Canadian Journal of Law and Technology

Volume 18 | Number 1

Article 3

6-2020

Searches of the Person: A New Approach to Electronic Device Searches at Canadian Customs

Justin Doll

Follow this and additional works at: https://digitalcommons.schulichlaw.dal.ca/cjlt

Part of the Computer Law Commons, Intellectual Property Law Commons, Internet Law Commons, Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation

Justin Doll, "Searches of the Person: A New Approach to Electronic Device Searches at Canadian Customs" (2020) 18:1 CJLT 91.

This Article is brought to you for free and open access by the Journals at Schulich Law Scholars. It has been accepted for inclusion in Canadian Journal of Law and Technology by an authorized editor of Schulich Law Scholars. For more information, please contact hannah.steeves@dal.ca.

Searches of the Person: A New Approach to Electronic Device Searches at Canadian Customs

Justin Doll*

1. INTRODUCTION

What goes through your mind at customs? As you wait in that folded line, edging closer to a row of enclosed booths manned by uniformed officers, surrounded by security cameras and warning signs? Perhaps you're trying to act naturally, then wondering if it shows? Perhaps you're mentally recalculating the amount you've scribbled onto your customs declaration? Or perhaps you're exhausted from your flight, maybe nursing a bit of a hangover, not thinking about much at all? When you finally get to the front of the line, how do you expect your conversation with the customs officer to go?

According to Canadian law, one thing that you have in this moment, whether you're thinking about it or not, is an expectation of privacy. And if search and seizure law can be distilled into a single question, it is whether your expectation of privacy is reasonable at any given moment. This paper discusses the expectation of privacy that travellers have at Canadian customs with respect to their electronic devices.

The paper proceeds first with an examination of two foundational Supreme Court of Canada cases, *Hunter* and *Simmons*. The paper then examines how the lower courts have interpreted these foundational cases so as to apply to searches of electronic devices (something not anticipated by the foundational cases themselves, which were decided in the 1980s). The paper then discusses more recent Supreme Court jurisprudence addressing the unique privacy considerations posed by modern technology outside of the customs context. The paper then examines different proposals for modifying the way that device searches are conducted at customs in order to comport with this more recent Supreme Court jurisprudence. Finally, the paper concludes by offering a new proposal for change, which relies heavily on a reassessment of the foundational cases.

In short, travellers have strong privacy interests in their devices, and customs searches should not be undertaken as a routine matter. Through either revised legislation or judicial interpretation, device searches at Canadian customs should be treated as being analogous to "searches of the person." As such, a device search at customs (a) should require that a customs officer form a "reasonable suspicion" of a contravention of customs law before initiating a search, (b) should be subject to a traveller's right to request a review of the custom officer's

^{*} Justin Doll, BA, LLB, LLM, is a member of the Alberta Bar, practicing in Calgary.

decision to initiate the search, and (c) should be subject to a traveller's right to speak to legal counsel prior to the initiation of the search.

2. THE FOUNDATIONAL CASES

The case of *Hunter v. Southam*¹ was the first time that the Supreme Court of Canada considered the effect of the *Canadian Charter of Rights and Freedoms*² on federal legislation authorizing search and seizure, and it is particularly notable for articulating the well-known criminal search standard of "reasonable and probable grounds." It remains the leading case on Charter protection against search and seizure.³ The case of *R. v. Simmons*,⁴ heard four years after *Hunter*, was the first time that the Supreme Court considered the effect of the Charter on Canadian customs searches,⁵ and it remains the leading case in that regard.⁶ Together, *Hunter* and *Simmons* provide the constitutional foundation for the modern approach to device searches at customs.

a. Hunter v. Southam

Although *Hunter* was not itself a customs case, Justice Dickson's discussion in *Hunter* about the appropriate "procedural safeguards" against unreasonable search and seizure weighed heavily on *Simmons*, as well as post-*Simmons* customs case law. In *Hunter*, officers attempted to execute a search at the business premises of the Edmonton Journal (a division of the named party Southam), pursuant to a sweeping "certified authorization" granted by the Restrictive Trade Practices Commission (the predecessor to the Competition Tribunal). Southam challenged the statutory provisions authorizing the search, which were found to be unconstitutional, and therefore inoperable, by the Alberta Court of Appeal. Justice Dickson (as he was then), writing for a unanimous Supreme Court, upheld the decision of the Alberta Court of Appeal.

Justice Dickson observed that the section 8 could be expressed not only as an individual's "negative" right to protection against "unreasonable search and seizure," but also as an individual's "positive" right to a "reasonable expectation

Canada (Director of Investigation Research, Combines Investigation Branch) v. Southam Inc., 1984 CarswellAlta 121, (sub nom. Hunter v. Southam Inc.) [1984] 2 S.C.R. 145 (S.C.C.) [Hunter].

² Canadian Charter of Rights and Freedoms, Part 1 of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.), c. 11 [Charter].

³ R. v. Oliynyk, 2005 BCSC 1895, 2005 CarswellBC 3611 (B.C. S.C.) at para. 17.

⁴ R. v. Simmons, 1988 CarswellOnt 91, [1988] 2 S.C.R. 495 (S.C.C.) [Simmons].

On the same date as *Simmons*, the Supreme Court also heard the case of *R. v. Jacoy*, 1988 CarswellBC 1314, [1988] 2 S.C.R. 548 (S.C.C.), which also involved the seizure of narcotics at an airport.

Robert Currie, "Electronic Devices at the Border: The Next Frontier of Canadian Search and Seizure Law?" (2016) 14:2 CJLT 289 at 298.

⁷ Combines Investigation Act, R.S.C. 1970, c. C-23, ss. 10(2) and 10(3).

of privacy." In any given situation, the determination of the reasonableness of an expectation of privacy would involve balancing the interests of the individual (such as the interest in being left alone, or, in more serious cases, the interest in bodily integrity) against the interests of the state (such as its interest in law enforcement or, in more serious cases, its interest in state security). This "balance of interests" involved the consideration of potential "procedural safeguards" against state overreach, such as (a) prior authorization, (b) judicial authorization, and (c) objective standards. ¹⁰

With respect to (a) prior authorization, Justice Dickson stated that section 8 strongly favoured a "means of preventing unjustified searches before they happen" rather than simply "determining, after the fact, whether they ought to have occurred in the first place." Prior authorization was usually accomplished "in the form of a valid warrant," which put "the onus on the state to demonstrate the superiority of its interest to that of the individual." While not always possible to obtain prior authorization, "where it is feasible [. . .] such authorization is a precondition for a valid search and seizure." ¹³

With respect to (b) judicial authorization, Justice Dickson observed that it mattered not only *when* authorization to perform a search occurred, but also *who* granted authorization to perform the search. In other words, "it is necessary for the person authorizing the search to be able to assess the evidence as to whether that standard has been met, in an entirely neutral and impartial manner." While it may be preferable for the authorizer to be a judge (as in the case of a criminal search warrant), this was not a "necessary precondition," as long as the authorizer was "capable of acting judicially." One way to assess whether the authorizer was acting judicially was to examine whether the authorizer was performing an "investigatory rather than adjudicatory" function. In the case before him, Justice Dickson observed that the "significant investigatory functions" of the Restrictive Trade Practices Commission had the result of "vitiating the ability of a member of the Commission to act in a judicial capacity when authorizing a search or seizure" (although Justice Dickson was careful to

⁸ Hunter, supra note 1 at para. 25.

⁹ *Ibid* at paras. 25—26, 42.

Hunter, supra note 1. Justice Dickson attributes the phrase "procedural safeguards" to Justice Prowse of the Alberta Court of Appeal (para 11, aff'g 1983 ABCA 32). In his own analysis, Justice Dickson weighs the appropriate procedural safeguards by posing three questions: "[w]hen is the balance of interests to be assessed" (paras 27-31); "[w]ho must grant the authorization" (paras 32-36); and "[o]n what basis must the balance of interests be assessed" (paras 37-43).

¹¹ *Ibid* at para. 27.

¹² *Ibid* at para. 28.

¹³ *Ibid* at para. 29.

¹⁴ *Ibid* at para 32.

¹⁵ *Ibid*.

¹⁶ *Ibid* at para. 34.

add that this was not "a matter if impugning the honesty or good faith of the Commission or its members"). 17

With respect to (c) objective standards, Justice Dickson observed that it mattered not only *when* authorization occurred, or *who* granted authorization, but also *what* standard was applied in determining whether authorization should be granted. Justice Dickson remarked that it was untenable to leave the search standard entirely to the "subjective appreciation of individual adjudicators" and found that some "objective standard must be established." Justice Dickson rejected the search standard proposed by the appellant Restrictive Trade Practices Commission (authorizing a search if there was a reasonable belief as to the "possible existence of relevant evidence") as being "a very low standard which would validate intrusion on the basis of suspicion, and authorize fishing expeditions of considerable latitude." Instead, Justice Dickson mandated the search standard of "reasonable and probable grounds, established upon oath, to believe that an offence has been committed and that there is evidence to be found at the place of the search" as the "minimum standard" for cases such as the one before him. ²⁰

b. R. v. Simmons

In *Simmons*, the accused, Ms. Simmons, arrived in Toronto on a flight from Jamaica.²¹ She was subjected to a "strip-search" by customs officers, which revealed six bags of hashish oil fastened to her midriff with plastic bandages. She was arrested and charged with importing narcotics. At trial, Ms. Simmons argued, amongst other things, that her Charter rights had been violated (a) because she was not informed of her right to contact legal counsel prior to being subjected to a strip-search, and (b) because the customs legislation authorizing her strip search had required something less than the procedural safeguards outlined in *Hunter*.²²

The trial judge agreed that the strip-search violated Ms. Simmons's Charter rights. The narcotics evidence discovered as result of the illegal search was excluded, and Ms. Simmons was acquitted. On appeal, the Ontario Court of Appeal set aside the acquittal and ordered a new trial.²³ On further appeal, Chief Justice Dickson, writing on behalf of the majority of the Supreme Court, found that, although Ms. Simmons's Charter rights had been violated, the narcotics

¹⁷ *Ibid* at para 35.

¹⁸ *Ibid* at para 41.

¹⁹ *Ibid* at para 42.

²⁰ *Ibid* at para 43.

²¹ Supra note 4.

R. v. Simmons, 1983 CarswellOnt 1471 (Ont. Co. Ct.), reversed 1984 CarswellOnt 46 (Ont. C.A.), affirmed 1988 CarswellOnt 91, 1988 CarswellOnt 968 (S.C.C.).

²³ R. v. Simmons, 1984 CarswellOnt 46, 45 O.R. (2d) 609 (Ont. C.A.), affirmed 1988 CarswellOnt 91, 1988 CarswellOnt 968 (S.C.C.).

evidence should not have been excluded.²⁴ He upheld the Court of Appeal's decision to order a new trial.

The operative legislation at the time of Ms. Simmons's arrest was the 1970 version of the *Customs Act*.²⁵ Section 143 provides that a customs officer may search a person entering Canada if the officer "has reasonable cause to suppose that the person searched has goods subject to entry at the customs, or prohibited goods, secreted about his person." And section 144 provides that a person being searched "may require the officer to take him before a police magistrate or justice of the peace, or before the collector or chief officer at the port or place, who shall, if he sees no reasonable cause for search, discharge the person."

Although there is only one search standard articulated in sections 143 and 144 — "reasonable cause to suppose" — Chief Justice Dickson famously found that there were in fact three distinct types of customs searches:

30 It is, I think, of importance that the cases and the literature seem to recognize three distinct types of border search. 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.

31 I wish to make it clear that each of the different types of search raises different issues. We are here concerned with searches of the second type, and what I have to say relates only to that type of search. Searches of the third, or bodily cavity, type may raise entirely different constitutional issues, for it is obvious that the greater the intrusion, the greater must be the justification and the greater the degree of constitutional protection.

The first issue (whether Ms. Simmons should have had the opportunity to speak to legal counsel prior to her strip-search) engaged section 10 of the Charter, which provides that, upon "arrest or detention," a person has the right to "retain and instruct counsel without delay and to be informed of that right."

Supra note 4.

²⁵ Customs Act, R.S.C. 1970, c. C-40 [Customs Act 1970].

Chief Justice Dickson found that, when Ms. Simmons was required to undergo a strip-search, the "customs officer had assumed control over her movements by a demand which had significant legal consequences," which amounted to a "detention," which in turn triggered Ms. Simmons's right to instruct counsel prior to the strip-search.²⁶

The second issue (as to whether sections 143 and 144 set out appropriate search standards) engaged section 8 of the Charter. On one hand, Chief Justice Dickson noted that sections 143 and 144 clearly did not meet the high standards that had been outlined in *Hunter:* prior authorization was not mandatory (although, notably, a review would occur upon request); there was no warrant requirement; and the standard of "reasonable cause to suppose" fell short of the standard of "reasonable and probable grounds established on oath."²⁷ On the other hand, Chief Justice Dickson noted that that the "reasonable expectation of privacy" of a person at Canadian customs differed from the "reasonable expectation of privacy" of a person in "most other situations."²⁸ This difference owed to the fact that (a) "travellers seeking to cross national boundaries fully expect to be subject to a screening process," and (b) states have important interests in "preventing the entry of undesirable persons and prohibited goods, and in protecting tariff revenue."²⁹ Thus, unlike *Hunter*, Chief Justice Dickson concluded that sections 143 and 144 were constitutional.

However, Chief Justice Dickson went on to conclude that, in the specific case of Ms. Simmons, customs officers had misapplied sections 143 and 144, causing a breach of her section 8 rights. Ms. Simmons had a right to know about the customs officers' scope of authority to conduct the strip search, and she had a right to know about her option to request a review of the custom officers' decision to initiate the search. 30 Customs officers had failed to directly inform Ms. Simmons about her rights, and she had also been deprived of the opportunity to learn about her rights by speaking to counsel. Unfortunately for Ms. Simmons, while Chief Justice Dickson found that Ms. Simmons's section 8 and section 10 rights had been breached by the strip-search, he also found that there were ample "objective, articulable facts" to "support the customs officer's suspicion that [Ms. Simmons] was concealing something on her body." Accordingly, Justice Dickson concluded that excluding the narcotics evidence "would bring the administration of justice into disrepute," pursuant to section 24 of the Charter, and he therefore declined to do so.

Notably, by the time that Ms. Simmons's appeal reached the Supreme Court, ³² the *Customs Act 1970* had been repealed and replaced by a new version

²⁶ Simmons, supra note 4 at para. 38.

²⁷ *Ibid* at para. 45.

²⁸ *Ibid* at para. 49.

²⁹ *Ibid* at paras 51-52.

³⁰ *Ibid* at paras 57—58, 62.

³¹ *Ibid* at 67.

of the *Customs Act*, which came into force in 1986 (after Ms. Simmons's arrest).³³ With respect to searches of the person, section 98 of the *Customs Act 1986* replaced sections 143-144 of the *Customs Act 1970*.³⁴ With respect to searches of goods, section 99 of the *Customs Act 1986* replaced section 133 of the *Customs Act 1970*.³⁵ The old and new *Customs Act* provisions respecting searches of the person are similar, with the notable difference that section 98 significantly narrows the scope of who may review a search decision to simply "the senior officer at the place where the search is to take place" (from a police magistrate, justice of the peace, or chief officer, according to the predecessor section). The provisions respecting searches of "goods" are also similar, with the notable difference that section 99(1) does not require an officer to have "reasonable grounds of suspicion" before initiating a search.

3. EARLY INTERPRETATIONS: ELECTRONIC DEVICES ARE "GOODS"

Citing *Simmons*, courts have tended to broadly construe the types of activities falling within first-level searches. For example, in *R. v. Nagle*, the British Columbia Court of Appeal found that the "search of a purse, in the context of a border crossing, is part of the routine screening procedure." Similarly, in *R. v. Hudson*, the Ontario Court of Appeal found that "asking the respondent to turn his pockets inside out was no more invasive than a search of baggage, or a purse, or a pat down or frisk of outer clothing."

³² *Ibid* at para. 8.

³³ Customs Act, R.S.C. 1985, c. 1 (2nd Supp.) [formerly Customs Act, S.C. 1986, c. 1] [Customs Act 1986].

With respect to searches of the person, the provision that a search may be initiated if an officer "has *reasonable cause to suppose*" that a person has secreted prohibited goods (section 143) was replaced with the provision that a search may be initiated "if the officer *suspects on reasonable grounds*" that a person has secreted prohibited goods, or secreted evidence of some contravention of customs legislation, on their person (section 98(1)). The provision allowing a person to request a review of a search decision to a "police magistrate or justice of the peace" or "collector or chief officer at the port or place" (section 144) was replaced with a provision allowing for review by "the senior officer at the place where the search is to take place" (section 98(2)).

With respect to the search of goods, the provision that an officer may "upon information, or upon reasonable grounds of suspicion, detain, open and examine any package suspected to contain prohibited property or smuggled goods, or goods respecting which there has been any violation of any of the requirements of this Act" (section 133(1)) was replaced with the provision that an officer may "examine any goods that have been imported and open or cause to be opened any package or container of imported goods and take samples of imported goods in reasonable amounts" (section 99(1)(a)). With respect to "mail," an officer may open "any such mail that the officer suspects on reasonable grounds" contains prohibited goods (section 99(1)(b)).

³⁶ R. v. Nagle, 2012 BCCA 373, 2012 CarswellBC 2859 (B.C. C.A.) at para. 75, leave to appeal refused 2013 CarswellBC 685, 2013 CarswellBC 686 (S.C.C.).

In early cases involving the status of electronic devices at the border, the courts continued to broadly construe first-level searches so as to include device searches. In *R. v. Leask*, a customs officer turned on Mr. Leask's laptop, performed a "routine border search" (clicked through the electronic folders), and discovered child pornography.³⁸ At trial, the Ontario Court of Justice concluded that the non-destructive search of the accused's laptop, which "required no special equipment or expertise," fell within the ambit of a first-level search, as defined by *Simmons*:

16 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 my view the search of Mr. Leask's computer was a routine border search that did not infringe his s. 8 Charter rights.

Leask has been followed, or cited with approval, in a number of subsequent cases. In R. v. Whittaker, the New Brunswick Provincial Court found that "a computer file such as the digital storage of photographic images is a document and falls squarely within the definition of 'goods' as that term is used in the Customs Act." In R. v. Appleton, the Ontario Superior Court of Justice found that a "Blackberry" was analogous to a briefcase, and that a "text message" was analogous to a "letter from a friend," all of which fell under the ambit of a firstlevel search. 40 In R. v. Moroz, the Ontario Superior of Justice found that "the cursory view of [the accused's] cell-phone or I-Phone was merely to review and peruse electronic information that may assist custom officials in their determination whether any illegal materials or 'goods' are concealed by the individual."41 Finally, in R. v. Buss, a customs officer turned on the accused's laptop and "pushed Windows and the F key and searched for jpgs, j pegs, a commonly used photo format," which the British Columbia Provincial Court found fell within the ambit of a first-level search. 42 Whittaker, Moroz, and Buss were child pornography cases, while Appleton involved the discovery of text messages that discussed smuggling a handgun into Canada.

³⁷ R. v. Hudson, 2005 CarswellOnt 7378, 77 O.R. (3d) 561 (Ont. C.A.) at para. 38.

³⁸ R. v. Leask, 2008 ONCJ 25, 2008 CarswellOnt 415 (Ont. C.J.) [Leask].

³⁹ R. v. Whittaker, 2010 NBPC 32, 2010 CarswellNB 489 (N.B. Prov. Ct.) at para. 8 [Whittaker].

⁴⁰ R. v. Appleton, 2011 CarswellOnt 11191 (Ont. S.C.J.) at para. 12 [Appleton].

⁴¹ R. v. Moroz, 2012 ONSC 5642, 2012 CarswellOnt 12614 (Ont. S.C.J.) at para. 21 [Morosz].

⁴² R. v. Buss, 2014 BCPC 16, 2014 CarswellBC 485 (B.C. Prov. Ct.) at para. 15 [Buss].

4. RECOGNIZING THE UNIQUE NATURE OF ELECTRONIC DEVICES

Interestingly, at roughly the same time that the lower courts were broadly construing the search authority of customs officers with respect to electronic devices, the Supreme Court of Canada began to narrow the search authority of police officers with respect to electronic devices. Out of Justice Dickson's finding in Hunter that section 8 of the Charter afforded a positive right to a "reasonable expectation of privacy," the Supreme Court developed, primarily through cases dealing with different types of police searches, a four-factor test to determine the nature and scope of a person's expectation of privacy. 43 First, the court should define the "subject matter" of the search. Second, the court should ask whether the claimant had a "direct interest" in the subject matter. Third, the court should ask whether the claimant has "a subjective expectation of privacy" in the subject matter. Finally, the court should ask whether the claimant's "subjective expectation of privacy was objectively reasonable." In applying this test, the Supreme Court has increasingly recognized that device searches engage unique privacy interests, which often require a higher degree of protection than searches of other objects or areas.

In the watershed⁴⁴ case of *R. v Morelli*, Justice Fish quashed the accused's conviction for possession of child pornography, citing deficiencies in a police search warrant executed with respect to the accused's home and computer.⁴⁵ In doing so, Justice Fish suggested that searching an accused's home and computer was more invasive than only searching an accused's home:

105 As I mentioned at the outset, it is difficult to imagine a more intrusive invasion of privacy than the search of one's home and 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.

In R. v. Vu, Justice Cromwell expanded upon Justice Fish's observations in Morelli, finding, definitively, that a warrant authorizing police to search a home did not also authorize police to search a computer located within that home. ⁴⁶ In that case, police searched electronic devices, which had in turn been discovered during the search of a grow-op residence, and retrieved electronic information

⁴³ R. v. Cole, 2012 SCC 53, 2012 CarswellOnt 12684 (S.C.C.) at para. 40 [Cole]; R. v. Marakah, 2017 SCC 59, 2017 CarswellOnt 19341 (S.C.C.) at paras. 8 - 12 [Marakah]; R. v. Reeves, 2018 SCC 56, 2018 CarswellOnt 20930 (S.C.C.) at para. 28 [Reeves]; R. v. Mills, 2019 SCC 22, 2019 CarswellNfld 161 (S.C.C.) at para. 13 [Mills].

⁴⁴ So noted in R. v. Fearon, 2014 SCC 77, 2014 CarswellOnt 17202 (S.C.C.) at para. 188 [Fearon].

⁴⁵ R. v. Morelli, 2010 SCC 8, 2010 CarswellSask 150 (S.C.C.) at para. 4 [Morelli].

⁴⁶ R. v. Vu, 2013 SCC 60, 2013 CarswellBC 3342 (S.C.C.) [Vu].

that allowed them to identify, and charge, the accused with drug-related offences. Justice Cromwell opined that computer searches were "markedly different" from searches of other "receptacles," such as "cupboards and filing cabinets," in four specific ways: (a) immense informational storage capacity (which may touch on an individual's "biographical core of personal information"); (b) automatic or inadvertent data retention; (c) data retention after apparent deletion; and (d) interconnectivity of data stored in multiple "locations." As such, "prior authorization" (as mandated by *Hunter*) needed to be assessed separately with respect to general searches and computer searches, requiring police to "first satisfy the authorizing justice that they have reasonable grounds to believe that any computers they discover will contain the things they are looking for" before such computers could be searched.⁴⁸

In R. v. Spencer, Justice Cromwell clarified and expanded upon his reasoning in Vu, noting that, when identifying the subject matter of an alleged search (the first part of the four-factor test), the court "must not do so narrowly in terms of the physical acts involved or the physical space invaded, but rather by reference to the nature of the privacy interests potentially compromised." In Spencer, the "subject matter" of the alleged search was found to be "the identity of a subscriber whose Internet connection is linked to a particular, monitored Internet activity [i.e. downloading child pornography]," as opposed to simply "a name and address of someone in a contractual relationship with [the internet service provider]." Thus, Justice Cromwell concluded that a specific warrant was required not only for police to seize and search a personal computer (his finding in Vu), but that a specific warrant was required for police to request, from an internet service provider, the subscriber information that was associated with an ISP address.

In *R. v. Fearon*, the issue before the court was the constitutionality of electronic device searches "incident to arrest." Notably, at least for the purposes of this paper, the Supreme Court directly compared these types of searches to "strip searches." In that case, the police obtained evidence that implicated the accused in an armed robbery by searching the accused's smartphone, which had itself been discovered during a pat-down search after the accused had been arrested. Justice Cromwell found that Mr. Fearon's *Charter* rights had been breached, although Justice Cromwell ultimately declined to exclude the cellphone evidence and upheld the accused's conviction. Justice Karakatsanis, writing in dissent, would have excluded the cellphone evidence.

⁴⁷ *Ibid* at paras. 25, 40—45.

⁴⁸ *Ibid* at para 48.

⁴⁹ R. v. Spencer, 2014 SCC 43, 2014 CarswellSask 342 (S.C.C.) at para. 31 [Spencer].

⁵⁰ *Ibid* at para 33.

⁵¹ *Ibid* at para 32.

⁵² Fearon, supra note 44.

Justice Cromwell noted, by way of comparison, that strip searches could be performed by police when they are "incident to a lawful arrest for the purpose of discovering weapons in the detainee's possession or evidence related to the reasons for the arrest" and the police "have reasonable and probable grounds for concluding that a strip search is necessary in the particular circumstances of the arrest." Although Justice Cromwell affirmed the unique privacy interests at stake with respect to the search of electronic devices, he ultimately concluded that these interests were less significant than those associated with strip searches, stating that the latter "are *invariably* and *inherently* very great invasions of privacy and are, in addition, a significant affront to human dignity." Accordingly, Justice Cromwell outlined a somewhat less stringent, 4-part, test for the search of an electronic device incident to arrest, requiring: (a) a lawful arrest, (b) a valid law enforcement purpose to search the device (such as safety or the preservation of evidence), (c) a tailoring of the nature and extent of the search to the scope of the search, and (d) detailed note taking by police. ⁵⁵

Unlike Justice Cromwell, Justice Karakatsanis suggested that "like the search of a private home, a strip search or the seizure of bodily samples, the search of the portal to our digital existence is invasive and impacts major privacy interests." She concluded that police should be required to obtain a warrant to search a cellphone incident to arrest, except when "(1) there is a reasonable basis to suspect that a search may prevent an imminent threat to safety or (2) there are reasonable grounds to believe that the imminent loss or destruction of evidence may be prevented by a warrantless search."

In R. v. Marakah, Chief Justice McLachlin strongly affirmed Justice Cromwell's characterization of the "subject matter" of the search, noting that "[t]he subject matter of a search must be defined functionally, not in terms of physical acts, physical space, or modalities of transmission." In that case, police obtained text messages between the accused and his accomplice, from a search of the accomplice's iPhone, implicating the accused in firearms-related offences. Chief Justice McLachlin declined to characterize the "subject matter" of the search to be simply the accomplice's iPhone, since "[n]either the iPhone itself nor its contents generally is what the police were really after." Rather, (1) the subject matter of the search was the "electronic conversation" between the accused and the accomplice; (2) the accused obviously had a direct interest in

⁵³ *Ibid* at para 24.

⁵⁴ *Ibid* at para 55 (emphasis in original).

Ibid at para. 83. In practice, the "tailoring" of a search meant that "generally, even when a cellphone 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": ibid at para. 76.

⁵⁶ *Ibid* at para 134.

⁵⁷ *Ibid* at 179.

⁵⁸ Marakah, supra note 43 at para 15.

⁵⁹ *Ibid*.

this electronic conversation (because he participated in the conversation); (3) the accused subjectively expected that this conversation would remain private; and (4) this expectation was reasonable. Chief Justice McLachlin excluded the iPhone evidence and acquitted the accused.

In *R. v. Reeves*, the accused's recently estranged common-law wife provided a shared household computer to the police, which was found to contain child pornography.⁶¹ The subject matter of the search was found to be "the computer, and ultimately the data it contained about [the accused's] usage, including the files he accessed, saved and deleted."⁶² In other words, "the police were not after the physical device (to collect fingerprints on it, for example)."⁶³ Justice Karakatsanis found that the accused had a reasonable expectation of privacy in the data contained on the shared computer, and that the accused's wife's decision to provide the computer to police did not waive his privacy rights. The computer evidence was excluded and the accused was acquitted.

R. v. Mills is notable because, after a period of expansion, the Supreme Court finally appears to have reached an outer limit as to an accused's reasonable expectation of privacy. ⁶⁴ In that case, a police officer, posing as a 14-year-old girl, communicated with the accused over the internet in the course of a sting operation. These internet communications were used as evidence to convict the accused of child luring. Similar to Marakah, Justice Brown defined the subject matter of the search to be "the electronic communications that took place on Facebook 'chat' and over email." However, unlike Marakah, Justice Brown found that the accused's subjective expectation of privacy was not objectively reasonable, since "adults cannot reasonably expect privacy online with children they do not know." adults cannot reasonably expect privacy online with children they do not know." In a concurring opinion, Justice Karakatsanis also found that the accused's expectation of privacy was not reasonable, since "it is not reasonable to expect that your messages will be kept private from the intended recipient (even if the intended recipient is an undercover officer)." The internet evidence was allowed and the accused's conviction was upheld.

Professor Steve Coughlan has observed that the most important part of the four-part test delineating an accused's reasonable expectation of privacy appears to be the first — the definition of the "subject matter of the search" (or "what the police were really after") — such that, once this occurs, "the rest of the argument flows largely lockstep." For example, in *Marakah*, it would have been difficult

⁶⁰ *Ibid* at para. 17.

⁶¹ Reeves, supra note 44.

⁶² *Ibid* at para 30.

⁶³ *Ibid* at para. 31.

⁶⁴ Mills, supra note 43.

⁶⁵ *Ibid* at para. 14.

⁶⁶ *Ibid* at para. 23.

⁶⁷ Ibid at para. 36.

⁶⁸ Steve Coughlan, "Case Comment: R v. Marakah," accessible through Westlaw Next

for the accused to establish a privacy interest in the "subject matter" of his accomplice's iPhone (the accused, after all, did not own, or control, that iPhone). However, the accused was able to establish a privacy interest in the "electronic conversation" that was contained on his accomplice's iPhone. In short, when assessing searches of "electronic devices," the Supreme Court has chosen to emphasize the "electronic" and deemphasize the "device." In many cases, it may no longer be sufficient to consider whether a reasonable expectation of privacy exists in a device as a whole; rather, it may be necessary to consider whether a reasonable expectation of privacy exists in the component parts, functions, or categories of information contained within the device.

5. CRITIQUE OF THE EARLY INTERPRETATIONS: ELECTRONIC DEVICES ARE NOT "GOODS"

In light of the Supreme Court's recent approach to police searches of electronic devices, the lower court decisions expressing the view that searches of electronic devices are equivalent to first-level searches of "goods" (*Leask*, *Whittaker*, *Appleton*, *Morosz*, and *Buss*) have been widely criticized. Professor Robert Currie has observed that "[d]espite 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." Daniel Therrien, the Privacy Commissioner of Canada, has stated that the "idea that electronic devices should be considered as mere goods and therefore be subject to border searches without legal grounds is clearly outdated and does not reflect the realities of modern technology." And the Canadian Bar Association has taken the position that "[i]nformation stored on an electronic device is not a 'Good' — and any interpretation of the *Customs Act* that would authorize a warrantless search of data stored on a device would likely be unconstitutional."

The Canadian Border Services Agency ("CBSA") has maintained the legal position that an electronic device is a "good" for the purposes of the *Customs Act* 1986.⁷² However, in practice, internal CBSA guidelines direct that an

Canada, 2017 CarswellOnt 19342; Steve Coughlan, "Case Comment: R v. Reeves," accessible through Westlaw Next Canada, 2018 CarswellOnt 20931.

⁶⁹ Currie, *supra* note 6 at 307.

House of Commons, Protecting Canadians' Privacy at the US Border: Report of the Standing Committee on Access to Information, Privacy and Ethics (December 2017) (Chair: Bob Zimmer) at 9 [HOC Standing Committee].

Canadian Bar Association, Privacy of Canadians at Airports and Borders (September 2017) at 2, online: http://cba.org/CMSPages/GetFile.aspx?guid=04e96564-b5b6-441b-b6de-20b3e0874975 [CBA].

R. v. Gibson, 2017 BCPC 237, 2017 CarswellBC 2306 (B.C. Prov. Ct.) at paras. 55-63 [Gibson]; Vaillancourt v. Her Majesty et al, 2017 MBQB 95, 2017 CarswellMan 240 (Man. Q.B.) at para. 2.

examination of a "digital device" should "not be conducted as a matter of routine," but rather "if there is a multiplicity of indicators that evidence of contraventions may be found on the digital device or media." Customs officers should "disable wireless and Internet activity," should "only examine what is stored within the device," and should begin with a search that is "cursory in nature and increase in intensity based on emerging indicators." Customs officers should also take notes with respect to "the indicators that led to the progressive search" as well as "what areas of the device or media were accessed during the search."

More recently, lower courts have begun to appreciate that section 99(1) may be vulnerable to a Charter challenge with respect to searches of electronic devices. ⁷⁶ In *R. v. Gibson*, ⁷⁷ Judge Gillespie of the British Columbia Provincial Court provided a useful summary of testimony given by customs officers about their practices respecting device searches. In that case, the accused, Mr. Gibson, attempted to enter Canada while carrying a cellphone, camera, and laptop. He exhibited "indicators" that caused him to be referred to secondary inspection ⁷⁸

Canadian Border Services Agency, "Operational Bulletin: PRG-2015-31: Examination of Digital Devices and Media at the Port of Entry - Interim Guidelines" (30 June 2015) at 1, online: https://www.lexsage.com/documents/CBSA%20Operational%20Bulletin%20PRG-2015-31%20Examination%20of%20Digital%20Devices%20and%20-Media%20at%20Port%20of%20Entry.pdf [CBSA Guidelines]; Robert Diab, "Protecting the Right to Privacy in Digital Devices: Reasonable Search on Arrest and at the Border" (2018) 69 U.N.B.L.J. 96 at 115; Meghan McDermott, Tamir Israel & Greg McMullen, Electronic Devices Privacy Handbook: A Guide to Your Rights at the Border (Vancouver: British Columbia Civil Liberties Association, 2018) at 9 [BCCLA]; HOC Standing Committee, supra note 78 at 5. As per Diab and the BCCLA, the CBSA Guidelines were current as of at least February 2017. The HOC Standing Committee, which heard evidence from the CBSA, appeared to treat the CBSA Guidelines as current as of the date of its report, December 2017.

⁷⁴ CBSA Guidelines, *supra* note 73 at 3.

⁷⁵ Ibid.

See BCCLA, *supra* note 73 at 12. In *United States of America v. Amadi*, 2017 ONSC 3446, 2017 CarswellOnt 8874 (Ont. S.C.J.), the applicants sought disclosure of customs officers' notes in the course of extradition proceedings. The Ontario Superior Court of Justice allowed the disclosure on the basis that there was an "air or reality" to the accused's argument that section 8 operated to limit customs searches (para 51). In *R v. Vaillancourt, supra* note 80, the accused argued that the cursory search of his iPhone by Canadian customs officers, which revealed child pornography, violated his Charter rights. In light of the decision in *Fearon*, the trial judge "found there was an inconsistency between s.99(1)(a) of the *Customs Act* and s.8 of the *Charter*," and therefore "imposed restrictions to the manner in which the section applies to electronic devices" (para 8). However, Crown successfully appealed this decision on the basis that the Crown did not receive proper notice of the Charter argument (and the text of earlier decision of the trial judge appears to be unavailable).

⁷⁷ Gibson, supra note 72.

⁷⁸ See Currie, *supra* note 6 at 299, noting the CBSA's own use of the terms "primary" and "secondary" inspection does not correspond with the search levels outlined in *Simmons*

(such as the fact that he was carrying commercial photography equipment although he claimed not be working in Canada). Mr. Gibson interacted with several different customs officers in the course of his secondary inspection. One officer testified that "there were no limitations on what he could look for in reviewing the phone or camera. He was free to look at intimate pictures of people on phones and in media on other devices."⁷⁹ Another officer testified that he "did not have a specific practice about how far back he scrolls in the messages" and that he "looks at the photos and videos that are stored on the device." Yet another officer testified that he "regularly" inspected cellphones as part of a "routine Customs examination," although he commenced his search by "putting the phone in airplane mode, so there are no incoming or outgoing calls."81 Despite this last officer's apparent practice, the court heard technical evidence that Mr. Gibson's cellphone was not actually put into airplane mode during its inspection.⁸² The customs officers discovered child pornography in the course of their search. At trial, Mr. Gibson argued that section 99(1) violated section 8 of the Charter, and Judge Gillespie held a voir dire on the issue.

While Judge Gillespie accepted the Crown's argument that electronic devices were "goods" for the purposes of the *Customs Act 1986*, he also read-in certain limits to section 99(1) in light of *Morelli*, *Vu*, and *Fearon*. He concluded that a first-level customs search of an electronic device must (a) be conducted for a valid customs purpose, (b) be limited to data stored on the device, (c) not involve seizure or full forensic search of the device, and (d) be terminated once contraband is located. ⁸³ As such, Judge Gillespie concluded that section 99(1) was constitutionally valid for the purposes of Mr. Gibson's trial.

6. PROPOSALS FOR CHANGE

Several proposals have been advanced to address the perceived deficiencies in the *Customs Act 1986* with respect to searches of electronic devices. These proposals can be lumped into three broad categories: (a) banning device searches, (b) requiring a warrant or exigent circumstances before initiating device searches, or (c) requiring that custom officers have "reasonable suspicion" of a contravention before initiating device searches.

⁽as will be familiar to most travellers). In most cases, a referral to "secondary inspection" involves "a more detailed conversation and search of an individual's belongings," and thus will fall within the ambit of a first-level search contemplated by *Simmons*.

⁷⁹ Gibson, supra note 72 at para 11.

⁸⁰ *Ibid* at para. 22.

⁸¹ *Ibid* at paras. 15—16.

⁸² *Ibid* at para. 30.

⁸³ *Ibid* at paras. 182—189.

a. Banning Device Searches

Professor Steven Penney argues that it is "wrong to equate digital information with contraband," and that, rather than "further the objectives of border control," customs searches of electronic devices instead "give the state back door access to intensely private information that it could not otherwise obtain." For example, in most child pornography cases, it seems to be a legal fiction that attempts were made to "import" illicit images into Canada. Rather, illicit images appear to have been downloaded from the internet without much regard for borders. If the state wishes to fight child pornography, it should do so through traditional law enforcement channels (which usually require a warrant), rather than the pretext of customs searches. Accordingly, Professor Penney proposes that digital data "should remain off limits for searches authorized under border control legislation."

b. Requiring a Warrant or Exigent Circumstances

Professor Robert Diab reiterates Professor Penney's concerns. However, he allows that customs officers should have authority to conduct device searches in rare cases. Taking inspiration from Justice Karakatsanis's dissent in *Fearon*, Professor Diab proposes that the *Customs Act 1986* be amended "to allow for a device search only with a warrant on probable grounds, except in exigent circumstances." Exigent circumstances would include (a) a reasonable suspicion of imminent harm, or (b) a reasonable belief of imminent danger of destruction of evidence.

c. Reasonable Suspicion

Professor Currie proposes three "modest" changes: (a) the search of an electronic device "should only occur if the CBSA officer has a reasonable suspicion⁸⁸ that contraband is being smuggled or some other statutory breach has occurred/is under way"; (b) CBSA officers should keep "detailed notes of

Steven Penney, "Mere Evidence"? Why Customs Searches of Digital Devices Violate Section 8 of the Charter" (2016) 49:1 U.B.C. L. Rev. 485 at 510—511 [Penney].

See Diab, *supra* note 73 at 122, expanding on Penney's point: "Obviously, the vast majority of illicit data that enters Canada does so through the internet. A cursory glance of the cases on device searches at the border will show that most involve accused persons of seemingly limited technical savvy caught in possession of small amounts of child pornography."

Penney, *supra* note 84 at 514.

⁸⁷ Diab, *supra* note 73 at 123.

See Steven Penney, "Standards of Suspicion" (2017) 65 Crim. L.Q. 23 at 36—41: Historically, courts did not recognize a difference between the standards of "reasonable suspicion" and "reasonable and probable grounds." However, beginning in the 1970's, courts began to define reasonable suspicion as having a lower probability threshold than reasonable and probable grounds. This lower standard was confirmed to be "constitutionally reasonable" with the advent of the Charter. The standard of reasonable

what they have examined"; (c) the search should be "limited to the more basic apps on the device — sent and draft emails and texts, photos, call logs, note-taking apps and anything similar," whereas "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."⁸⁹

At the time that Professor Currie made his suggestions, the CBSA Guidelines respecting electronic device searches had not been made public. ⁹⁰ As indicated above, the CBSA Guidelines already contain provisions with respect to (b) limiting the scope of searches and (c) notetaking. In 2017, the House of Commons Standing Committee on Access to Information, Privacy and Ethics ("ETHI") recommended that the CBSA Guidelines be "written into the *Customs Act*." Mirroring Professor Currie, the ETHI also recommended that the CBSA "multiplicity of indicators" approach to authorizing device searches be replaced with the legal standard of "reasonable grounds to suspect."

Notably, at least one American court has recently endorsed a "reasonable suspicion" standard for devices searches by customs officers (although it is outside the scope of this paper to provide a detailed commentary on the American jurisprudence). In Alasaad v. Nielsen, 92 eleven plaintiffs alleged, amongst other things, that border searches of their electronic devices had violated their Fourth Amendment rights. The government conceded that "advanced searches" (i.e. attaching a device, through a wired or wireless connection, to external equipment) required a standard of reasonable suspicion, although the government also argued that "basic searches" (i.e. not attaching a device to external equipment) could be performed without suspicion. 93 Judge Casper disagreed, finding that the standard of "reasonable suspicion" (defined as "a showing of specific and articulable facts, considered with reasonable inferences drawn from those facts, that the electronic devices contain contraband") should be required for both advanced and basic searches, given that both searches implicated the same privacy interests. 94 Notably, Judge Casper specifically rejected the argument that device searches required a warrant.

suspicion has been expressed in phrases such as "reasonable cause to suspect," "suspects on reasonable grounds" (section 98), or "reasonable cause to suppose" (section 144).

⁸⁹ Currie, *supra* note 6 at 308—314.

⁹⁰ *Ibid* at 320.

⁹¹ HOC Standing Committee, *supra* note 68 at 10—11.

Alasaad v. Nielsen, 2019 WL 5899371 (U.S. Dist. Ct., D. Mass., 12 November 2019) [Alasaad]. The plaintiffs brought their suit with the assistance of the American Civil Liberties Union and the Electronic Frontier Foundation as against the departments of Homeland Security, Customs and Border Protection, and Immigration and Customs Enforcement.

⁹³ *Ibid* at 2.

⁹⁴ *Ibid* at 15.

7. ASSESSING THE PROPOSALS FOR CHANGE

Professor Penney makes an important point about the worldwide accessibility of illicit material through the internet. However, it seems likely that there will continue to be cases where it will be appropriate to treat digital information as contraband. For example, consider the case of a person who attempts to bring illicit digital images into Canada in an offline storage system (such as an external hard drive or flash drive), perhaps specifically to evade detection by Canadian internet service providers. 95 Or the case of a person who has created illicit digital images using a smartphone or camera, without the intention of uploading or sharing those images over the internet. 96 More significantly, there will continue to be cases where digital information will be evidence of a contravention of customs law (rather than contraband itself). 97 As society's use of technology increases, the use of technology to coordinate illicit activity will also increase. As Justice Cromwell noted in Fearon, cellphones are the "bread and butter of the drug trade," and it stands to reason that this includes the drug trade over international borders. 98 Accordingly, it seems reasonable that customs officers should have some ability to search devices. The key seems to be articulating reasonable limits on this ability.

Professor Diab offers an attractive solution with his suggestion that a customs search of an electronic device should require either a warrant or exigent circumstances. However, this proposal would impose a higher standard for a device search than for a strip search (an issue that Professor Diab himself acknowledges). This sits uneasily not only with Justice Cromwell's majority view, expressed in *Fearon*, that a device search is "not as invasive as a strip search," but also with Justice Karakatsanis's dissenting view, also expressed in *Fearon*, that there seems to be some equivalence between a device search and a strip search. 100

Professor Currie's suggestion that a device searches should be accompanied by detailed notetaking seems reasonable. As indicated above, this practice appears to have been *substantially* incorporated into the current CBSA

See Whittaker, supra note 39. Although the decision does not explain where the accused originally obtained the child pornography that was found on his devices, he attempted to enter Canada with "two portable computers as well as a bag which contained a number of external hard drives or mass storage devices," which were found to contain a vast quantity of pornographic images (paras 3, 5).

⁹⁶ See *Gibson*, *supra* note 72. Customs agents searched the accused's digital camera, although seemingly no child pornography was found on that particular device.

⁹⁷ See *Appleton*, *supra* note 40; *Fearon*, *supra* note 44. In those cases, device searches revealed text messages showing illegal activity.

Fearon, supra note 44 at para. 48. The original source of the phrase is Constable Garland Carmichael, cited in R. v. Howell, 2011 NSSC 284, 2011 CarswellNS 972 (N.S. S.C.) at para. 39.

⁹⁹ Diab, *supra* note 73 at 123.

¹⁰⁰ *Ibid* at 121.

Guidelines. In addition, Professor Currie's suggestion that device searches should be limited in scope to "basic" functions also seems reasonable, and this practice appears to have been *partially* incorporated into the current CBSA Guidelines. As indicated above, customs officers are instructed to disable wireless activity, examine only what is stored on the device, and only increase the "intensity" of the search if "emerging indicators" are found to justify doing so. It remains unclear at what point customs officers may begin to attach external equipment to a device for the purpose of data retrieval or forensic analysis (i.e. an "advanced search" in the language of *Alasaad*). I agree with Professor Currie, in contrast to *Alasaad*, that the attachment of external equipment to an electronic device should be viewed as sufficiently invasive so as to require a warrant. ¹⁰¹

Furthermore, emphasizing the "cursory" nature of a device search that can be performed on the basis of reasonable suspicion should go at least some way to alleviating the concerns of commentators such as Professor Penny and Professor Diab. To the extent that a device contains highly sensitive or confidential information (such as a lawyer's privileged work product or detailed financial records), this information should be viewed as falling outside of a cursory search. If it is really necessary for a customs officer, in the course of investigating a potential customs violation, to look beyond the "basic" functions of a device (being emails, text messages, photographs, note-taking apps, and the like), then the officer should be required to obtain a warrant. Notably, this approach to device searches (contrasted to an "all or nothing" approach) would seem to comport reasonably well with the Supreme Court of Canada's emphasis on assessing the privacy interests that attach to categories of information, rather than assessing the privacy interests that attach to categories of devices.

Professor Currie's final suggestion, that customs officers form a "reasonable suspicion" of a contravention before initiating a device search, also appears to be reasonable. This is, after all, the current legal standard for strip searches pursuant to section 98. In addition, the standard of "reasonable suspicion" is similar to the current CBSA Guidelines, which direct that customs officers look to a "multiplicity of indicators."

Currie, *supra* note 6 at 312—317. Notably, Professor Currie appears to make a distinction between the use of external equipment to perform a forensic analysis or "mirror" a device's hard drive (p 312), and the use of external equipment to "crack" a password (p 314-317). He concludes that a traveller likely has the right to refuse to provide a device password, but that customs officers likely have the right to confiscate and "crack" a device password if they have formed (only) a reasonable suspicion of a customs violation. It is not essential, for the purposes of this paper, to provide an opinion on this particular point. However, I note that one finding open to the Court is (a) a traveller has the right to refuse to provide any password relating to a device, and (b) customs officers must obtain a warrant to crack any password relating to a device. Another finding is that (a) a traveller has the right to refuse to provide any password relating to a device, and (b) customs officers have a right to crack *only the device password*, on the basis of reasonable suspicion, for the purpose of performing a cursory search.

That being said, the case of *Gibson* should serve as a warning sign that the changes proposed by Currie may not go far enough. In that case, the customs officers appeared to be unaware of, or perhaps indifferent to, the current CBSA Guidelines. They described device searches with a surprisingly casual attitude—occurring as matter of "routine," without a "specific practice," and with "no limitations." While this attitude would undoubtedly be mitigated if the CBSA Guidelines were given the force of law, there seems to be a deeper issue. Three years earlier, in *Fearon*, Justice Karakatsanis predicted a similar issue arising with respect to device searches incident to arrest: "I doubt not that police officers [. . .] would act in good faith, but I do not think that they are in the best position to determine 'with great circumspection' whether the law enforcement objectives clearly outweigh the potential significant intrusion on privacy in the search of a personal cellphone or computer." In other words, it is problematic for customs officers, acting as investigators, to also have complete discretion over whether their investigations meet the appropriate legal standards.

8. A NEW PROPOSAL: DEVICE SEARCHES ARE PERSONAL SEARCHES

In *Hunter*, Justice Dickson found that weighing individual and state interests in the search and seizure context involved consideration of three procedural safeguards: (a) prior authorization, (b) judicial authorization, and (c) objective standards. Adopting a "reasonable suspicion" standard for frontline device searches at customs, as well as limiting the scope of such searches, helps to establish objective standards. Notetaking is undoubtedly a good practice, although it seems to be aimed primarily at having a clear record to assess decision making after a search has already been executed. ¹⁰⁴

A robust approach to protecting individual privacy interests at the border should consider all three procedural safeguards, not only objective standards. My own modest proposal is that a customs device search be treated as a section 98 "search of the person" as opposed to a section 99 "examination of goods." In addition to requiring (a) that a customs officer has "reasonable suspicion" that an individual has contravened customs law in order to initiate a device search, this proposal will also provide an individual with (b) the right to a limited review of a customs officer's decision to initiate a search and (c) the right to counsel.

¹⁰² Diab, supra note 73 at 117. Diab points out that while the searches of the accused's devices in Gibson occurred prior to the implementation of the CBSA Guidelines, the customs officers involved gave evidence as to their current search practices at trial, after the CBSA Guidelines had been implemented.

¹⁰³ Fearon, supra note 44 at para. 172.

¹⁰⁴ Hunter, supra note 1 at para 27.

a. The Equivalence of Privacy Interests

In *Fearon*, Justice Cromwell found that while "[a] cell phone search engages very significant informational privacy interests," it is "not as invasive as a strip search." This is a reference to the famous distinction between "personal privacy, territorial privacy, and informational privacy," whereby personal privacy has been described as having "perhaps the strongest claim to constitutional shelter" because of its connection to human dignity. However, it is also important to remember that while the "distinction between personal, territorial and informational privacy provides useful analytical tools [...] in a given case, the privacy interest may overlap the categories." 107

In the case of a second level customs search (i.e. a "strip or skin-search"), ¹⁰⁸ "[o]fficers do not touch the subject, [and] the subject obviously doesn't touch the officers." ¹⁰⁹ In other words, the subject is asked to remove articles of clothing, in a private area, in the presence of a customs officer. This differs markedly from a third level customs search (i.e. a "body cavity search"), ¹¹⁰ or a collection of bodily samples, ¹¹¹ where the subject is physically probed or manipulated by an agent of the state.

In the case of a device search, even a cursory device search, a customs officer can expect to find a large quantity of intensely personal information that speaks directly to a person's "biographical core." Notably, a 2015 study of American adults aged 18 to 82 found that 87.80% of participants had "sexted" in their lifetime, while 82.20% had done so in the last year. 112 And not only is sexting a very common practice, it can also, apparently, be a healthy practice. The study's author remarked that the "findings show a robust relationship between sexting and sexual and relationship satisfaction." Notably, in *Gibson*, Judge Gillespie remarked that Mr. Gibson had "naked photos of himself on his iPhone," although customs officers testified they had no interest in those photos, "other than to scroll through them in the search for other items." 114

¹⁰⁵ Fearon, supra note 44 at 63.

R. v. Tessling, 2004 SCC 67, 2004 CarswellOnt 4351 (S.C.C.) at paras. 20-21 [Tessling]; R. v. Saeed, 2016 SCC 24, 2016 CarswellAlta 1145 (S.C.C.) at para. 103.

¹⁰⁷ Tessling, supra note 106 at para. 24.

¹⁰⁸ See *Simmons*, *supra* note 4 at para. 30.

¹⁰⁹ R. v. Nagle, 2011 BCPC 481, 2011 CarswellBC 3859 (B.C. Prov. Ct.) at para. 33 [Nagle].

¹¹⁰ Simmons, supra note 4 at para 30.

¹¹¹ R. v. Stillman, 1997 CarswellNB 107, [1997] 1 S.C.R. 607 (S.C.C.).

Emily Stasko & Pamela Geller, "Reframing Sexting as a Positive Relationship Behavior" (paper delivered at the American Psychological Association's 123rd Annual Convention, Toronto, 8 August 2015). "Sexting" was defined by the authors as "sending, receiving, or forwarding sexually explicit messages, images or photos through electronic means."

American Psychological Association, "How Common is Sexting?" (Press release dated 8 August 2015), online: https://www.apa.org/news/press/releases/2015/08/common-sexting.

It is misleading to characterize viewing a person in the state of undress as an issue of "personal privacy," while viewing pictures of a person in a state of undress on a cellphone as an issue of "informational privacy." The dignity interest involved — not to be viewed in a state of undress by a stranger — is nearly identical in both cases. It would also be misleading to characterize "sexting" as an anomalous or deviant behaviour (such that a person might deserve to be exposed for daring to use a cellphone in such a way). In short, a customs officer should not be permitted to casually "scroll through" a person's "naked photos," just as they should not be permitted to casually request that a person remove their clothing. A recognition that a device search is analogous to a section 98 "search of the person" would apply matching procedural protections to matching dignity interests.

b. Review of a Custom Officer's Decision to Search

Sections 98(2) and 98(3) provide that a traveller who is subject to a "search of the person" may request to be taken before "the senior officer at the place where the search is to take place," who shall, "if he sees no reasonable grounds for the search, discharge the person." This provision should also apply to device searches, which would provide at least some oversight of a custom officer's judgment as to whether sufficient grounds exist to initiate a search.

That being said, there remains a question as to whether the protection afforded by way of the section 98 review procedure is sufficient (either in the existing case of strip-searches or the proposed case of device searches). As noted above, section 144 of the *Customs Act 1970* provides that a person can request to be taken before "a police magistrate or justice of the peace, or before the collector or chief officer at the port or place." In *R. v. Williams*, the Ontario District Court found that "s. 144 intentionally provides a means for a person to appear before a judicial person if he or she wishes to do so," meaning that a traveller could choose between any of the three different types of reviewer. New sections 98(2) and 98(3) of the *Customs Act 1986* remove the option to request a review by a "judicial person" (such as a "police magistrate" or "justice of the peace"). Instead, a review can only be done by a "senior officer." It appears that the CBSA has interpreted "senior officer" to mean a "superintendent" or a "person who is the airport director or a chief—someone within senior management."

Recall that, in *Hunter*, Chief Justice Dickson found that it was not necessary for a judge to authorize a search in all cases, as long as the authorizer was capable of "acting judicially" or in a "neutral and impartial manner." But an

¹¹⁴ Gibson, supra note 72 at para 189.

¹¹⁵ R. v. Williams, 1985 CarswellOnt 128, 22 C.R.R. 340 (Ont. Dist. Ct.) at para. 28.

¹¹⁶ R. v. Stanbridge, 1988 CarswellOnt 3237 (Ont. Dist. Ct.) at para. 31.

¹¹⁷ Nagle, supra note 109 at para. 33.

¹¹⁸ Simmons, supra note 4 at para. 32.

authorizer that exercised both investigatory and adjudicatory functions should be viewed with caution. It seems obvious that a frontline customs officer would not be able to satisfy the *Hunter* criteria — the frontline officer's function as an investigator could be expected to inhibit the officer's ability to adjudicate, in a "neutral and impartial" manner, whether sufficient grounds existed so as to initiate a device search. But more significantly, it is also unclear whether even the *reviewer* of the frontline officer, as contemplated by the *Customs Act 1986* (i.e. the "senior officer" who, apparently, can simply be "someone with senior management"), would be able satisfy the *Hunter* criteria. Making a determination on this point would likely require more information as to the reviewer's position, training, and experience.

In any event, it is concerning that a review by a more obvious "judicial person" (specifically a "justice of the peace") was viewed as feasible for the purposes of section 144 of the *Customs Act 1970*, only to be dropped with the introduction of section 98 of the *Customs Act 1986*. In *Simmons*, Chief Justice Dickson specifically found that section 144 was constitutionally valid (although the choice between different types of reviewers was not an issue that was before the court). The Supreme Court has not yet been asked to opine on whether the reduced right of review now articulated in section 98 is constitutionally valid. I suggest that it may not be, and that defence counsel may be wise to challenge section 98 on this basis. In addition, Judges and lawmakers should consider whether changes should be made to section 98 in order to bring it in line with *Hunter*.

c. The Right to Counsel

In Simmons, Chief Justice Dickson found that when Ms. Simmons was required to undergo a strip-search, she was detained for the purposes section 10 of the Charter, which triggered her right to speak to counsel. Building on Simmons, subsequent decisions have broadly construed the definition of "detention" for the purposes of section 10. In R. v. Jones, the Ontario Court of Appeal remarked that while "routine questioning and inspection of luggage at the border does not result in detention," if a customs officer has decided, "because of some sufficiently strong particularized suspicion, to go beyond questioning of a person and to engage in a more intrusive form of inquiry, it may well be that the individual is detained when subject to that routine questioning." Similarly, in R. v. Darlington, the Ontario Superior Court of Justice remarked that "constitutional interests of self-incrimination and right to counsel become engaged where the generality and routineness of the screening exercise give way to more specific and intrusive measures." 121

¹¹⁹ *Ibid* at para. 55.

¹²⁰ R. v. Jones, 2006 CarswellOnt 4972, 81 O.R. (3d) 481 (Ont. C.A.) at paras. 37 & 42.

¹²¹ R. v. Darlington, 2011 ONSC 2776, 2011 CarswellOnt 9732 (Ont. S.C.J.) at para. 75(6).

Since any section 98 search (either in the existing case of strip-searches or the proposed case of device searches) should require that a customs officer form "reasonable suspicion" of a contravention, I suggest that any section 98 search should be considered a "more intrusive form of inquiry" sufficient to trigger section 10. In short, as with a strip search, a person should be given the opportunity to speak to counsel prior to the initiation of a device search.

In the case of a strip search, a traveller who wishes to speak to counsel prior to the initiation of a search is usually directed to telephone "duty counsel." ¹²² In the case of a device search, duty counsel would be able to provide a traveller with valuable advice, such as the scope of the search to be expected (i.e. the device should be placed in "airplane mode"), ¹²³ whether a device password must be provided to customs officers, ¹²⁴ whether access should be provided to a device that contains privileged or confidential information, ¹²⁵ or what the consequences may be for refusing to provide access to a device. ¹²⁶

9. CONCLUSION

The foundational search and seizure cases of *Hunter* and *Simmons* did not contemplate the digital age. However, these cases did outline important procedural protections that are still relevant today. It is not reasonable, and likely not constitutionally permissible, to treat devices simply as "goods." At the same time, it is likely not reasonable for travellers to expect absolute privacy at the border with regard to their electronic devices. What is reasonable is an approach that is sensitive to both legitimate privacy interests of travellers and legitimate state interests to maintain border security. The proposal to treat device searches as section 98 personal searches is such an approach, which charts a

R. v. Marin, 1994 CarswellOnt 7357 (Ont. Gen. Div.) at paras. 5 & 24; R. v. Perzan, 1998
 CarswellOnt 4495, 58 C.R.R. (2d) 80 (Ont. Gen. Div.) at paras. 2 & 14; Kelly v. Palazzo,
 2008 ONCA 82, 2008 CarswellOnt 564 (Ont. C.A.) at paras. 44-45, leave to appeal refused 2008 CarswellOnt 3741, 2008 CarswellOnt 3742 (S.C.C.).

¹²³ See Gibson, supra note 72 at para 30. This case shows that customs officers do not always follow the practice of putting cellphones into "airplane mode" before conducting a search

¹²⁴ See BCCLA, supra note 73 at 30; Currie, supra note 6 at 314. There is ongoing uncertainty as to whether a traveller is legally required to disclose a device password to a customs officer.

¹²⁵ See BCCLA, *supra* note 73 at 57: "The CBSA is supposed to take precautions not to look at privileged materials when it is warned that those materials exist."

See Currie, *supra* note 6 at 289—291, 314—321. Currie discusses the novel case of Alain Philippon, who refused to provide cellphone password and was charged with "hindering" an officer pursuant to section 153.1 of the *Customs Act 1986*. Mr. Philippon ultimately plead guilty to the charge (the facts of his particular case were unflattering, as he was carrying two cellphones, \$5000 in cash, and had traces of cocaine on his luggage). Accordingly, no judicial determination has been made as to the appropriateness of charging a traveller under section 153 for refusing to provide a device password.

course not only between competing privacy interests but also between the existing proposals for change.

What should go through your mind at customs? You should be cognizant that a customs officer could initiate a search of your body or your devices. But you should also feel confident that the customs officer would need some grounds to suspect that you had contravened customs law before engaging in such searches. In short, you should feel confident that your privacy will be respected. And you should feel lucky to be returning to a country that takes the dignity of its citizens seriously.

Appendix

Customs Act, RSC 1970, c C-40 (the "Customs Act 1970")

- 133. (1) Every such officer or person as mentioned in section 132, and every sheriff, justice of the peace, or person residing more than ten miles from the residence of any officer and thereunto authorized by any collector or justice of the peace, may, upon information, or upon reasonable grounds of suspicion, detain, open and examine any package suspected to contain prohibited property or smuggled goods, or goods respecting which there has been any violation of any of the requirements of this Act, and may go on board and enter into any vessel or vehicle of any description whatever, and may stop and detain the same, whether arriving from places beyond or within the limits of Canada, and may rummage and search all parts thereof for such goods.
- (2) If any such goods are found in any such vessel or vehicle, the officer or person so employed may seize and secure such vessel or vehicle together with all the sails, rigging, tackle, apparel, horses, harness and all other appurtenances that, at the time of such seizure, belong to or are attached to such vessel or vehicle, with all goods and other things laden therein or thereon.

[. . .]

SEARCH OF THE PERSON

- 143. Any officer, or person by him authorized thereunto, may search any person on board any vessel or boat within any port in Canada, or on or in any vessel, boat or vehicle entering Canada by land or inland navigation, or any person who has landed or got out of such vessel, boat or vehicle, or who has come into Canada from a foreign country in any manner or way, if the officer or person so searching has reasonable cause to suppose that the person searched has goods subject to entry at the customs, or prohibited goods, secreted about his person.
- 144. (1) Before any person can be searched, the person may require the officer to take him before a police magistrate or justice of the peace, or before the collector or chief officer at the port or place, who shall, if he sees no reasonable cause for search, discharge the person, but, if otherwise, he shall direct the person to be searched; but where the person is a female she shall be searched by a female, and any such magistrate, justice of the peace or collector may, if there is no female appointed for such purpose, employ and authorize a suitable female person to act in any particular case or cases.
- (2) Every officer required to take any person before a police magistrate, justice of the peace, or chief officer as aforesaid, shall do so with all reasonable dispatch.

Customs Act, RSC 1985, c 1 (2nd Supp) [formerly Customs Act, SC 1986 c 1] (the "Customs Act 1986")

Definitions

2(1) In this Act,

 $[\ldots]$

goods, for greater certainty, includes conveyances, animals and any document in any form;

[...]

PART VI

ENFORCEMENT

POWERS OF OFFICERS

Search of the person

- 98 (1) An officer may search
 - (a) any person who has arrived in Canada, within a reasonable time after his arrival in Canada.
 - (b) any person who is about to leave Canada, at any time prior to his departure, or
 - (c) any person who has had access to an area designated for use by persons about to leave Canada and who leaves the area but does not leave Canada, within a reasonable time after he leaves the area.

if the officer suspects on reasonable grounds that the person has secreted on or about his person anything in respect of which this Act has been or might be contravened, anything that would afford evidence with respect to a contravention of this Act or any goods the importation or exportation of which is prohibited, controlled or regulated under this or any other Act of Parliament.

Person taken before senior officer

(2) An officer who is about to search a person under this section shall, on the request of that person, forthwith take him before the senior officer at the place where the search is to take place.

Idem

(3) A senior officer before whom a person is taken pursuant to subsection (2) shall, if he sees no reasonable grounds for the search, discharge the person or, if he believes otherwise, direct that the person be searched.

Search by same sex

(4) No person shall be searched under this section by a person who is not of the same sex, and if there is no officer of the same sex at the place at which the search is to take place, an officer may authorize any suitable person of the same sex to perform the search.

Examination of goods

- 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 and take samples of imported goods in reasonable amounts;
 - (b) at any time up to the time of release, examine any mail that has been imported and, subject to this section, open or cause to be opened any such mail that the officer suspects on reasonable grounds contains any goods referred to in the Customs Tariff, or any goods the importation of which is prohibited, controlled or regulated under any other Act of Parliament,

and take samples of anything contained in such mail in reasonable amounts:

- (c) at any time up to the time of exportation, examine any goods that have been reported under section 95 and open or cause to be opened any package or container of such goods and take samples of such goods in reasonable amounts;
- (c.1) at any time up to the time of exportation, examine any mail that is to be exported and, subject to this section, open or cause to be opened any such mail that the officer suspects on reasonable grounds contains any goods the exportation of which is prohibited, controlled or regulated under any Act of Parliament, and take samples of anything contained in such mail in reasonable amounts;
- (d) where the officer suspects on reasonable grounds that an error has been made in the tariff classification, value for duty or quantity of any goods accounted for under section 32, or where a refund or drawback is requested in respect of any goods under this Act or pursuant to the Customs Tariff, examine the goods and take samples thereof in reasonable amounts;
- (d.1) where the officer suspects on reasonable grounds that an error has been made with respect to the origin claimed or determined for any goods accounted for under section 32, examine the goods and take samples thereof in reasonable amounts;
- (e) where the officer suspects on reasonable grounds that this Act or the regulations or any other Act of Parliament administered or enforced by him or any regulations thereunder have been or might be contravened in respect of any goods, examine the goods and open or cause to be opened any package or container thereof; or
- (f) where the officer suspects on reasonable grounds that this Act or the regulations or any other Act of Parliament administered or enforced by him or any regulations thereunder have been or might be contravened in respect of any conveyance or any goods thereon, stop, board and search the conveyance, examine any goods thereon and open or cause to be opened any package or container thereof and direct that the conveyance be moved to a customs office or other suitable place for any such search, examination or opening.
- (2) and (3) [Repealed, 2017, c. 7, s. 52]

Samples

(4) Samples taken pursuant to subsection (1) shall be disposed of in such manner as the Minister may direct.

The Constitution Act, 1982, being Schedule B to the Canada Act 1982 (UK), 1982, c 11, Part I, Canadian Charter of Rights and Freedoms (the "Charter")

FUNDAMENTAL FREEDOMS

Fundamental Freedoms

2. Everyone has the following fundamental freedoms:

- (a) freedom of conscience and religion;
- (b) freedom of thought, belief, opinion and expression, including freedom of the press and other media of communication;
- (c) freedom of peaceful assembly; and
- (d) freedom of association.

[...]

LEGAL RIGHTS

Life, liberty and security of person

7. Everyone has the right to life, liberty and security of the person and the right not to be deprived thereof except in accordance with the principles of fundamental justice.

Search or seizure

8. Everyone has the right to be secure against unreasonable search or seizure.

Detention or imprisonment

9. Everyone has the right not to be arbitrarily detained or imprisoned.

Arrest or detention

- 10. Everyone has the right on arrest or detention
 - (a) to be informed promptly of the reasons therefor;
 - (b) to retain and instruct counsel without delay and to be informed of that right; and
 - (c) to have the validity of the detention determined by way of habeas corpus and to be released if the detention is not lawful.

[. . .]

ENFORCEMENT

Enforcement of guaranteed rights and freedoms

24.(1) Anyone whose rights or freedoms, as guaranteed by this Charter, have been infringed or denied may apply to a court of competent jurisdiction to obtain such remedy as the court considers appropriate and just in the circumstances.

Exclusion of evidence bringing administration of justice into disrepute

(2) Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.