Canadian Journal of Law and Technology

Volume 14 | Number 2 Article 3

6-1-2016

Electronic Devices at the Border: The Next Frontier of Canadian Search and Seizure Law?

Robert J. Currie

Electronic Devices at the Border: The Next Frontier of Canadian Search and Seizure Law?

Robert J. Currie*

Abstract

Over the last several years the Supreme Court of Canada has developed its jurisprudence regarding the search and seizure of electronic devices, applying section 8 of the Canadian Charter of Rights and Freedoms *in such a way as to assert and protect a significant amount of privacy in the devices and their data. Recent cases regarding the search of devices at Canada's borders, however, do not reflect this case law. This is a situation made all the more complex by the generally attenuated expectation of privacy in the border context, and is worthy of inquiry. Using a pending border case as a leaping-off point, this paper explores how section 8 should be applied to searches of electronic devices in the possession of people entering Canada, concluding that an appropriate analysis would impose more robust privacy protection than has been seen to date. It also examines the issue of whether individuals can be compelled to unlock devices or surrender passwords during border searches.*

INTRODUCTION

In March 2015, a Quebec resident named Alain Philippon was returning from a trip to the Dominican Republic and arrived in the Halifax airport. He was stopped by Canadian Border Services Agency (CBSA) officials for what appears to have been "secondary inspection." This involved a search of material he had with him, including his cellphone. The official who stopped him demanded that he provide the phone's password, but Philippon refused to provide it. He was arrested and charged under section 153.1(b) of the *Customs Act*,[1] which provides:

> 153.1 No person shall, physically or otherwise, do or attempt to do any of the following:
>
> . . .

* Professor, Schulich School of Law, Dalhousie University (robert.currie@dal.ca). This paper was originally presented at the 29th Annual Conference of the International Society for the Reform of Criminal Law, on 28 June 2016, and I am grateful for discussion and feedback that emerged. Thanks are also due to my colleague, Steve Coughlan, and to Stephen Aylward and Michael Osborne for their comments, and to Sophie DeViller for excellent research assistance and astute analysis. In light of my editorial role in this publication, it should be stated that this article was subjected to expert peer review.

[1] R.S.C. 1985, c. 1 (2nd Supp) [hereinafter *Customs Act* or *Act*].

> (b) hinder or prevent an officer from doing anything that the officer is authorized to do under this *Act*.

Philippon was released on bail and returned to his home in Ste-Anne-des-Plains, Quebec. He has entered a plea of not guilty to the *Customs Act* offence, and his trial is scheduled for August 2016 before the Nova Scotia Provincial Court in Dartmouth, Nova Scotia.[2]

Philippon's seemingly-ordinary case is remarkable in a number of respects, not least of which is the reaction to it. Beginning with an initial report by the Canadian Broadcasting Corporation's (CBC) reporter Jack Julian that appeared on CBC's website and the regional television program,[3] the story quickly ignited a storm of international interest—so much so that Mr. Julian was moved to do a follow-up story which mostly dealt with the intense level of interest in the case among the general public.[4] While the flurry of attention may have been unusual, it seems understandable because the topic is of great interest to everyone who a) travels, and b) owns a cell phone, tablet or computer—which adds up to a lot of people. This interest boils down to a set of basic questions: are CBSA officials allowed to search our devices at the border? Under what conditions and to what extent? And if so, can people be compelled to surrender the passwords for their locked devices, or to unlock the devices themselves, to facilitate the search?

This case also arrives at an interesting time in the development of Canadian search and seizure jurisprudence. For some time courts all over the country have been wrestling with why, how and under what circumstances a balance must be struck between the privacy interests of individuals in their electronic lives and devices, on the one hand, and the interests of the state and society in effective criminal law enforcement, on the other. Striking such a balance is obviously as necessary now, in the "Digital Age", as it ever was; as Binnie J. commented in *R. v. Tessling*, "social and economic life creates competing demands. The community wants privacy but it also insists on protection. Safety, security and the suppression of crime are legitimate countervailing concerns."[5]

Since 2010, the Supreme Court of Canada has issued what in relative terms is a large number of significant decisions on the search and seizure of computers and other electronic devices, leading one commentator to refer to the

---

2 Personal communication from Joel Pink, Q.C., local counsel to Mr. Philippon.

3 Jack Julian, "Quebec resident Alain Philippon to fight charge for not giving up phone password at airport", *CBC News* (4 March 2015), online: < http://www.cbc.ca/news/canada/nova-scotia/quebec-resident-alain-philippon-to-fight-charge-for-not-giving-up-phone-password-at-airport-1.2982236 >. I provided commentary for this story and very quickly received requests for comments from numerous other media, both in Canada and in several other countries.

4 Jack Julian, "Alain Philippon phone password case may meet Charter challenge conditions", *CBC News* (7 March 2015), online: < http://www.cbc.ca/news/canada/nova-scotia/alain-philippon-phone-password-case-may-meet-charter-challenge-conditions-1.2985694 >.

5 2004 SCC 67, 2004 CarswellOnt 4351, 2004 CarswellOnt 4352 (S.C.C.) at para. 17.

"digitization of section 8 of the *Charter*."[6] Yet the border context has remained largely untouched in this new digital privacy era and is quite unsettled as a result. This is in no small part because of the unique balance—or, more accurately, imbalance—of privacy concerns and state interests that has historically existed at the border, and which is being confronted with the new reality of ubiquitous electronic devices being brought back and forth by travellers. This may explain the intense interest in the Philippon case.

Using the Philippon case as a leaping-off point, this paper seeks to examine how section 8 applies to searches of electronic devices at the border. Section I will provide a brief review of the Supreme Court's recent decisions on search and seizure of computers and like devices. Section II will review the current approach taken by courts in applying section 8 of the *Charter* to device searches under the *Customs Act*. It will also examine the few cases on point that have emerged, and will attempt to distil something of a sensible approach to search and seizure of electronic devices at the border. Section III will examine the particular issue raised by the facts of the Philippon case: can individuals be compelled to unlock their devices to facilitate a search at the border, or does this offend the principle and *Charter* protections against self-incrimination? Section IV will offer a few modest conclusions.

I. SEARCHING DEVICES: THE RECENT CASE LAW

It is not hyperbolic to say that the penetration of electronic devices into our lives over the last decade or so has been systemic, unforeseen and far-reaching in scope. We use them for entertainment, education, work and communication. We also use them for storage of all kinds of information; we do this both deliberately, in that we save emails, notes, documents, music, movies and photos on them, and passively, in that as the devices themselves generate and store data (often referred to as "*metadata*") about how we use them, particularly (though not exclusively) for internet use. Criminals use them for all of these purposes, any of which might be useful towards committing or facilitating unlawful acts, or generating evidence of them. Stalkers and intimidators carry out their urges via text, email or Facebook message; cyberbullies take and post embarrassing photos with their cell phones; child pornographers use all manner of devices to circulate their wares; Crown prosecutors are often heard to remark on the evidentiary bonanza created by the tendency of gang members to take and text photos of drugs and guns. Moreover, many people use their devices for purposes that are perfectly lawful but which they wanted to remain private—such as booking sessions with a marriage counselor or divorce lawyer, taking nude "selfies," doing their banking, viewing legal pornography, or purchasing tickets to a Nickelback concert.[7]

---

[6] Steven Penney, "The Digitization of Section 8 of the Charter: Reform or Revolution?" (2014) 67 SCLR 505. See *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982,* being Schedule B to the *Canada Act 1982* (UK), c. 11 [*Charter*].

This being the case, it was inevitable that the Canadian law of search and seizure under section 8 of the *Charter* would need to engage with our newly digitized reality. The Supreme Court of Canada, beginning with its landmark decision in *R. v. Morelli* in 2010,[8] has actively responded to this need with a series of decisions designed to accommodate the new realities of both police investigation and individual privacy regarding devices. This section will quickly hit the highlights of that jurisprudence, focusing on the aspects that are relevant to the border context to be discussed below.[9]

A preliminary point worth noting at the outset is one that most readers will know: while the cases deal with computers, tablets or cell phones/smart phones based on their specific facts, the distinction between these devices is largely meaningless. Technology companies that manufacture the devices have actively sought to blur whatever distinctions might exist and ensure that each device is capable of carrying out roughly the same functions. For example, the Apple Mac computer takes pictures and video, as does the iPad tablet, as do both the iPod and iPhone, and all have virtually identical apps for texting, email and document storage. The Microsoft "Surface Book" is a computer with a touch-sensitive screen that acts like a large tablet (or it may be a tablet that acts like a small computer—it is difficult to tell). As the Supreme Court remarked in *R. v. Vu*, "[a]lthough historically cellular telephones were far more restricted than computers in terms of the amount and kind of information that they could store, present day phones have capacities that are, for our purposes, equivalent to those of computers."[10]

Accordingly, the internal workings and functionality of this machinery is so similar that the law applies, for all meaningful purposes, in the same way. The various devices will be referred to, generically, as "devices" unless the factual setting dictates otherwise.

(a) *Morelli* (2010)

At issue in *Morelli* was whether the police had reasonable and probable grounds to search the accused's personal computer for child pornography and the defectiveness of the Information to Obtain (ITO) that had been used to

---

7 I make the latter observation solely on the basis that this hugely successful Canadian rock band is nonetheless intensely unpopular in some circles, and not to take a position on the issue; though see Shaunacy Ferro, "A Scientific Explanation for Why Everyone Hates Nickelback" *mental_floss* (6 April 2016), online: <http://mentalfloss.com/article/78221/scientific-explanation-why-everyone-hates-nickelback>.

8 2010 SCC 8, 2010 CarswellSask 150, 2010 CarswellSask 151 (S.C.C.) [*Morelli*].

9 This section draws on an excellent recent article by Nader Hasan, "A Step Forward or Just a Sidestep? Year Five of the Supreme Court of Canada in the Digital Age" (2015) 71 SCLR 439 [Hasan].

10 2013 SCC 60, 2013 CarswellBC 3342, 2013 CarswellBC 3343 (S.C.C.) at para. 38 [*Vu*]. And see *R. v. Fearon*, 2014 SCC 77, 2014 CarswellOnt 17202, 2014 CarswellOnt 17203 (S.C.C.) at para. 51 [*Fearon*].

obtain the search warrant. There were two points of interest: first, it was clear that the accused had a reasonable expectation of privacy in his computer such that a warrant was required—so clear that the court simply took it as given. Second, in commenting on the invasiveness of a search of a device during his section 24(2) exclusion analysis, Fish J. for the majority threw down the gauntlet of electronic privacy:

> It is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer. . .
>
> Computers often contain our most intimate correspondence. They contain the details of our financial, medical, and personal situations. They even reveal our specific interests, likes, and propensities, recording in the browsing history and cache files the information we seek out and read, watch, or listen to on the Internet.
>
> It is therefore difficult to conceive a s. 8 breach with a greater impact on the *Charter*-protected privacy interests of the accused than occurred in this case.[11]

This robust privacy interest in devices also impacted the court's analysis in *R. v. Cole*,[12] where a teacher was held to have a reasonable expectation of privacy in his workplace computer, despite the fact that it was owned by the school board by which he was employed, because he had been permitted to use it for some personal purposes. The data in the computer could reveal financial, medical or personal matters, and his "specific interests, likes, and propensities;" this was personal information that "falls at the very heart of the 'biographical core' protected by s. 8 of the *Charter*."[13]

(b) *Vu* (2013)

In *Vu* the police obtained a warrant to search a residence for evidence that would indicate the owners and occupants of the residence. While the ITO specified "computer generated documents" it did not specifically authorize the search of computers. Two computers and a cell phone were found and searched, revealing that Vu was a resident. The British Columbia Court of Appeal reversed the trial judge's exclusion of the evidence, reasoning that the warrant did not have to specifically authorize the search of devices, since such a device was analogous to a "four-drawer filing cabinet" which could be searched because it was found within the place for which the search was authorized.[14]

---

[11] *Morelli*, *supra* note 8 at paras. 2, 105-106.

[12] 2012 SCC 53, 2012 CarswellOnt 12684, 2012 CarswellOnt 12685 (S.C.C.).

[13] *Ibid,* at paras. 47-48. The court paid particular attention to the fact that there were images of Cole's wife on the computer, and the police witnesses even acknowledged that he had a privacy interest in those (see, e.g., para. 119), illustrating the point made above about device content that is lawful but intensely private.

A unanimous Supreme Court disagreed with Cromwell J. writing a judgment that rested on the "markedly different" privacy interests in devices as distinguished from cupboards, filing cabinets or other "receptacles."[15] Beyond the highly personal nature of the information contained in devices, which they had discussed in *Morelli* and *Cole*, the court set out four ways in which computers were so "markedly different":

1) **"immense" capacity**: devices have the capability of storing exponentially larger amounts of data than any physical receptacle.[16] "An 80-gigabyte desktop drive—and commercial hard drives have far greater capacities—-can store the equivalent of 40 million pages of text."[17]
2) **storage scope**: a device, the court emphasized, is a "fastidious record keeper," with word processors generating temporary files and browsers generating search records, all of which is created by users "unwittingly," amounting to a kind of information that "has no analogue in the physical world."[18]
3) **lack of deletion**: devices do not actually destroy data that a user has deleted by way of normal deletion functions, but rather re-assign the disc space used and move the data around so that it is functionally inaccessible, but forensically retrievable. "Computers thus compromise the ability of users to control the information that is available about them in two ways: they create information without the users' knowledge and they retain information that users have tried to erase."[19]
4) **connectivity**: while traditional warrants allow police to access a "building, receptacle or place," devices will most often be connected to either a network or the internet that provide access to a wide variety of other data in other locations. "Thus, a search of a computer connected to the Internet or a network gives access to information and documents that are not in any meaningful sense at the location for which the search is authorized."[20]

Accordingly, devices cannot be searched unless the warrant specifically authorizes it and ITOs must provide grounds for doing so. Moreover, the manner of search had to be reasonable, and *ex post* review would pay attention to this—police do not necessarily have "licence to scour the devices

---

14 *R. v. Vu*, 2011 BCCA 536, 2011 CarswellBC 3551 (B.C. C.A.) at para. 63, affirmed in *Vu, supra* note 10.

15 *Vu*, *supra* note 10 at para. 24.

16 *Ibid,* at para. 41.

17 Gerald Chan, "Life After *Vu*: Manner of Computer Searches and Search Protocols" (2014) 67 SCLR 433 at 438, and *ibid.*

18 *Vu*, *supra* note 10 at para. 42.

19 *Ibid,* at para. 43.

20 *Ibid,* at para. 44.

indiscriminately," and in some situations *ex ante* search protocols will be required.[21]

(c) *Spencer* (2014)

In *R. v. Spencer*[22] a Saskatoon police officer involved in a child pornography investigation obtained the Internet Protocol address (IP address) of an individual who appeared to be sharing images with others, and approached the Internet Service Provider, Shaw, with a "law enforcement request" for information identifying the user under the *Personal Information Protection and Electronic Documents Act*.[23] He obtained this information, without a warrant. The Supreme Court held that despite the fact that the identifying information (name, address, and telephone number) matched a publicly available IP address, the user did have a reasonable expectation of privacy in the information because "it was the identity of an Internet subscriber which corresponded to particular Internet usage."[24] Knowledge of a person's internet usage would tend to reveal a great deal about them—likes, dislikes, habits, and predilections. Unfettered state access to this kind of knowledge would impact the individual's informational privacy,[25] particularly the right to use the internet in a reasonably anonymous manner:[26]

> the police request to link a given IP address to subscriber information was in effect a request to link a specific person (or a limited number of persons in the case of shared Internet services) to specific online activities. This sort of request engages the anonymity aspect of the informational privacy interest by attempting to link the suspect with anonymously undertaken online activities, activities which have been recognized by the court in other circumstances as engaging significant privacy interests[.][27]

In the circumstances, Spencer's expectation of privacy in the subscriber information had been reasonable, and a warrant or production order should have been obtained.

(d) *Fearon* (2014)

In *Fearon,* the Supreme Court dealt with what had until then been a divisive issue: what is the scope for searching devices in a person's possession when the individual is being searched incident to arrest?[28] Fearon was searched after being

---

21 *Ibid,* at para. 61.

22 2014 SCC 43, 2014 CarswellSask 342, 2014 CarswellSask 343 (S.C.C.) [*Spencer*].

23 See *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5.

24 *Spencer*, *supra* note 22 at para. 32.

25 As the court noted, its section 8 jurisprudence has dealt with "three broad types of privacy interests—territorial, personal and informational" (*ibid*, at para. 35).

26 *Ibid*, at paras. 39-46.

27 *Ibid*, at para. 50.

arrested for an armed robbery and his phone was taken. The arresting officers looked through various applications on his phone and discovered a draft text with an incriminating admission, as well as a photo of a gun that turned out to be the one used in the robbery. The majority of the court ruled that phones could properly be searched incident to arrest, so as not to defeat the important law enforcement needs during arrests.

However, emphasizing once again the significant differences between a device and any other kind of material that would normally be found on an individual's person,[29] Cromwell J. for the majority held that the search should be strictly limited. This was a warrantless search, an exception carved out by the common law for the naturally-occurring law enforcement interests that needed to be served in the context of an arrest; otherwise, reasonable and probable grounds would be required. Accordingly, a search following a lawful arrest must be truly incidental to the arrest, with three specific limitations:

– both the nature and the extent of the search must be incidental to the arrest.

> In practice, this will mean that, generally, even when a cell phone search is permitted because it is truly incidental to the arrest, only recently sent or drafted emails, texts, photos and the call log may be examined as in most cases only those sorts of items will have the necessary link to the purposes for which prompt examination of the device is permitted. But these are not rules, and other searches may in some circumstances be justified.[30]

– the "discovery of evidence" purpose which would make a search truly incident to arrest must be treated restrictively and only in play if "the investigation will be stymied or significantly hampered absent the ability to properly search the cell phone";[31]
– since the search is available without prior authorization, "after-the-fact judicial review is especially important" to ensure the constitutionality of the search. Accordingly, police should keep careful notes of the search: "The record should generally include the applications searched, the extent of the search, the time of the search, its purpose and its duration."[32]

In sum, then, the Supreme Court of Canada has determined that both the nature and the scope of the data stored within a device—be it a cell phone, computer or tablet—mean that these are places that people have a very intense and justiciable privacy interest. These findings are also commensurate with those

---

28 *Fearon*, *supra* note 10.

29 The privacy interest inherent in a cell phone, particularly, was also spoken to quite powerfully by the Nova Scotia Court of Appeal in *R. v. Hiscoe*, 2013 NSCA 48, 2013 CarswellNS 242 (N.S. C.A) at paras. 75-76.

30 *Fearon*, *supra* note 10 at para. 76.

31 *Ibid*, at para. 83.

32 *Ibid,* at paras. 82-83.

in the 2014 decision of the U.S. Supreme Court in *Riley v. California*,[33] in which that court noted, "a cell phone search would typically expose to the government far more than the most exhaustive search of a house."[34] As one commentator noted, "the idea that an individual has a reasonable expectation of privacy in the contents of his cell phone and other digital devices is no longer the subject of serious debate."[35] The intense nature of this privacy interest, however, bumps up against other perhaps equally intense state interests at the border, and the discussion will now turn there.

II. SECTION 8 AT THE BORDER

(a) The Customs Context

The CBSA is charged with administering several pieces of federal legislation that might operate at the border, including the *Immigration and Refugee Protection Act*, the *Criminal Code*,[36] and the *Customs Act*. For present purposes I am concerned with the powers to question and search individuals entering Canada, which CBSA agents exercise pursuant to the *Customs Act*. It is clear that once CBSA agents have reasonable and probable grounds to believe that an offence has been committed (and/or that they will find evidence of an offence), then regular criminal procedure and attendant *Charter* standards kick in. What often gets the CBSA officials to that conclusion, however, is the exercise of their broader *Customs Act* questioning and search powers; the usual pattern is that an individual arriving in Canada is subjected to "ordinary" border screening, during which the CBSA staff notice something unusual or find evidence of some kind of contraband, which leads to a more intrusive search, which in turn leads to arrest, *Charter* caution and—almost inevitably—conviction.

The *Customs Act* contains an array of provisions that authorize CBSA staff to question individuals, search their persons and belongings, and examine items in their possession and/or which they are importing. Sections 11 and 13 require people arriving in Canada to: present themselves to a customs officer and answer truthfully any questions asked; answer questions about any goods they have imported; and unload, unpack or open any container containing the goods. The actual search provisions break down into three sets of searches: searches of people on the basis of reasonable suspicion that an offence has been committed

---

[33] 134 S.Ct. 2473 (U.S. Cal. Sup. Ct., 2014) [*Riley*]. The overall finding in *Riley* was that a search warrant is required to search a cell phone incident to arrest, a position which the Supreme Court of Canada was not prepared to take in *Fearon*, *supra* note 10.

[34] *Ibid,* at 2491.

[35] Agathon Fric, "Reasonableness as Proportionality: Towards a Better Constructive Interpretation of the Law on Searching Computers in Canada" (2016) 21 Appeal 59 at 64 (QL) [Fric].

[36] *Immigration and Refugee Protection Act*, S.C. 2001, c. 27; *Criminal Code*, R.S.C. 1985, c. C-46.

(sections 98(1), 99.2(1)); searches of a person's goods (whether imported or on their person) on the basis of reasonable suspicion that an offence has been committed (sections 99(1)(e), 99.1(2)(b) and 99.3(2)); and searches of imported goods and any goods in custody or possession of an individual entering or leaving a customs-controlled area, without any grounds (sections 99(1)(a) and 99.3(1), respectively). All of these searches are warrantless.

As will be seen, most important here are the latter two provisions:

- section 99(1)(a), which allows a CBSA officer to examine any goods that have been imported and "open or cause to be opened any package or container of imported goods"; and
- section 99.3(1), which allows a CBSA officer to conduct a "non-intrusive examination of goods in the custody or possession of a person who is in or leaving a customs-controlled area."

Again, unlike the rest of the search provisions, neither of these latter searches require that the official have reasonable grounds or even reasonable suspicion that an offence has been committed or that anything at all is awry.

As in all *Charter*-related matters, context is everything, and the border context has received specialized treatment by the courts due to the unique interplay of state interests and individual freedoms that is engaged. Starting with the leading 1988 case of *R. v. Simmons*,[37] the Supreme Court of Canada and all Canadian courts have recognized that the state is given a wide and permissive scope of inspection and interference with individual interests because of its compelling duty to protect its sovereignty and populace by "control[ling] both who and what enters their boundaries."[38] In particular, there is a much-reduced expectation of privacy at the border. As Justice Doherty expressed it (though speaking specifically to the principle of self-incrimination):

> No one entering Canada reasonably expects to be left alone by the state, or to have the right to choose whether to answer questions routinely asked of persons seeking entry to Canada. As the appellant himself testified, travellers reasonably expect that they will be questioned at the border and will be expected to answer those questions truthfully. Travellers also reasonably expect that Customs authorities will routinely and randomly search their luggage. Put simply, the premise underlying the principle against self-incrimination, that is, that individuals are entitled to be left alone by the state absent cause being shown by the state, does not operate at the border. The opposite is true. The state is expected and required to interfere with the personal autonomy and privacy of persons seeking entry to Canada. Persons seeking entry are expected to submit to and co-operate with that state intrusion in exchange for entry into Canada.[39]

---

[37] 1998 CarswellOnt 91, 1988 CarswellOnt 968, [1988] 2 S.C.R. 495 (S.C.C.) [*Simmons*].

[38] *Ibid,* at para. 49.

[39] *R. v. Jones*, 2006 CarswellOnt 4972, [2006] O.J. No. 3315 (Ont. C.A.) at para. 30 [*Jones*].

Justice Ryan summarized the general tenor of this jurisprudence effectively in *R. v. Sekhon*, emphasizing its "two key features":

> First, that travellers reasonably expect that they will be subject to screening procedures when crossing international boundaries, and second, that there is a compelling state interest in protecting the security of Canada's borders, and in preventing the entry of illegal or contraband goods into the country through our borders. . .
>
> Authorities have repeatedly noted that travellers seeking to cross national boundaries fully expect to be subject to a screening process. Furthermore, this process will typically require the production of identification, travel documentation, and involve a search process.[40]

In *Simmons*, Dickson C.J. identified three levels of border search which still appear to govern the case law:

> First is the routine of questioning which every traveller undergoes at a port of entry, accompanied in some cases by a search of baggage and perhaps a pat or frisk of outer clothing. No stigma is attached to being one of the thousands of travellers who are daily routinely checked in that manner upon entry to Canada and no constitutional issues are raised. It would be absurd to suggest that a person in such circumstances is detained in a constitutional sense and therefore entitled to be advised of his or her right to counsel. The second type of border search is the strip or skin search of the nature of that to which the present appellant was subjected, conducted in a private room, after a secondary examination and with the permission of a customs officer in authority. The third and most highly intrusive type of search is that sometimes referred to as the body cavity search, in which customs officers have recourse to medical doctors, to X-rays, to emetics, and to other highly invasive means.[41]

A full review of border search jurisprudence is obviously beyond the scope of this paper. However, one important technical point emerges from the case law around the scope of the *Simmons* first-level search. Many readers will be familiar with the idea of "secondary inspection," whereby an initial conversation with a CBSA official (whether at an airport or auto-traffic border inspection facility) is followed by "secondary inspection" where a more detailed conversation and search of the individual's belongings is carried out. Secondary inspection is treated as a wholly discretionary decision on the part of CBSA staff for which they need not have reasonable grounds or even form a reasonable suspicion (though CBSA staff have indicated in testimony that they do look for

---

[40] *R. v. Sekhon*, 2009 BCCA 187, 2009 CarswellBC 1094 (B.C. C.A.) at paras. 68, 22, leave to appeal refused 2009 CarswellBC 2991, 2009 CarswellBC 2992 (S.C.C.). A later-stage appeal on an unrelated issue was dismissed, see 2014 SCC 15, 2014 CarswellBC 379, 2014 CarswellBC 380 (S.C.C.).

[41] *Simmons*, *supra* note 37 at para. 27.

"indicators" for referral to secondary inspection, such as nervousness, hesitancy in answering questions, odd travel patterns indicated by passport contents, or receiving information via other government sources).[42] Also, a "secondary" inspection does not remove the situation from the first *Simmons* search level—it "remains a routine part of the general screening process for persons seeking entry to Canada."[43]

(b) Canadian Case Law on E-Device Searches at the Border

While there is a reasonably substantial jurisprudence on border searches, there have not been a large number of reported cases specifically dealing with devices; my research turned up only eight, with a few scattered references to unreported decisions therein.[44] Perhaps unsurprisingly, six of the eight dealt with child pornography that was found on the devices[45] and all of them were dealt with as being "first level" routine searches under the *Simmons* criteria. In one case, *Moroz*, the court appeared to find that section 8 did not apply; in six cases the court found that there had been no breach of section 8 or any other *Charter* rights; in the eighth, the court found a section 8 breach but dismissed an application by the accused for exclusion of the evidence under section 24(2).[46]

As a group these cases have raised a number of different issues. While, as explored below, the decisions do not always adhere rigorously to the Supreme Court's established section 8 methodology, it is helpful to organize the issues raised in keeping with that framework, which can be summarized as follows. First, was there a "search," i.e. was there a reasonable expectation of privacy in

---

[42] See, e.g., *R. v. Buss*, 2014 BCPC 16, 2014 CarswellBC 485 (B.C. Prov Ct.) at para. 12 [*Buss*]; *R. v. Agyeman-Anane*, 2009 CarswellOnt 5956, [2009] O.J. No. 6005 (Ont. S.C.J.) at paras. 4-6 [*Agyeman-Anane*].

[43] *R. v. Hudson*, 2005 CarswellOnt 7378, 77 O.R. (3d) 561 (Ont. C.A.) at para. 35, quoting *Deghani v. Canada (Minister of Employment & Immigration)*, 1993 CarswellNat 57, 1993 CarswellNat 1380, [1993] 1 S.C.R. 1053 (S.C.C.).

[44] *R. v. Leask*, 2008 ONCJ 25, 2008 CarswellOnt 415 (Ont. Ct. J.) [*Leask*]; *R. v. Bares*, 2008 CarswellOnt 1265, [2008] O.J. No. 900 (Ont. S.C.J.); *R. v. Mozo*, 2010 CarswellNfld 447, [2010] N.J. No. 445 (N.L. Prov. Ct.) [*Mozo*]; *R. v. Whittaker*, 2010 NBPC 32, 2010 CarswellNB 489 (N.B. Prov. Ct.) [*Whittaker*]; *R. v. Appleton*, 2011 CarswellOnt 11191, 97 W.C.B. (2d) 444 (Ont. S.C.J.) [*Appleton*]; *R. v. Moroz*, 2012 ONSC 5642, 2012 CarswellOnt 12614 (Ont. S.C.J.) [*Moroz*]; *R. v. Saikaley*, 2012 ONSC 6794, [2012] O.J. No. 6024 (Ont. S.C.J.) [*Saikaley*]; *Buss*, *supra* note 42.

[45] Strictly speaking, the images in *Bares*, *ibid*, were not on a device but on a CD; however, the law was applied similarly.

[46] This result was very much a function of the facts of this case, *Appleton*, *supra* note 44. During a routine border search, a handgun had been found in a glove compartment of the accused's car. The CBSA officer was later handed the accused's cellphone and testified that he searched it "for information"; the court held this to be a search in furtherance of arrest, which required a warrant, and thus section 8 had been breached. However, the breach was minimal due to the accused's reduced expectation of privacy at the border, the limited intrusion into the phone and the officer's belief that he was acting in good faith.

the subject matter affected by the police investigational technique? Second, was the search reasonable, which breaks down to the three sub-questions of the *Collins*[47] test: i) was the search authorized by law; ii) was the law itself reasonable; and iii) was the manner in which the search was carried out reasonable?[48]

(i) Reasonable Expectation of Privacy at the Border

The first prong of a section 8 analysis is whether the accused had a reasonable expectation of privacy in the circumstances of the case, as a search is only a "search" that engages section 8 if there was a reasonable expectation of privacy.[49] It is well-established that the reasonableness of the expectation of privacy varies with the context,[50] not least at the border. As the British Columbia Court of Appeal stated in *R. v. Nagle*, "Border crossings are not *Charter*-free zones."[51] However, there is an odd streak around the applicability of section 8 in the context of the first-level searches, which appears to stem from *Simmons*. As set out above, in *Simmons* Chief Justice Dickson stated the following about the first-level inspection:

> [T]he routine of questioning which every traveller undergoes at a port of entry, *accompanied in some cases by a search of baggage and perhaps a pat or frisk of outer clothing*. No stigma is attached to being one of the thousands of travellers who are daily routinely checked in that manner upon entry to Canada and *no constitutional issues are raised*. It would be absurd to suggest that a person in such circumstances is detained in a constitutional sense and therefore entitled to be advised of his or her right to counsel [emphasis added].[52]

In remarking that "no constitutional issues are raised," Dickson C.J. was making the point that the first-level inspection was not a detention and therefore the *Charter* did not apply—in particular, section 10 of the *Charter*, but the

---

47 *R. v. Collins*, 1987 CarswellBC 94, 1987 CarswellBC 699, [1987] 1 S.C.R. 265 (S.C.C.) at para. 23; *R. v. Gomboc*, 2010 SCC 55, 2010 CarswellAlta 2269, 2010 CarswellAlta 2270 (S.C.C.) at para. 20.

48 This distillation is drawn from Steve Coughlan, *Criminal Procedure*, 3rd ed. (Toronto: Irwin, 2016) at 67, and see generally Chapter 4 [Coughlan]. See also Steven Penney, "Unreasonable Search and Seizure and Section 8 of the *Charter*: Cost-benefit Analysis in Constitutional Interpretation" in Errol Mendes & Stéphane Beaulac, eds, *Canadian Charter of Rights and Freedoms*, 5th ed. (Markham, ON: LexisNexis Canada, 2013) 745 [Mendes & Beaulac].

49 Coughlan, *ibid* at 67.

50 *Canada (Director of Investigation & Research, Combines Investigation Branch) v. Southam Inc.*, 1984 CarswellAlta 121, 1984 CarswellAlta 415, [1984] 2 S.C.R. 145 (S.C.C.) at 159 [S.C.R.] [*Hunter*].

51 2012 BCCA 373, 2012 CarswellBC 2859 (B.C. C.A.) at para. 81, leave to appeal refused 2013 CarswellBC 685, 2013 CarswellBC 686 (S.C.C.).

52 *Simmons*, *supra* note 37 at para. 27.

statement does seem to imply that no part of the *Charter* applies to the first-level inspection. It is not entirely clear, and it is important to note that the case itself dealt with a second-level search and whether and how sections 8 and 10 applied in that context; nothing else was said about the applicability of the *Charter* to first-level searches. The statement has nonetheless been interpreted as meaning that *Charter* rights simply do not apply to the first-level search. In *Jones* Justice Doherty cited this part of *Simmons* and stated:

> The first, or least intrusive level of that action, involves routine questioning of travellers, the search of their luggage, and perhaps a pat-down search of the person. If state action involves only this level of intrusion, *the rights protected by s. 10(b) and s. 8 of the Charter are not engaged* [emphasis added].[53]

Similarly, in *Nagle* the Court of Appeal remarked:

> In the context of border crossings, routine questioning, the search of baggage and pat-down searches are standard practices, applicable to every ordinary traveller, and is expected and tolerated by anyone wishing to travel internationally. This conduct by border agents *does not engage constitutional rights*, including detention, the right to counsel *or a reasonable expectation of privacy* [emphasis added].[54]

Perhaps unsurprisingly, it is not unusual to see the Crown relying upon this case law and urging upon the courts the proposition that section 8 of the *Charter* simply does not apply to the first-level searches.[55] And yet, the courts dealing with searches of devices have consistently treated section 8 as applicable to even the first-level searches. *Nagle*, though it dealt with the search of the accused's purse during a routine inspection, was a case of this sort and is cited in the device cases. Even after making the statement cited above, the Court of Appeal went on to assess the reasonableness of the search, noting along the way that:

> The expectation of privacy *is considerably lower* for an international traveller. *There is clearly some expectation of privacy*, which is addressed in many cases, commencing with *Simmons*, but no constitutional right to be free from the search of bags, purses, luggage or a pat down exists when one decides to cross a border [emphasis added].[56]

The key may be acknowledging that *Simmons*, a 1988 case, well pre-dates the section 8 methodology that we now use. Arguably starting with *R. v. Edwards* in 1996,[57] the threshold question about section 8's applicability is whether a traveller has a reasonable expectation of privacy—here, in their person, items on the person and in luggage (including electronic devices). The argument cannot be

---

[53] *Jones*, *supra* note 39 at para. 32, and see para. 37.

[54] *Nagle*, *supra* note 51 at para. 34.

[55] E.g. *Saikaley* and *Mozo*, *supra* note 44.

[56] *Nagle*, *supra* note 51 at para. 75.

[57] 1996 CarswellOnt 2126, 1996 CarswellOnt 1916, [1996] 1 S.C.R. 128 (S.C.C.).

that one simply does not have any expectation of privacy in these places, since they are paradigmatically "personal" and contain information going to one's biographical core. On this basis, even the first-level search is a "search" and thus engages section 8. Rather, the important point of *Simmons* is that due to the unique context of the border, the expectation of privacy is a very attenuated one. Accordingly, a standard first-level search impacts on what is already a reduced expectation of privacy and will most often be "reasonable" in its execution.

This helps to explain the result of *Nagle*, if not all of its language, as well as the usual approach of the courts in the device cases. In the context of electronic devices it also lays to rest the idea that the extremely powerful privacy interest with which the Supreme Court has imbued devices and their contents, laid out in the previous section, can simply evaporate when one arrives at the border; more on this below.

(ii) Was the Search Authorized by Law?

In the cases it is essentially taken as given that the first-level search is authorized by law because of the expansive search powers set out in the *Customs Act* as outlined above. The searches are in every case conducted without recourse to the "reasonable grounds to suspect" language in some of the provisions, and tend to be argued on the basis of section 99(1)(a) of the *Act* which permits warrantless searches of goods that have been "imported." However, the notion of "importation" does not correspond very well to items that an individual has on his/her person, even though the definition of "import" was amended to provide that taking a good out of Canada and returning with it "is an importation of those goods."[58] Section 99.3(1) seems to be the more applicable provision, and it has been suggested that basing the authority for these searches on section 99(1)(a) is an error in statutory interpretation.[59]

Another common point on statutory authorization is that the courts have consistently accepted that the search of a device is authorized on the basis that the statute speaks to examining "goods." In *R. v. Whittaker*,[60] for example, Chief Judge Jackson noted that the definition of "goods" in section 2 of the *Act* "includes. . .any document in any form," and that the dictionary definition of "documents" includes "a computer data file." Thus, computer files fell squarely into this definition and the search was authorized.[61] Other courts have made similar findings.[62] It will be suggested below that this is a particularly troubling application in light of the recent Supreme Court of Canada case law on devices.

---

[58] *Customs Act*, *supra* note 1, s. 12(3.1).

[59] Nader R. Hasan & Stephen Aylward, "Where We've Been and Where We're Going: New Frontiers in Digital Privacy and s. 8 of the *Charter*" (2016) at 11 (copy on file with author) [Hasan & Aylward].

[60] *Whittaker*, *supra* note 44.

[61] *Ibid,* at para. 8.

[62] *Leask, Appleton, Moroz, Saikaley, supra* note 44, and *Buss*, *supra* note 42.

One ticklish issue that has arisen in a couple of cases is where a "routine" secondary search occurred, not because the CBSA staff picked up on any "indicators" or decided to do a random check, but because they were given information by another law enforcement agency to the effect that the accused was suspected of criminal activity and essentially requested to do a "routine" search *to further the criminal investigation*. In *Moroz*,[63] for example, the police suspected that the accused possessed child pornography but were unsure whether they had grounds for a warrant. They conveyed this information to CBSA, which put a "Lookout" into the computer system. As a result the accused was automatically subjected to a "routine" search of his phone when he entered Canada[64] and a child porn image was found. The court did not accept the accused's argument that the presence of the police investigation imposed any standard of suspicion or belief upon the search, ruling that due to the routine nature of the search it did not matter how the CBSA officials came to decide to undertake it—they were empowered under section 99(1) to do it in any event.[65] The same finding was made on fairly similar facts in *Saikaley*,[66] where the court also relied on the "dual purpose search" doctrine from *R. v. Nolet*[67] to find that the search came under the authority of the *Customs Act* and therefore did not require any standard of suspicion or belief for the search.[68]

(iii) Reasonableness of the Law

In every reported case the courts have been at great pains to hold, while not always framing it as such, that the *Customs Act*'s authorization of first-level searches is eminently reasonable. The rationale applied always rests on the two-step policy justification explained above, typically citing both *Simmons* and *Jones*. First, the state has a powerful, sovereign interest in maintaining the integrity of its borders and protecting Canadians from the importation of illegal and/or harmful materials. Second, and stemming from the latter policy, there is an extremely attenuated expectation of privacy at the border generally, "lower than in most other situations,"[69] and in particular for people who are seeking to enter Canada. In *Jones* Justice Doherty held that the need for border protection was a principle of fundamental justice under section 7 of the *Charter*,[70] and distilled the situation to a *quid pro quo* proposition: "Persons seeking entry are

---

63 *Moroz*, *supra* note 44.

64 *Ibid,* at para. 5.

65 *Ibid,* at paras. 16-21, relying on *R. v. Sahota*, 2009 CarswellOnt 4989, [2009] O.J. No. 3519 (Ont. S.C.J.).

66 *Saikaley*, *supra* note 44.

67 2010 SCC 24, 2010 CarswellSask 268, 2010 CarswellSask 369 (S.C.C.) cited at para. 88.

68 *Saikaley* is apparently pending before the Ontario Court of Appeal; Hasan & Aylward, *supra* note 59.

69 *Simmons*, *supra* note 37 at para. 49.

70 *Jones*, *supra* note 39 at para. 31.

expected to submit to and co-operate with that state intrusion in exchange for entry into Canada."[71]

Courts also rely on the finding that a device is "good" for *Customs Act* purposes, not just as a way of demonstrating that the search is authorized by law, but as a means of demonstrating the reasonableness of the law. There is a great degree of comfort found in analogizing devices to suitcases or other objects that individuals might have with them.[72] However, this consideration tends to be discussed more as an aspect of the reasonableness of the search, considered in the next subsection.

(iv) Reasonableness of the Search

First-level customs searches of devices are nearly inevitably found to have been executed reasonably by those courts that consider them. This analysis has proceeded along two lines. First, judges have consistently rejected defence arguments that searches of their devices were more invasive, and produced a greater impact on privacy, than searches of their luggage. Justice Nadel's statements to this effect in *Leask* are demonstrative and have been cited frequently in subsequent cases:

> Exceptional storage capacity is what makes a computer such a potentially dangerous reservoir of the most pernicious forms of child pornography, viz videos and photographs. I reject the contention that a search of a computer is tantamount to a psychological strip or cavity search. In the context of a search at the border, the suggestion that a computer ought to be viewed an extension of one's memory is pure hyperbole. Moreover, the suggestion that searching a computer being imported into the country would cause fear and apprehension in a reasonable person is, to my mind, incredible and untenable. The kind of computer search conducted here required no special equipment and no special expertise. There is no suggestion that after such a search is performed there will be any damage or change to the condition or content of the computer.
>
> Moreover, any search at the border of one's pockets, carryall or baggage could result in all manner of personal and private items being surveyed or touched by a stranger and resulting in some level of embarrassment or a feeling of discomfort. I see no intrinsic difference between the effects of the computer search at issue here and the intrusiveness or the embarrassment attendant upon a search of a wallet or purse or the requirement to turn out of one's pockets or to be subjected to a detailed examination of the contents of one's suitcase. . .
>
> In brief compass, the search of Mr. Leask's computer was a routine border search for child pornography. It was no different than routine

---

[71] *Ibid,* at para. 30.

[72] See e.g. *Mozo*, *supra* note 44 at para. 12.

> searches conducted, without any prior reasonable suspicion, for other forms of contraband, including searches for firearms, explosives, narcotics, undeclared alcohol or tobacco or other goods that a traveller may seek to smuggle into Canada.[73]

While *Leask* itself is from 2008, it is odd that this passage has, indeed, been quoted so extensively by cases that came after the release of *Morelli* in 2010, given how completely inconsistent with *Morelli* it is.

Second, courts have often emphasized that the searches being considered were relatively un-intrusive, in the sense that they were "cursory" and did not change or impair the devices or their data in any way. This was cited specifically in the passage from *Leask*, quoted above. In *Buss* (the only post-*Vu* case, though it came before *Fearon*) Judge Oulton held that the case law established that a "non-destructive" routine search of a device at the border was reasonable.[74] While acknowledging the increased privacy interest in devices that had been found by the Supreme Court in *Morelli* and *Vu*, she distinguished those cases on the basis that what was being discussed was full forensic searches of computers, as opposed to "the type of brief cursory search of sent text messages, photo galleries and photos on a computer, generated by the device's own search capacity and relying on no tools or software"[75] which she was considering. Similarly, in *Whittaker* Chief Judge Jackson noted that while specialized software[76] had been used to search the device, "it did not alter or impair in any manner either the computers themselves or their contents, that is, the data stored."[77]

To the extent it can be discerned from the reported cases, this practice of "cursory" searches seems to be an act of voluntary restraint on the part of CBSA officials. In nearly all of the cases the "routine" search was confined to easily accessible parts of the device and terminated upon the finding of (usually) a single child pornography image, or in one case[78] drug trafficking-related evidence that the officers had been told to look out for. In *Buss*, a CBSA officer testified that CBSA policy is "to stop examination after one image is found."[79] This seems a reasonable and careful practice in the context of a search that can be made by the CBSA without reasonable grounds or even reasonable suspicion, and subsequent searches appear to be made under warrant. The scope of the search, then, is similar to that permitted by the Supreme Court in *Fearon* for a search

---

73 *Leask*, *supra* note 44 at paras. 15, 16, 18.

74 *Buss*, *supra* note 42 at para. 30.

75 *Ibid,* at para. 23. The search in *Vu* had, in fact, been a fairly cursory one and not forensic (*Vu*, *supra* note 10 at para. 72).

76 A program called "I see what you see," which at least in this case only searched the C: drive of a computer.

77 *Whittaker*, *supra* note 44 at para. 13.

78 *Saikaley*, *supra* note 44.

79 *Buss*, *supra* note 42 at para. 17.

incident to arrest, a comparison that will be useful when I propose a new set of analytical criteria for device searches at the border, below.

(c) Constructing a New Standard

As noted at the outset of this article, thus far in the case law the border context has remained untouched by the manner in which the Supreme Court has developed the privacy protections for electronic devices under section 8 of the *Charter*. The one decision released after *Vu* and *Spencer*, *Buss*, dealt with this sea change in only a perfunctory manner. It is high time that this situation was brought up to date. Despite the overall lower expectation of privacy at the border, computers are not truly "goods" as that term is defined in the *Customs Act*, are not analogous to suitcases, handbags or purses, and need to be treated with greater attention to the privacy interest attached to them. While on the reported facts of the *Philippon* case it is not clear whether a search even took place, the legality of the search will no doubt form an important backdrop to the ultimate ruling in the case.

While the developments in the law around search and seizure regarding devices have been significant, I would contend that nothing revolutionary is needed to adapt border searches and bring them in line with these developments. Rather, all that is required is careful attention to the established section 8 methodology, with an eye to properly weighing the privacy interest in devices against the state objectives in the border context. Mirroring section (b), above, below I set out a proposal for an analytical framework that might accomplish this.

(i) Reasonable Expectation of Privacy

It is trite indeed to recite *Hunter*'s holding that section 8 protects "people, not places,"[80] but it does emphasize that, at the border, the reasonable expectation of privacy inquiry is focused on the individual's body and on objects which they own and possess. It is also important not to forget the prophylactic function ascribed to section 8 in *Hunter*, the idea that section 8 should prevent unreasonable searches before they occur rather than simply provide remedies after; indeed, Chief Justice Dickson invoked this in *Simmons* itself, noting that the prophylactic function is "foremost" among the values that section 8 was designed to protect.[81] It may be that the border search case law generally has gone awry because of failure to adhere to these propositions. Starting with *Simmons* there was arguably too much attention to the relatively reduced level of privacy an individual enjoys at the border due to the powerful countervailing state interests. This is a fair enough point, but it has obscured the fact that there is, nonetheless, *some* reasonable expectation of privacy at the border, and that

---

[80] *Hunter*, *supra* note 50 at 159.

[81] *Simmons*, *supra* note 37 at para. 50.

fact alone means that the search of a device at the border—however "routine" or "cursory"—is a search nonetheless, and section 8 applies.

Practically speaking, it is well-known that most people travelling through a border will not be subjected to a search, since this would impede the desired efficiency of border processing. This statistical likelihood of being left alone is itself a form of reasonably-anticipated privacy. Moreover, people do not expect that they must, as a pre-requisite for entering or leaving the country, spill out absolutely every grain of their core of biographical information; rather, they reasonably expect that some lesser amount of privacy is attached to their persons, luggage and items they have brought with them.

Finally, as regards electronic devices specifically, in light of the recent Supreme Court jurisprudence it is fallacious to assert that there is no reasonable expectation of privacy in them or their contents. That much is obvious. In *Spencer* the court restated its 4-part framework for determining whether a reasonable expectation of privacy exists: 1) the subject matter of the alleged search; 2) the claimant's interest in the subject matter; 3) the claimant's subjective expectation of privacy in the subject matter; and 4) whether this subjective expectation of privacy was objectively reasonable, having regard to the totality of the circumstances.[82] Bearing in mind the case law canvassed in Section I, above, the reasonableness of an expectation of privacy in devices—and specifically in the information and data contained in them—is clear. Even though the "totality of the circumstances" must include the unique factors in play at the border, some expectation of privacy remains reasonable.

What is needed is a way of measuring the reasonably reduced expectation of privacy that exists at the border and the extent of permissible state intrusion into it. However, that is better accomplished with the *Collins* test, as considered below. Accordingly, the most principled argument to be made is that, to the extent that older case law such as *Simmons* and *Jones* appears to suggest that section 8 does not apply to routine border searches, it is out of keeping with the current law—and it is probably time for the Crown to stop arguing the contrary.

(ii) Collins Part 1: Is the Search Authorized by Law?

As noted earlier, the *Customs Act* explicitly authorizes the routine, groundless and warrantless searches being discussed here. The two apparently authorizing sections are set out below, for convenience:

> 99(1) 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 [. . .]
>
> 99.3(1) An officer may, in accordance with the regulations and without individualized suspicion, conduct a non-intrusive examination of goods

---

[82] *Spencer*, *supra* note 22 at para. 18.

> in the custody or possession of a person who is in or is leaving a customs controlled area.

Accordingly, section 99(1) allows searches of "imported goods," while section 99.3(1) provides for "a non-intrusive examination of goods in the custody or possession of a person who is in or is leaving a customs controlled area." Each explicitly authorizes a search of "goods" and the use of such a broad term by Parliament probably does carry the intent that essentially everything brought into a border area by an individual is caught, particularly when one considers that screening of materials is one of the primary objectives of the *Act*.

As will be seen below, my overall argument is that since the privacy interest in devices makes them profoundly different from other "goods" that an individual might have at the border, they deserve different treatment under section 8 than conventional "goods." Accordingly, it could be argued that they should be the subject of a separate defined term in the *Act* in order to convey this. However, the overall argument does not turn on this, since the courts themselves can and should treat devices differently for constitutional purposes whatever the definitional content of the *Act*.

The case law thus far has proceeded on the basis that devices are properly treated as "imported" goods under section 99(1)(a), with section 99.3(1) (a more recent addition to the *Act*) going un-considered, apparently serving as a back-up of some kind. There is some dissonance at play here, since despite the way in which section 99(1)(a) is framed, carrying a computer or cell phone with one for work or personal reasons does not easily comport with the idea of "importing goods"; if I bring a suitcase with my own clothes or a briefcase with work materials across the border, I am hardly an importer as that term is colloquially understood. I do not need to pay duty on it, nor do I need to declare it on my Customs card. Moreover, treating section 99(1)(a) as the authorization for searching items located on an individual's person arguably renders section 99.3(1) redundant,[83] other than that it specifically refers to a customs-controlled area.

Accordingly, while it seems clear that the routine search of a device is authorized under the *Act*, section 99.3(1) is the more appropriate section from which to draw the authority. That the search in the latter section is required to be "non-intrusive" figures neatly into the reasonableness analysis set out below.

(iii) Collins Part 2: Is the Law Itself Reasonable?

Thus we arrive at the crux of the matter: how to balance the significant individual privacy in devices with the intense state interests in border security and all that accompanies it. There is no doubt that the state's interests in protecting the border must shape its interactions with individuals and their privacy interests at border crossings. It is both logical and desirable that the state may more reasonably interfere with privacy in this setting. Yet while this shapes the

---

[83] Hasan & Aylward, *supra* note 59.

contextual privacy at play, it is important to remember that the inherent informational privacy interest an individual has in the contents of their device does not shrink; as Fric notes, "The qualities of a computer that invite heightened privacy interests in the information it contains are not magically transformed when an individual seeks entry into Canada."[84] To borrow an analogy from Justice Binnie, as state interest in regulating borders advances, privacy in devices does not recede.[85]

In the case law to date the courts have consistently rejected the argument that a search of a device is properly placed in the context of the second-level *Simmons* search, "tantamount to a psychological strip or cavity search" as Justice Nadel put it in *Leask*.[86] This is probably correct, at least in terms of the cursory scope of the search as it is usually done. On the other hand, however, a device search sits uneasily at the border of what would be considered a "routine" search, due to the privacy interest. In *Fearon*, it is worth remembering, the court decided that a cell phone search incident to arrest was not as intrusive as a strip search incident to arrest (which is *necessarily* humiliating and degrading) but it was still sufficiently more intrusive than other searches to require special rules beyond the ordinary ones.[87]

While it is not appropriate to over-emphasize the "external situation in which the search occurs,"[88] in my view the key point of this context was hit upon by Justice Doherty in *Jones*, when he remarked, "In a general sense, everyone who is questioned at the border and whose luggage is examined is the target of an investigation."[89] Border scrutiny is a quasi-law enforcement activity; in fact, it is related in species to the deployment of sniffer dog searches that was considered by the Supreme Court of Canada in *R. v. Brown*,[90] *R. v. M. (A.)*[91] and *R. v. Chehil*.[92] In that setting, as Justice Karakatsanis wrote in *Chehil*, the section 8 law strikes a balance "between society's interest in routine crime prevention and an individual's interest in her own privacy."[93]

It is probably not useful to torture the analogies between the use of sniffer dogs in airports and other border settings outside the customs area, and the screening of travellers within the fairly different setting of the actual border

---

84 Fric, *supra* note 35 at 76.

85 In *R. v. Handy*, 2002 SCC 56, 2002 CarswellOnt 1968, 2002 CarswellOnt 1969 (S.C.C.), Justice Binnie was considering the admissibility of similar fact evidence and stated, at para. 149: "As probative value advances, prejudice does not necessarily recede."

86 *Leask*, *supra* note 44, para. 15, and see *Buss*, *supra* note 42.

87 I owe this observation to Steve Coughlan.

88 Fric, *supra* note 35 at 76.

89 *Jones, supra* note 39 at para. 40.

90 2008 SCC 18, 2008 CarswellAlta 523, 2008 CarswellAlta 524 (S.C.C.).

91 2008 SCC 19, 2008 CarswellOnt 2257, 2008 CarswellOnt 2258 (S.C.C.)

92 2013 SCC 49, 2013 CarswellNS 693, 2013 CarswellNS 694 (S.C.C.).

93 *Ibid,* at para. 2.

crossing. What is useful, however, is the balance that was struck by the court in the sniffer dog scenario, which was accomplished by imposing a standard of "reasonable suspicion" on the searches. The justification for using this standard for devices is similar enough to that used in the sniffer dog cases; as Professor Coughlan states it, "where the impact of a search on a person's privacy interests is seen as relatively minimal, the standard for being allowed to search is lower."[94] "Reasonable suspicion," as it has been constructed by the Supreme Court, seems tailor-made for the border device search scenario: it must amount to more than a generalized suspicion and be based on objectively reasonable facts within the totality of the circumstances; even potentially innocent factors (nervousness, failure to make eye contact) can be taken into account; and officer training about criteria to look for can be taken into account, so long as they are sufficiently proven.[95]

In fact, "reasonable suspicion" bears a startling resemblance to the constellation of factors that CBSA personnel look for in deciding to refer an individual to a "secondary" search,[96] and it is also the standard that is set out in the other search provisions of the *Customs Act*. Thus, it is a standard that is easily articulable and which the CBSA has experience applying. It is lower than "reasonable and probable grounds," reflecting the reduced privacy in the border context, but requires more than pure discretion, which suits the heightened privacy interest in devices. It follows, then, that a search of a device will only take place as a "secondary" search, following the determination of reasonable suspicion by the official.

The effect of this proposal is to read a requirement of "reasonable suspicion" into either of section 99(1) or section 99.3(1) (whichever is the appropriate authorizing provision, as discussed above), but only where that search power is invoked regarding a device. This proposal might also solve the "ancillary search" problem raised by cases like *Moroz* and *Saikaley*, since the CBSA using information obtained from other law enforcement personnel would be more amenable to justifying a formalized search standard than the current, rather surreptitious, practice.[97]

A reasonable suspicion standard, however, has also been held to be appropriate because of the comparatively lower level of invasiveness in those

---

94 Coughlan, *supra* note 48 at 140.

95 Drawn from *ibid* at 140-141.

96 See *Buss* and *Agyeman-Anane*, *supra* note 42 and accompanying text.

97 Analogously, police have powers to randomly stop vehicles under provincial highway legislation, but if they form actual suspicion about a particular vehicle then they cannot rely on the random stop power, but must show that they have reasonable suspicion; see e.g. *R. v. Schaeffer*, 2005 SKCA 33, 2005 CarswellSask 154 (Sask. C.A.), *R. v. Houben*, 2006 SKCA 129, 2006 CarswellSask 746 (Sask. C.A.), *R. v. Schell*, 2006 SKCA 128, 2006 CarswellSask 742 (Sask. C.A.), *R. v. McCammon,* 2013 MBCA 68, 2013 CarswellMan 357 (Man. C.A.) and *R. v. Papilion*, 2014 SKCA 45, 2014 CarswellSask 260 (Sask. C.A.).

situations, e.g. dog sniffer searches, where it is applied. This is best dealt with at the final *Collins* stage, regarding the manner of search.

(iv) Collins Part 3: Is the Search Carried Out in a Reasonable Manner?

The other means of striking the correct balance of state interests and individual privacy in devices, in my view, is to restrict the scope of the search. While it seems almost too easy a solution to graft existing law onto the border, the court's framing of cell phone searches as part of a search incident to arrest in *Fearon* offers a useful framework. Recalling Justice Doherty's *dictum* that everyone at the border is under investigation in some sense, combined with the very low expectation of privacy, gives the border search context a similar contextual flavour to the arrest context. First, the search incident to arrest, said the court in *Fearon*, must be "truly" incidental, in that the search must be necessary to further the arrest. Here, the search should only occur if the CBSA officer has a reasonable suspicion that contraband is being smuggled or some other statutory breach has occurred/is under way, and so the search of the device should be clearly linked to this purpose.

Second, the search is not open-ended, but rather is limited to the more basic apps on the device—sent and draft emails and texts, photos, call logs, note-taking apps and anything similar. As noted above, this is quite consistent with the way in which CBSA searches are currently conducted, and suits the major concern at play, which is that contraband (almost inevitably child pornography) is being smuggled in on the device. It also comports with section 99.3(1)'s requirement that the search be "non-intrusive." The search should stop, naturally, when any actual contraband is found, and a warrant obtained for further search (no doubt following an arrest). Similarly, any search of the device exceeding this "cursory" search, such as forensic analysis or mirroring the hard drive, would require reasonable and probable grounds and a warrant.

Restricting the scope in this way also provides a means to avoid a fairly major problem that, while it has gone mostly unaddressed in Canadian case law, has significant international ramifications, which is often referred to as "the portal problem." As the Supreme Court noted in *Vu*, part of the privacy problem with devices is that they are often networked or connected to the internet, which expands the scope of what can be searched. The cell phone or computer of a traveller at the airport, then, might have apps containing banking information, or which allow access to social media accounts, streamed software tools or other cloud-stored data. Importantly, the data itself may actually be located in another country, and by searching too obtrusively the CBSA official might be engaged in gathering evidence from the other state. As innocuous as it seems to the eye, this is a major point of contention in international law enforcement circles,[98] since

---

[98] See generally Robert J. Currie, "Cross-Border Evidence Gathering in Transnational Criminal Investigation: Is *Microsoft Ireland* the 'Next Frontier'"? (forthcoming); Bertrand de la Chapelle & Paul Fehlinger, *Jurisdiction on the Internet: From Legal Arms*

there is a solid prohibition of cross-border evidence-gathering under customary international law which is taken very seriously by governments around the world.[99] Restricting the scope of the search can at least help Canadian officials avoid this problem—and this is easily accomplished by simply disabling the device's access to the internet prior to the search beginning, which limits the search to data that is actually stored on the device.

Finally, in *Fearon* the court underscored the importance of after-the-fact review of such searches where they turn up evidence of an offence, due to the fact that "we are dealing here with an extraordinary search power that requires neither a warrant nor reasonable and probable grounds."[100] "[A]s a constitutional imperative," Cromwell J. required the police to keep "detailed notes of what they have examined," which "should generally include "the applications searched, the extent of the search, the time of the search, its purpose and duration."[101] This seems entirely suited to the border device search setting, since the same "constitutional imperative" is present. Notes can be kept with reasonable ease by the CBSA officer conducting the secondary search; in fact, there might be technological solutions to keep the search efficient, such as by hooking the phone to computer software that records the details of the search, or even something as simple as a video recording of the search[102] (which could itself be done on something as portable as a smart phone).

While the foregoing framework may not be perfect, it is at least a starting point on the path towards accommodating the new "digital reality" that confronts Canadian society at the border, which thus far has gone undisturbed by thorough *Charter* analysis. It is, however, a fairly modest proposal, acknowledging the importance of the state's interest in border security and

---

Race to Transnational Cooperation, Global Commission on Internet Governance Paper Series No. 28 (April 2016); Kate Westmoreland and Gail Kent, "Foreign Law Enforcement Access to User Data: A Survival Guide and Call For Action" (2015) 13:2 Canadian JL & Technology 225; Bert-Jaap Koops & Morag Goodwin, *Cyberspace, the cloud and cross-border criminal investigation: The limits and possibilities of international law* (Tilburg: Tilburg University, 2014); Cybercrime Convention Committee (T-CY), *Transborder access and jurisdiction: What are the options?* (6 December 2012), Doc no T-CY (2012). Courts are beginning to acknowledge this issue; see *Riley*, *supra* note 33 at 2491.

99 The U.S. and U.K. are currently seeking to create a treaty to address this issue; see Ellen Nakashima & Andrea Peterson, "The British want to come to America—with wiretap orders and search warrants," *The Washington Post* (4 February 2016), online: < https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america–with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html > .

100 *Fearon*, *supra* note 10 at para. 82.

101 *Ibid.*

102 Nader Hasan has proposed this as a means of enhancing the after-the-fact review of searches incident to arrest, noting that it is a means to ensure the search is narrowly tailored and may, in fact, be "less cumbersome and less time-consuming than requiring officers to capture the same information in their notes" (Hasan, *supra* note 9 at 472).

integrity, which after all is of pressing concern to Canadians. In essence, it simply applies the standard of reasonable suspicion (which already attaches to most customs searches) to all searches of electronic devices on the person or in the custody of people crossing the border, and provides that the search can only be of limited scope and duration. It is fairly close to CBSA's current practices, but is probably superior in that it ensures that this invasive kind of search is authorized by law and underpinned by actual grounds to believe something is awry; random searches of devices should not be permitted, just as random searches of our houses and body cavities are not permitted.

III. UNLOCK THIS! COMPELLING PASSWORDS

Having proposed a framework for the legality of device searches at the border, it is worth considering the main issue in the *Philippon* case: could the accused be compelled to unlock his phone? Recall that this is the main issue because Philippon was charged, under section 153.1(b) of the *Customs Act*, that he "hinder[ed] or prevent[ed] an officer from doing anything that the officer is authorized to do under" the *Act*. For the purpose of argument, I will assume that the CBSA officer in question had a reasonable suspicion that grounded the search of Philippon's cell phone (though no facts of that nature emerge from the media coverage), and thus that the section 8 framework suggested above was complied with. Even if the search was lawful, however, Philippon is only guilty of "hindering or preventing" if the CBSA officer was authorized to compel the phone's password, and if Philippon had a legal duty to do anything beyond refusing to provide the password.

By way of background, it is worth remembering that the *Customs Act* imposes a number of duties on individuals to do things that would facilitate their scrutiny by CBSA agents. In particular, sections 11 and 13 require people to submit to questions, answer the questions honestly, and with regard to imported goods that have been reported as such, to, "if an officer so requests, present the goods to the officer, remove any covering from the goods. . .or open or unpack any package or container that the officer wishes to examine" (section 13(b)). As the known facts of the *Philippon* case demonstrate, CBSA appears to have used these provisions (or some part of the *Customs Act*) as authority for demanding that people unlock their password-protected devices. The case is reminiscent of *Whittaker*, where the CBSA official told the accused he was required to provide passwords for his computers or else be arrested for "hindering a CBSA officer in the execution of his duties," and the computer would be sent "to CBSA experts to search."[103] It is important, then, that these are first-level "routine" searches

[103] *Whittaker*, *supra* note 44 at para. 4. The assumption here is that section 13 is being used by CBSA as the authority for compelling individuals to unlock the device. Section 11 requires individuals to answer questions honestly, but appears to be oriented towards acquiring information. Section 11 does not seem geared towards the question "What is the password to your computer?" which is truly directed at facilitating the search rather than acquiring information.

under section 99(1), since the reasoning being used by CBSA appears to be as follows: section 13 requires individuals to facilitate the search of any "goods" that a CBSA official wishes to inspect; a device is a "good;" in order to inspect a password-locked device the officer must have the password; therefore the individual is required to provide the password. There appears to be no similar requirement attached to the searches in the *Act* that proceed explicitly on the basis of reasonable suspicion.

The question, of course, is whether this reasoning holds up, since the idea of being compelled to help the state find evidence against you smacks strongly of a violation of the principle against self-incrimination. This argument was made in *Buss*, where the accused voluntarily gave up the passwords to his phone and computer, but claimed that his right to be free from self-incrimination under section 7 of the *Charter* had been infringed. The court tersely dismissed this argument on the basis that a routine search in the border context did not amount to a detention or trigger any *Charter* rights arising therefrom.[104]

Is this constitutionally satisfactory? A great deal depends, in my view, on what is being searched. Traditionally, this regime permits a CBSA agent who has formed the desire to search someone's luggage, briefcase or wallet—and therefore has likely begun a secondary inspection—to simply ask the individual to open the suitcase, briefcase or wallet. No doubt on a daily basis such inspections reveal problems that get people charged or arrested, whether for items on which duty was not paid, animal parts, drugs or anything else which an individual might have and/or be trying to smuggle into Canada. We know from *Jarvis*[105] that compelling individuals to facilitate warrantless searches for regulatory purposes is *Charter*-compliant up to the point at which penal jeopardy is engaged. The regulatory purpose, screening people and items at the border, is an important one and routine searches are a part of it. So long as the process shifts to a proper criminal investigation once the contraband is found, it might be argued, then compelling the unlocking of the phone is consistent with that regulatory purpose. If a cell phone is indeed a "good," and no different from a briefcase, then while section 13 of the *Customs Act* is a bit unspecific, it may be reasonably good authority to compel the password. On this reasoning, Philippon may be guilty.

As has been argued above, however, a device is not like a briefcase. The Supreme Court stated clearly in *Vu* that a computer is not like a filing cabinet,[106] which obviously means it is not like a briefcase or suitcase either. I have suggested above that the intense informational privacy interest in devices necessitates the formation of reasonable suspicion to ground a cursory search of a device at the border. By "reasonable suspicion" is meant "reasonable suspicion

---

[104] *Buss*, *supra* note 42 at paras. 32-35.

[105] *R. v. Jarvis*, 2002 CarswellAlta 1440, 2002 CarswellAlta 1441, [2002] 3 S.C.R. 757 (S.C.C.).

[106] *Vu*, *supra* note 10 at paras. 24, 44.

that the individual has contraband or illegal material, or is breaking or has broken some criminal or quasi-criminal law, grounded on objectively reasonable facts." Searches of devices should not be permitted randomly or on the basis of some mild suspicion, curiosity or personal whim on the part of a CBSA agent.

From a statutory interpretation point of view, then, the term "goods" should not be interpreted as including devices. Section 13 explicitly applies to *imported* goods, and as argued above a device carried with an individual is no more an "imported good" than a pair of shoes that one wears on a business trip or vacation. Also, section 13 only applies to "imported goods" *which have been reported as such under section 12*. Just as one does not report one's shoes as "imported goods," one does not report one's personal device as an imported good.[107] Section 99.3(1), which allows a non-intrusive search of goods in a person's custody or possession, contains no language compelling the individual to open or unpack the goods. Accordingly, a duty to facilitate inspection of "imported goods" may not apply at all.

If any of this is correct, then while the state may be empowered to search the device, there is no corresponding power to compel the individual to facilitate the search. As the Supreme Court stated in *R. v. Mann*, "Absent a law to the contrary, individuals are free to do as they please. By contrast, the police (and more broadly, the state) may act only to the extent that they are empowered to do so by law."[108] Accordingly, if the police come to my house with a search warrant and I refuse to unlock the door, they may indeed batter down the door and enter the house, since a court has given them authority to do so, but they may not compel me to unlock the door. Similarly, if CBSA has the authority to search my phone or computer, they can probably seize it, utilize whatever software or forensic means are necessary to "crack" the password and do the search—but they cannot compel me to unlock it.

A demand for the password, so that the CBSA agent can unlock it him/herself, would have the same effect and would even more directly infringe the principle against self-incrimination. Unless a *Charter* caution was read and the accused voluntarily gave up his right to remain silent and agreed to facilitate the investigation, this would simply be a conscripted statement and in breach of section 7.[109] By comparison, even in the context of an otherwise lawful investigative detention, an individual does not have to answer questions.[110]

---

[107] Possibly excepting the situation where one bought the device in the foreign state from which one is coming.

[108] *R. v. Mann*, 2004 SCC 52, 2004 CarswellMan 303, 2004 CarswellMan 304 (S.C.C.) at para. 15.

[109] Carissima Mathen, "Section 7 and the Criminal Law" in Mendes & Beaulac, *supra* note 48 at 715-716. I emphasize that this is an argument and that this question, to the limited extent it has come up thus far, is unsettled. In *R.* c. *Boudreau-Fontaine*, 2010 QCCA 1108, 2010 CarswellQue 5672, 2010 CarswellQue 15139 (C.A. Que.) Doyon J.A. held that a target cannot be compelled to produce passwords under a search warrant, as this would violate the principle against self-incrimination (para. 39). My research has not uncovered similar findings elsewhere in Canada, however. The English Court of Appeal has held

The argument might be raised that this slightly more restrictive interpretation will create unnecessary mischief and deprive the state of an important border screening power, since individuals would simply refuse to unlock their device or provide the password and (at least potentially) escape scot-free with whatever contraband or evidence is on their device. This should not be a large concern, however. What is proposed is that CBSA officials may not search a device until they have formed a reasonable suspicion about its contents. At that point, as argued above, they have the legal authority to do a cursory search, and they can likely continue their current practice of telling the individual that either he/she can unlock the phone or it can be taken away and searched. The latter option is likely to be time-consuming and presumably most people would voluntarily unlock the device and submit to the cursory search rather than be deprived of it.

What would be unacceptable, however, would be an individual facing conviction under section 153.1 of "hindering or preventing" a CBSA officer's duties based on their refusal to do something that the state has no power to compel them to do. On this argument, then, Alain Philippon could not be found guilty of the offence with which he is charged.

IV. CONCLUSION

The protection and security of Canada's borders engages a set of public interests that are quite distinct from those involved in the day-to-day life of Canadians within those borders, and which interact uneasily with the protection of personal privacy under section 8 of the *Charter*. While there is jurisprudence on these matters, the Supreme Court's recent case law on the protection of privacy in electronic devices has not yet seen any significant consideration in the border context. Given the incredible permeation of our lives by devices it is inevitable that such consideration will happen, because it is needed; the intense media interest in the case of Alain Philippon tells us that, even if it tells us nothing else.

The central argument of this article, however, has been that the Philippon case does indeed tell us something else, in particular because it provides a solid

---

that an encryption key "exists separately from each defendant's will," and thus is neutral and non-incriminating: *R. v. S. (F.)*, [2008] EWCA Crim 2177, [2009] 1 W.L.R. 1489, and see discussion of the overall U.K. position in Andrew L-T Choo, *The Privilege Against Self-Incrimination and Criminal Justice* (Portland, OR: Hart Publishing, 2013) at pp. 46-50. The situation in the U.S. is mixed, but one court has found that device passcodes were testimonial in nature and thus subject to self-incrimination protections: *Securities and Exchange Commission v. Bonan Huang et al.*, Civil Case No. 15-269 (September 23, 2015, E.D. Pa.). However, another court was prepared to find the password to be simply analogous to a lock on a suitcase, in the border context: *United States v. McAuley*, 563 F.Supp.2d 672 (W.D. Texas, 2008).

[110] *R. v. Suberu*, 2009 SCC 33, 2009 CarswellOnt 4106, 2009 CarswellOnt 4107 (S.C.C.) at paras. 27-29.

platform for considering: 1) under what conditions can CBSA officials search devices as part of normal screening procedures (and outside the standard warranted search in a criminal investigation)?; and 2) does an individual subject to such a search have to unlock a password-protected device in order to facilitate it? The best answer to the first question, I have argued here, is arrived at by subjecting the first-level border search to the established section 8 jurisprudence and adapting it conservatively but appropriately. Accordingly:

- individuals do have a reasonable expectation of privacy in the contents of their devices and therefore the routine first-level inspection is nonetheless a "search" and section 8 applies;
- the first-level inspection is authorized by law, specifically the *Customs Act*, but the invocation of section 99(1)(a) by the Crown and the courts may be an error in statutory interpretation, and section 99.3(1) is the more appropriate authority;
- in any event, the law will only be reasonable where the search is carried out on the basis that the official has reasonable grounds to suspect that the device contains illegal material or evidence of an offence;
- the search will also only be executed reasonably if carried out analogously to the search incident to arrest standards from *Fearon*, i.e. that it includes only sent and draft emails and texts, photos, call logs, note-taking and anything similar. Detailed notes—or perhaps even a video-recording—should be taken of the search. Officials should be careful to avoid searching items/apps that will obviously access cloud-stored data, probably by disabling the device's internet access functionality.

This article has been focused on Canadian law and has not engaged significantly with the American jurisprudence on point. However, as it was being finalized a U.S. case emerged that employs a similar methodology to the one proposed here. In the 3 June 2016 decision in *U.S. v. Ramos*,[111] the accused had his cell phone searched after being arrested for drug trafficking at the border, and challenged the search on the basis that a warrant was required. District Court Judge Miller attempted to rationalize recent case law regarding device and border searches, in particular the U.S. Supreme Court's decision in *Riley*[112] which highlighted a heightened level of privacy in devices and their data in a manner similar to that of the Supreme Court of Canada. In deciding that a standard of reasonable suspicion should apply to all searches of cell phones at the border, Judge Miller stated:

> Adopting the reasonable suspicion standard currently used only for forensic examinations of digital devices, see *Cotterman*, 709 F.3d at 968, as the standard for all border searches of cell phones, may be a prudent way to harmonize *Riley*'s concerns with the salutary border search

---

[111] — F.Supp. 3d —, 2016 WL 3552140 (U.S. Cal. D., 2016). I am grateful to Professor Norman Abrams for bringing this case to my attention.

[112] *Riley*, *supra*, note 34.

> principles. First, the privacy interests involved in searches of modern cell phones are present both during manual and forensic searches. While a forensic examination is more intrusive, a manual search of a modern cell phone certainly exposes the same type of information discussed in *Riley* — messages, photos, contacts list, call logs, etc. — both in isolated form and in combination. Accordingly, a manual search can be just as invasive as a full forensic examination. . .
>
> Second, current Ninth Circuit law on border searches requires no suspicion at all for manual searches of cell phones. . .*Riley*'s threshold recognition that cell phone searches are inevitably intrusive suggests the concept of a "routine" cell phone search provides little guidance to law enforcement officials and courts.
>
> Finally, from the practical point of view, reasonable suspicion represents a workable standard, as it would allow customs officials to predictably do their job while affording a heightened level of privacy protection suggested by *Riley*. According to the Department of Homeland Security, "officers very likely do have reasonable suspicion in most searches of electronic devices based on existing screening methods and objective factors." See Thomas Mann Miller, Digital Border Searches After Riley v. California, 90 Wash. L. Rev. 1943, 1996 (2015), citing Government Data Regarding Electronic Device Searches, ACLU. Thus, requiring reasonable suspicion for forensic and manual searches would likely impose only minimal burdens on customs officials' current methods.[113]

On the second question, the only authority apparent in the *Customs Act* for compelling individuals to unlock their devices to facilitate inspection is section 13, which is explicitly about "imported goods" that have been reported as being imported under section 12. It is highly doubtful whether a device can be properly interpreted as coming within the definition of either "goods" or certainly "imported goods." There is therefore no statutory requirement to unlock the device, and any purported common law power would appear to be unconstitutional. Accordingly, individuals are not required to provide passwords or otherwise unlock devices in order to facilitate a search.

In the end, if this argument is correct or even moves in the right direction, one thing it points to is the need to reconsider and re-draft the *Customs Act*. The issue of how electronic devices should be treated at the border demonstrates that the piecemeal amendments that the *Act* has seen over previous decades are not sufficient for current purposes, as its language is becoming increasingly antiquated. As regards the search provisions, in particular, revision in line with an understanding of technological realities and current constitutional norms is probably overdue.

---

[113] *Ibid.*

POSTSCRIPT

As this article was going to press, a number of developments emerged which should be flagged, even though it was too late to incorporate them into the overall article. First, to the disappointment of a number of criminal lawyers who were watching the case (including the present author), Alain Philippon pleaded guilty to the *Customs Act* charge and received a fine of $500.00.[114] In the agreed statement of facts underpinning the plea, it was noted that when he was stopped at the airport, Philippon had two cell phones and $5,000.00 in cash, and there were traces of cocaine on his luggage. Under the analytical framework I have proposed here, these facts would certainly have provided a reasonable suspicion justifying a cursory search—and, in fact, CBSA indicated that they were still retaining the phone.[115] However, even if that search framework is correct, the question of compelling the password will have to await a future case.

Or will it? In August 2016 the Canadian Association of Chiefs of Police proposed that Parliament pass a new law that would compel people to disclose their passwords or encryption keys to police, once judicial authorization was obtained.[116] The proposal saw robust public debate, and not unexpectedly it has been criticized as overly corrosive of individual privacy.[117] However, the most interesting point was the concession by RCMP Assistant Commissioner Joe Oliver that "[t]here is nothing currently in Canadian law that would compel someone to provide a password to police during an investigation."[118] This certainly makes it more doubtful that CBSA has the corresponding power in first-level border searches.

In fact, it appears that the CBSA itself is in some disarray on this issue. Also in August 2016, in an article touching on the Philippon case, the British Columbia Civil Liberties Association (BCCLA) revealed the contents of freedom of information requests that had obtained various operational information from CBSA.[119] This included statements to the effect that CBSA felt it had the authority to compel passwords, but acknowledged that the law on point was not

---

[114] Brett Ruskin, "Alain Philippon pleads guilty over smartphone password border dispute," *CBC News* (15 August 2016) online: < http://www.cbc.ca/news/canada/nova-scotia/alain-philippon-to-plead-guilty-cellphone-1.3721110 > .

[115] *Ibid.*

[116] "Police chiefs want law that would force people to reveal passwords," *The Globe & Mail* (16 August 2016), online: < http://www.theglobeandmail.com/news/national/police-chiefs-want-law-that-would-compel-people-to-reveal-passwords/article31428735/ > .

[117] See, e.g., Nader Hasan & Stephen Aylward, "Password protection a crucial Charter right," *Toronto Star* (23 August 2016), online: < https://www.thestar.com/opinion/commentary/2016/08/23/password-protection-a-crucial-charter-right.html > .

[118] *Supra* note 116.

[119] Micheal Vonn, "What Happens If You Don't Provide Your Cellphone Password to Border Agents?", British Columbia Civil Liberties Association (25 August 2016), online: < https://bccla.org/2016/08/what-happens-if-you-dont-provide-your-cellphone-password-to-border-agents/ > .

clear. Moreover, as of 25 June 2015 CBSA officials were instructed not to charge anyone under s. 153.1 of the *Customs Act* for failing to surrender a password, until the law was clarified "in ongoing court proceedings" (apparently a reference to the Philippon case itself).[120]

All of this suggests two things. First, it provides support for the argument made here that compelling passwords in customs searches is not permitted under Canadian law as it stands. Second, as encryption technology becomes more advanced and makes it difficult for law enforcement to forensically "crack" devices that they have lawful authority to search, the state will increasingly seek powers to compel individuals to cooperate and unlock the devices. The extent to which privacy will be traded away to facilitate law enforcement in this setting will, as always, bear watching.

---

[120] *Ibid*. It is worth noting that the information also revealed that CBSA agents were under instructions to limit their searches to the contents of the devices themselves and avoid viewing or obtaining any data by way of internet connection. This is a salutary limitation which comports with the search limits I proposed in section 3(c)(iv), above.