeping of a client's confidential information".[10] Knowing that a BSO may demand to see the contents of your phone without any evidentiary basis requires that we consider what precautions we are duty-bound to take.

Minimize the Data that You Carry Across the Border

The simplest and most reliable precaution you can take is to reduce the amount data you carry with you across the border. Many law firms and other businesses already insist that their employees travel with blank laptops, and then log into their firm's server through a VPN,[11] and download whatever they need upon their arrival.

Such a precaution is easier to take with a laptop than with your phone. Most people today carry a single device, which is their portal for both business and personal communications. One option, however, is to carry a temporary travel phone. You may even be able to switch your SIM

---

[6] *United States v. Cotterman*, 709 F.3d 952 at 965 (9th Cir.) (en banc).

[7] *LSUC Rules of Professional Conduct*., r. 3.2-1.

[8] *Ibid*, r. 3.1-1(e)

[9] *Ibid*,, r. 3.2-1, Commentary [6].

[10] *Ibid.*, r. 3.5-2, Commentary [2], r. 3.3-1.

[11] A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

card from your regular phone into your temporary travel phone (provided that your mobile phone uses the GSM standard).[12]

Short of using a different phone altogether, you can remove all of your confidential and privileged information. This is not as labour-intensive or painstaking as it sounds. Depending on the phone you use, it may only be a few clicks away. On the I-Phone, for example, you can simply go to Settings → Mail → Accounts and delete your work e-mail account. Your work e-mails will no longer appear on your phone. Upon arrival, you can reinstall your work account and (subject to your phone and server settings) you should immediately be able to download all of your work e-mails from your server.

This measure, however, will not permanently remove all of your work e-mails from the phone. A forensic search done by a sophisticated party would still be able to recover them. However, a manual search — the type you are most likely to be subjected to at the border — will likely not uncover what you have removed.

We would not recommend features or "cheater" apps aimed at "hiding" data on your device. BSOs are trained to look for such measures and to be suspicious of people who employ them.

Assert Privilege

The law jealously protects solicitor-client privilege. The *Criminal Code,* for instance, contains a robust regime setting out the procedure for searching a law office that minimizes the risk to solicitor-client privilege.[13]

Courts have held that a lawyer's phone should be treated no differently from her law office when it comes to search and seizure.[14] But we know of no law or policy that adequately protects solicitor-client privilege in the event that a BSO asks to search a lawyer's phone. At the time that this article was written, CBSA counsel had advised the authors that CBSA was working on a policy to deal with searches of lawyers' phones at the border, but would not provide any further detail on current practice or policy.

Despite this blindspot, if a BSO asks to search your phone, you should advise that you are a practising lawyer; that your phone does contain solicitor-client material; that you are asserting that privilege on behalf of your clients; and that you would like to speak to a CBSA supervisor. Such measures may not prevent the phone from being searched but it will be difficult for the Law Society to impugn your conduct (and you will have laid an evidentiary record for a great test case!).

Should I Give Them My Passcode?

---

[12] GSM (Global System for Mobile communications) is an open, digital cellular technology used for transmitting mobile voice and data services. This standard is ubiquitous in most countries.

[13] *Criminal Code*, s. 488.1.

[14] *R. v. Shah*, 2015 ONSC 4853; *R. v. A.B.*, 2013 NLTD(G) 76, aff'd 2014 NLCA 8.

It is no secret it can be tough for law enforcement to crack an I-Phone.[15] But all the encryption in the world does not help you when you are asked to give up your passcode. Both Canada and the U.S. assert that their BSOs can compel travellers to surrender their passcodes at the border. We take the position that this practice is unconstitutional, but you probably do not want to be our test-case litigant. Last year, a Quebec man was arrested and charged at the Halifax airport for refusing to provide BSOs with his passcode. His case was watched closely because he would have been the forced to challenge CBSA's authority to compel passwords. On the eve of trial, however, he pleaded guilty to hindering a *Customs Act* investigation and paid a $500 fine.[16]

To that end, you may conclude that you are better off complying with requests — and taking the precautions set out above before you fly — rather than putting yourself in this unwinnable dilemma.

[15] NPR.org, "A Year After San Bernardino And Apple-FBI, Where Are We On Encryption?" online: http://www.npr.org/sections/alltechconsidered/2016/12/03/504130977/a-year-after-san-bernardino-and-apple-fbi-where-are-we-on-encryption.

[16] CBC, "Alain Philippon pleads guilty over smartphone password border dispute" (April 16, 2016), online: http://www.cbc.ca/news/canada/nova-scotia/alain-philippon-to-plead-guilty-cellphone-1.3721110.